Размислувања за гласање преку интернет :

Преглед за носители на одлуки во доменот на избори

Бела книга од IFES

Април 2020

USAID
FROM THE AMERICAN PEOPLE

Canada

UKaid
from the British people

INTERNATIONAL FOUNDATION FOR ELECTORAL SYSTEMS
IFES
30 Years

Размислувања за гласање преку интернет:
Преглед за носители на одлуки во доменот на избори

април 2020

Meredith Applegate
Програмски советник, IFES Украина

Thomas Chanussot
Виш експерт за изборни технологии и информатичка безбедност

Vladlen Basysty
Раководител за технологија и информатичка безбедност, IFES Украина

Авторите изразуваат благодарност кон Peter Erben, Ronan McDermott, Dr. Beata Martin-Rozumiłowicz, Dr. Staffan Darnolf и Olha Antonova за нивниот придонес и стручен преглед.

Размислувања за гласање преку интернет: Преглед за носители на одлуки во доменот на избори

Овој извештај е изработен благодарение на поддршката од Global Affairs Canada, UK aid и американскиот народ преку Американската агенција за меѓународен развој (USAID). Мислењата изразени во овој документ се на авторите и не ги одразуваат нужно ставовите или мислењата на Global Affairs Canada, Владата на Канада, Владата на Обединетото Кралство, USAID или Владата на Соединетите Американски Држави.

Фотографија на корицата: Brett Sayles (Pexels)

Содржина

Резиме

Општествата сé повеќе се потпираат на технологија во различни сектори, сè поголем број трансакциски процеси се дигитализираат. Ова почнува да се однесува и на изборните процеси, каде компјутерите и другите технологии станаа неопходни за нивно спроведување. Пандемијата КОВИД-19 што се одвива во моментов го зголеми интересот и побарувачката за преместување на услугите кон мрежниот простор, каде може да се користат далечински. Како што ќе се зголемува оваа побарувачка, носителите на одлуки за изборните процеси ќе треба да ја препознаат единствената природа на изборните процеси и да водат сметка за важните фактори на ризик кога размислуваат за гласање преку интернет.

Во денешно време повеќето изборни органи (ИО) користат одредено ниво на технологија за подобрување на изборните процеси. Од стандардни алатки за канцелариска работа и основни веб-страници, до софистицирани биометриски бази на податоци за регистрација на гласачите и системи за гласање целосно преку интернет, новите технологии можат да ветат нови можности за реализирање на поефикасни, поточни и потенцијално потранспарентни избори. Овде исто така се присутни и нови ризици: технологијата што не е доволно разработена, слабо планирана, користена неправилно од страна на необучени корисници или отвора нови можности за злонамерни актери да ја попречуваат безбедноста и интегритетот на изборните процеси, може да ја поткопа довербата на јавноста.

Воведување на гласање преку интернет - конкретно, употребата на интернет за гласање надвор од избирачките места - веројатно претставува најтешка технолошка надградба за еден изборен орган, бидејќи ја зафаќа самата суштината на целиот изборен процес. Далечинско гласање преку интернет во голема мерка ја намалува директната контрола на изборните органи врз изборниот процес. Ваквиот начин на гласање дава можност да се решат некои историски изборни проблеми - како што е подобрување на условите за гласачи што се наоѓаат во странство, гласачи со попреченост и внатрешно раселени лица - и претставува можност потенцијално да се добиваат побрзи резултати без човечки грешки произлезени од пребројувањето на гласови, на пример. Но, исто така, воведува и широк спектар на нови ризици и причини за загриженост од гледна точка на безбедноста, тајноста, транспарентноста и довербата. Следствено, дискусиите за гласање преку интернет обично предизвикуваат повеќе критики и спорови отколку која било друга технологија за изборни процеси. Гласањето преку интернет сè уште е многу нова технологија, со многу мал број успешни примери што може да се проучуваат и од кои може да се извлекуваат поуки.

Релевантноста на оваа технологија треба соодветно да се процени пред да се примени во било кој контекст, според пет параметри: трошоци, учество, ефикасност, доверба и безбедност. Безбедност во овој контекст не се однесува само на потенцијалот за упади во компјутерски системи, на пример, туку и личната безбедност - имено, личната приватност и тајност потребни за испраќање на гласачкото ливче.

Додека **трошоците за гласање преку интернет** по одреден период би можеле да станат пониски од традиционалното гласање, ќе бидат потребни неколку изборни циклуси да се оствари тоа, бидејќи има значителни нови набавки, обука, кампањи за подигнување на јавната свест и

безбедност, што се потребни за воведување на ваков систем. Гласањето преку интернет честопати се потпира врз средства како што е силна инфраструктура за лична идентификација - биометриски избирачки легитимации, паметни лични карти, итн. - што може да биде скапо, ако не е веќе воведено од порано.

Иако гласањето преку интернет може да изгледа привлечно како начин за зголемување на излезноста на гласачите, истражувањата покажаа дека тоа најчесто не е случај. Тие истражувања покажа дека **гласањето преку интернет може да направи гласањето да биде "поудобно" за постојните гласачи, но нема тенденција да привлекува нови гласачи**. Особено на младите гласачи се чини дека им е поважно размислувањето зошто воопшто би гласале, отколку на кој начин.

Повеќето форми на електронско гласање, вклучително и гласање преку интернет, ја подобруваат брзината и сигурноста на испраќањето на гласачки ливчиња. Гласањето преку интернет може да биде полезно во смисла поширока група луѓе да може да ги остварат своите права, како што се гласачите кои не се во можност да патуваат до нивните избирачки места или гласачите со попреченост. Сепак, во исто време, гласањето преку интернет може практично да исклучи некои од другите заедници - оние кои немаат пристап до или не знаат да користат интернет, меѓу кои несразмерно се застапени повозрасните и руралните гласачи во многу случаи. Доколку се спроведе, ќе има потреба од опсежна едукација на гласачите.

Технологијата врз којашто се темели гласањето преку интернет е високо софистицирана, опфаќа напредна математика и криптографија. Повеќето гласачи нема да разберат како точно функционира, а овој недостаток на разбирање може да ја поткопа **јавната доверба**. Оваа доверба може да се заслужи со воспоставување на темелни процедури, вклучително и контроли, и обезбедување на доволно информации за чинителите да можат целосно да ги разберат редоследот и механизмите на процесот на гласање. Треба да се внимава во поглед на ставовите на јавноста. Недостаток на доверба во изборниот процес може драматично да влијае врз впечатокот за легитимност на избраните функционери.

Безбедноста - како и перцепциите за безбедноста - треба да биде клучна тема пред воведување на гласање преку интернет. Неколку земји ги напуштија пробните програми за гласање преку интернет - вклучително Франција, Холандија и Норвешка – токму поради загриженоста околу безбедносните аспекти. Држави кои доживуваат чести, а понекогаш и разурнувачки информатички напади, мора да ги преземат сите неопходни мерки за да ја зголемат отпорноста на нивната изборна инфраструктура. Исто така, мора да се води сметка и за личната безбедност, односно приватноста на гласачите. За далечинско гласање преку интернет мора да се преземат мерки за да се почитува и спроведува тајноста на гласањето.

Технологиите можат да ги зајакнат изборните процеси ако внимателно се разработат и спроведат; со вакви процеси не треба да се брза заради огромните последици ако евентуално се случи неуспех. Првата фаза во процесот на размислување за усвојување на електронски технологии за гласање и броење на гласовите е робусна физибилити студија и испробување на новата технологија во помала изборна единица, пред да се воведе со целосен опфат.

Вовед

Како што напредува во технологијата и сé повеќе трансакции стануваат електронски, често се поставуваа прашањето кога гласањето на избори навистина ќе влезе во дигиталната ера. На крајот на краиштата, голем број интернет корисници им веруваат на веб-страниците и мобилните апликации во однос на финансиски информации и друштвени интеракции - се чини природно да се има исто ниво на доверба кога се гласа онлајн.

За време на пандемијата КОВИД-19 целата деловна активност, работните места, јавните и образовните услуги брзо се преселуваа на интернет. Сепак, изборите имаат одредени посебни одлики. Голем е бројот на сложени, сериозни прашања што треба да се земат предвид кога станува збор за гласање преку компјутер или телефон во неконтролирано опкружување - овие теми значајно влијаат на впечатокот во јавноста за легитимноста на избраните функционери и интегритетот на самата демократија. Овие теми опфаќаат јавна доверба, тајност на гласањето, принуда, заплашување и сигурни механизми за идентификација. Системот треба да биде потполно проверлив за да се обезбеди дека сите гласови се испратени како што е наменето и се изброени онака како што се испратени, без да се загрозува тајноста на гласањето.

Овој документ нема намера да настапи со став дали треба да се користи или да се избегнува гласање преку интернет; Меѓународната фондација за изборни системи (International Foundation for Electoral Systems - IFES) не е универзално за или против гласање преку интернет. Всушност, преку преглед на студиите на случаи и постојната литература, овој документ има за цел да им помогне на изборните чинители да ги постават вистинските прашања за да утврдат дали гласањето преку интернет дополнително би го подобрило интегритет на изборите и демократијата, или дали наместо тоа би ја поткопало довербата на јавноста и безбедноста на изборниот процес.

Историја и примена на гласање преку интернет

Додека гласањето од далечина преку интернет има потенцијал за во иднина, тоа претставува нов пристап кој само во многу мал број случаи бил успешно спроведен. Гласањето преку интернет сè уште е технологија во развој кога станува збор за безбедност и доверба; поради овие потешкотии, голем број држави одлучија избраа да не го употребуваат откако спроведоа физибилити студии или пробни активности. интернет-гласањето за прв пат се користеше за обврзувачки политички избори во 2000 година во Соединетите држави (САД) како пилот-проба во неколку сојузни држави наменета за гласачите што престојуваат надвор од земјата. Оттогаш, околу десетина земји експериментирале со оваа технологија. Овој документ не разгледува гласање преку интернет во контролирани услови/средини, како што се избирачките места, бидејќи тоа е слично на разновидни други електронски методи на гласање за кои веќе се реализирани значителен број истражувања.

Естонија е единствената држава што користи гласање преку интернет на целата територија. Неколку други користат гласање преку интернет во одредени региони или за одредени сегменти на гласачкото тело (Ерменија, Австралија, Канада, Панама, Швајцарија и САД). Некои земји имаат спроведено ограничени пилот-проби на гласање преку интернет и се определиле да не ја продолжат неговата употреба (Велика Британија и Норвешка). Други отпрвин усвоиле гласање преку интернет, но потоа одлучиле да го прекинат (Индија, Франција, Холандија и Шпанија).[1] Погледнете во Анекс 2 за дополнителни информации за тоа како одделни земји го користеле или испробале гласањето преку интернет. Земјите што применуваат гласање преку интернет најчесто го насочуваат кон определени категории на гласачи - на пример, гласачи што престојуваат во странство, дипломатски или воен персонал на служба во странство, привремено отсутни гласачи или гласачи со попреченост. Општо земено, гласањето преку интернет им се нуди на гласачите пред општиот ден на избори во период што се разликува од земја до земја, но најчесто една до две недели.

Тематска анализа

За да се процени дали би било соодветно гласање преку интернет, една држава мора да спроведе физибилити студија што анализира како оваа промена би влијаела врз критичните аспекти на демократскиот процес. Таквата студија треба да се фокусира конкретно на потешкотиите што државата се обидува да ги поправи или подобри преку воведување на оваа технологија: на пр. трошоци или излезност на гласачите. Општо гледано, технологијата треба да се воведе како „решение“ само доколку постои проблем што може да го ублажи. Додека Естонија користи гласање преку интернет на ниво на целата држава, постојат сериозни причини што другите земји одлучиле да не го спроведат овој механизам. Секоја одлука треба да ја земе предвид не само

[1] Повеќе детали и ажуриран список на држави и модели на реализација се дадени во Анекс 2.

технологијата што ќе биде потребна, туку и добрите и лошите страни што реализацијата би ги имала врз гласачкото тело и интегритетот на изборниот процес. Можностите - и ризиците - на овие технологии треба соодветно да се оценат пред евентуална примена во кој било контекст, според пет параметри: трошоци, учество, ефикасност, доверба и безбедност.

Трошоци

Изборите честопати се сметаат за најголеми логистички предизвици со кои се соочува една земја во мирнодопски услови. Тешко е да се проценат вкупните трошоци за изборите бидејќи често се користи јавната инфраструктура за поддршка на активностите на денот на гласање и во процесот на пребројување на гласовите. Поради ваквите огромни логистички трошоци и користењето на инфраструктурата, замислата за дигитализација на изборните активности е привлечна. Можно е на долг рок навистина да се реализираат заштеди на трошоците, под претпоставка ако излезноста на гласачите е константна, бројот на интернет гласачи се зголемува а бројот на традиционални гласачи се намалува.[2] Сепак, слаби се изгледите дека гласањето преку интернет би ги намалило трошоците за инаку скапи потфати, како што се регистрација на гласачите, означување на граници на изборни окрузи/единици и предлагање на кандидати. Покрај тоа, веројатно е дека далечинското гласање преку интернет не би било единствената опција за гласање достапна во првиот или два изборни циклуси, што значи дека изборната администрација ќе мора да понуди и традиционално гласање со лично присуство и гласање преку интернет, па затоа ќе се забележи пораст наместо намалување на трошоците на краток до среден рок.

Поуки од Естонија

Естонската програма за лични карти и систем за онлајн гласање не беше без спорни елементи.

Ревизијата објавена во 2014 година од тим меѓународни истражувачи ја критикуваше слабата оперативна и процедурална безбедност. Беа утврдени клучни слабости кои можат потенцијално да се искористат за бришење гласови и преземање на контрола врз серверите.

Критична слабост, утврдена во 2017 година во системот за лични карти, дозволува на секој што го знае јавниот клуч на личната карта да го копира приватниот клуч релативно евтино и да го користи за целосна контрола врз идентитетот на некое лице без да ја има во посед физичката лична карта. Влијанието на оваа слабост врз изборниот процес можеше да биде исклучително штетно доколку тајмингот на разоткривањето беше поинаков. Естонските власти се повратија од кризата со усвојување на политика на максимална транспарентност за влијанието на слабоста и дејствијата што ги преземаа за да ја ублажат. Ова е можно само во контекст кога јавноста им верува на властите и населението е релативно малуброjно и хомогено - Естонија имаше 887.420 гласачи во 2019 година.

[2] International Foundation for Electoral Systems, Ben Goldsmith, *Internet Voting: Past, Present and Future, 2013*; https://www.ifes.org/news/Internet-voting-past-present-and-future

Повеќе студии и изданија покажуваат дека трошоците за гласање преку интернет се многу пониски од стандардното гласање - приближно за половина. Сепак, *во тие проценки не се пресметани трошоците за обука и активностите за подигнување на јавната свест, ниту трошоците за воспоставување на сигурна инфраструктура за електронски идентитет, врз која се потпира естонскиот систем за гласање преку интернет*.

Естонскиот систем за гласање преку интернет во основа е изграден врз естонската лична карта. Затоа, не е можно разумно да се издвојат трошоците за гласање преку интернет од дециниските инвестиции во голем екосистем за електронска администрација кој вклучува меѓуресорски систем за размена на податоци (X-road), задолжителен електронски документ за лична идентификација (и двете естонската влада ги развива од 90-тите години) и обезбедување на гласање преку интернет (eesti.ee).[3] Естонската картичка е задолжителна државна лична карта за граѓаните, претставува смарт-картичка што овозможува и безбедна далечинска автентикација и правно обврзувачки дигитални потписи за употреба во естонската државна инфраструктура со јавни клучеви.[4] Смарт-картичките беа воведени во 2002 година, а услугите се прошируваат постепено со години. Оваа инфраструктура може да се користи за идентификација и автентикација за сите јавни услуги како што се даночни пријави, доказ за идентитет за пристап до банкарски сметки, проверка на медицински картони и употреба на е-рецепти и друго. Има критики за време на ревизорските

Поуки од Норвешка

Норвешка направи проба со ограничен систем на гласање преку интернет за локалните избори во 2011 и 2013 година, но го откажа проектот во 2014 година, повикувајќи се на загриженост околу безбедноста и заклучок на владата дека, спротивно на очекувањата, новиот систем не ја подобрил излезноста. Институтот за социјални истражувања во Норвешка наведе дека *„нема докази дека пробата доведе до пораст на вкупниот број лица што гласале, ниту дека мобилизирала нови групи, како што се младите, да гласаат“. Дури и само „лесен“ преглед на системот од компјутерски експерти од Норвешкиот компјутерски центар и Норвешкиот универзитет за наука и технологија најде „значајни проблеми“ со безбедноста, меѓу другото, до тој степен што експертите велат дека софтверот „нема прифатлив квалитет за употреба во систем на е-гласање“*. Вреди да се напомене дека норвешките власти не ја спомнаа безбедноста како првенствена тема, спротивно на повеќето други оценки и студии на случаи. Како и да е, се наведува дека гласачите имаат многу ограничени знаења за безбедносните механизми во системот, што влијае врз премисата на слободни и фер избори.

[3] Естонија има значителни вложувања во својот екосистем на е-администрација, чиишто вкупни трошоци е тешко да се проценат и не се јавно достапни. Некои проценки велат дека само одржувањето на x-road чини 50 до 60 милиони USD годишно https://www.innovations.harvard.edu/blog/estonia-one-small-country-digital-government-having-big-impactx-road

[4] Robert Krimmer, David Duenas-Cid and Iuliia Krivonosova (2020) *New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper?*, Public Money & Management: https://www.tandfonline.com/doi/full/10.1080/09540962.2020.1732027

проверки[5] и откривањето на слабостите[6] (видете „Лекции од Естонија“ во полето погоре)[7]. Во Естонија, гласачите вршат лична автентикација на веб-страница за да го дадат својот електронски глас. Користат и дополнителен хардвер: читач на лични карти поврзан со нивниот компјутер, што го чита криптираниот клуч на картичката. Гласачите можат да ги менуваат своите електронски гласови неограничен број пати, а последниот глас е оној што се евидентира. Исто така е можно секој кој гласа преку интернет да гласа и на избирачко место за време на раниот период на гласање, со што автоматски се поништува гласањето на тоа лице извршено преку интернет, но за тоа се потребни избирачки места кои можат да ги опслужат гласачите без разлика дали гласале онлајн или не.

Затоа, иако првичните пресметки на трошоците може да изгледаат дека одат во прилог на гласањето преку интернет на краток рок, земање предвид на среднорочни и долгорочни трошоци кои не се веднаш очигледни може да доведе до мошне различна пресметка на трошоците. Императивно е тоа да се случи на почетокот на дискусиите со цел чинителите целосно да ги разберат критериумите врз основа на кои одлучуваат дали да се воведе таква технологија.

Влијание врз излезноста

Излезноста на избори се намалува во целиот свет. Голем број државни раководства бараат начини да ги подобрат традиционалните системи на гласање за да се спротивстават на она што го сметаат за закана поради опаѓањето на демократско учество. Гласањето преку интернет може да изгледа како разумен одговор на овие проблеми, особено ако се има предвид потенцијалната леснотија на пристап и заштеда на време за некои гласачи. Постојат повеќе истражувања кои претпоставуваат дека обезбедувањето разновидни начини на гласање ја зголемува излезноста. За жал, овие студии обично се изразено пристрасни, истакнувајќи ги само придобивките што може да ги донесе технологијата, додека претежно се потпираат врз хипотези и анкети, наместо на истражувања засновани врз докази. Честопати овие студии даваат широки заклучоци без да водат сметка за специфичниот политички или државен контекст, општествените импликации или други фактори што ја определуваат излезноста на гласачите: на пр. недоверба во системот, задоволство од постојната состојба, видот или нивото на избори, довербата во партиите и кандидатите, интензитетот на кампањата и интересот на медиумите за изборите.

Пандемијата КОВИД-19 претставува беспримерна ситуација за современиот свет, при што граѓаните во повеќе земји не можат да патуваат или да ги напуштат своите домови. Онлајн систем за далечинско гласање може да реши некои од пречките за учество ако, на пример, големи сегменти од гласачкото тело не се во можност физички да дојдат до избирачкото место заради ненадејна државна (или, во овој случај, глобална) вонредна состојба. Но, ефикасно

[5] Преглед на службените објави и одговорот по наоѓањето на ROCA грешката во естонската лична карта; https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf and https://e-estonia.com/wp-content/uploads/faq-a4-v02-id-card-1.pdf)

[6] Презентација на ревизијата од меѓународната екипа; https://estoniaevoting.org/ и https://nordicinnovationlabs.com/wp-content/uploads/2018/07/ivotingccs14.pdf; одговор од Изборната комисија на Естонија; https://estoniaevoting.org/press- release/responsenational-election-committees-statement/

[7] Препораки од конечните извештаи на ОБСЕ/ОДИХР за парламентарните избори во Естонија, 2005-2019.

воспоставување на систем за далечинско гласање преку интернет е долготраен процес. Ако е веќе воспоставен и испробан пред вонредната состојба, тоа може да биде позитивно во однос на излезноста во време на криза како што е КОВИД-19. Сепак, поради потребата од опсежно планирање, подготовка и тестирање, слаби се изгледите дека државите што немаат веќе воспоставени системи би биле во состојба - или дека дури би требало да се обидуваат - да започнат со гласање преку интернет како одговор на криза.

Како единствена земја што спроведува гласање преку интернет на ниво на цела држава, Естонија повторно може да понуди одредени некои квантитативни податоци и сознанија.[8] Во Естонија немаше значителна промена во учеството на гласачите по воведувањето на гласање преку интернет; се утврди дека тоа е заменски механизам за гласање за гласачите кои веќе се вклучени во изборниот процес.[9] Главниот заклучок во однос на искуството на гласачите е дека ваквиот вид гласање е „поудобно“ за гласачите што и инаку редовно излегувале на избори, наместо да се зголеми учеството на оние кои претходно не гласале.[10] Трендот покажува дека сè повеќе луѓе гласаат онлајн и дека гласачите кои еднаш гласале преку интернет ќе продолжат да гласаат на тој начин.

Норвешкиот пример наведува и интересен наод во врска со помладите гласачи, кои често се посочуваат како аргумент во корист на гласањето преку интернет. Младите гласачи што учествуваа во пилот-изборите во Норвешка се чинеше дека претпочитаа да гласаат на гласачкото место на денот на гласање, како изразување на политички став. Според наодите на комисијата што ги анализираше резултатите од пилот-пробата, младите изјавија дека поважно им е прашањето зошто воопшто младите би требало да гласаат, отколку на кој начин би гласале.[11] Иако гласањето преку интернет не треба да се исклучува во однос на неговиот потенцијал за зголемување на учеството на гласачите, тоа мора да биде придружено со широко граѓанско образование, едукација на гласачите и јавно информирање што ќе ги охрабри гласачите да учествуваат во политичкиот процес.

Пристапност

Правото да се гласа за избраните претставници е камен-темелник на демократијата, загарантирано во бројни меѓународни повелби и договори, вклучително и Копенхашкиот

[8] Tove Wigartz (University of Gothenburg), *Does Internet voting in Estonia affect voter turnout?, 2017*; https://core.ac.uk/download/pdf/95665595.pdf

[9] Kitsing Meelis, *Online participation in Estonia: Active voting, low engagement*, *2011*; https://www.researchgate.net/publication/221547555_Online_participation_in_Estonia_Active_voting_low_engagement

[10] Други статии за влијанието на онлајн гласање врз излезноста во Естонија; http://www.democraticaudit.com/2013/10/03/the-estonian-experience-shows-that-while-online-voting-is-fasterand-cheaper-it-hasnt-increased-turn-out/; преглед на статистички податоци од Владата на Естонија за гласањето преку интернет; https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia

[11] Истражување за влијанието на гласањето преку интернет во Норвешка; https://www.regjeringen.no/en/historicalarchive/Stoltenbergs-2nd-Government/Ministry-of-Local-Government-and-Regiona/tema-og-redaksjoneltinnhold/kampanjesider/e-vote-trial/evaluations-of-the-e-voting-trials/evaluation-of-the-e-voting-trials-in201/summary-of-the-isf-report/id685824/

документ и Конвенцијата на Обединетите нации за правата на лицата со попреченост. Сепак, за гласачите со попреченост чии избирачки места не се достапни, ова право во голема мерка не се почитува во многу земји низ целиот свет. Гласањето преку интернет би можело да понуди можност за поголем број лица со попреченост да добијат пристап до своето право да гласаат ако нема други опции за далечинско гласање. Покрај тоа, можноста гласачот со попреченост да користи свој електронски уред за гласање може да обезбеди полесна пристапност, бидејќи голем број уреди вклучуваат функции за пристапност што нудат дополнителни можности за аудио или зголемен (полесно читлив) текст, на пример. Меѓутоа, дури и ако далечинското гласање преку интернет обезбедува полесен пристап за лицата со попреченост, тоа мора да биде придружено со достапни постапки за регистрација и идентификација на гласачите, како и информации и едукација на гласачите во форми што се достапни и лесно разбирливи за сите гласачи, вклучително и гласачите со попреченост.

Ефикасност

Гласањето преку интернет потенцијално може значително да го забрза процесот на гласање за гласачите кои се во можност да го користат, со заштедување на време и можеби избегнување на физички пречки како што е одење до и од гласачкото место, избегнување на евентуални редици/турканици и овозможување на брзо гласање од дома. Сепак, важно е да се напомене дека употребата на компјутери или технологија не им оди лесно на сите гласачи; треба да се води посебна грижа за да се разбере нивото на технолошка писменост во една земја. Треба да се посвети внимание на инфраструктурата, како во однос на нивоата на јавно достапен интернет, така и личната инфраструктура - какви мобилни телефони (и соодветни претплатнички пакети за податочен сообраќај) поседуваат луѓето, имаат ли компјутери со доволен капацитет на интернет-врска, итн.

Иако резултатите и самото гласање се многу побрзи со гласање онлајн, неопходно е да се разгледа што се жртвува во името на оваа непосредност и практичност, и кои чекори мора да се преземат за ублажување. Во однос на тајмингот - и законитоста - носителите на одлуки исто така мора да размислат какви законски измени се неопходни за да се воведе далечинско гласање преку интернет како можност.[12] Во зависност од контекстот, овој процес на изменување и дополнување може да биде обемен и долготраен. Правните размислувања треба опфатат:

[12] Постојат бројни референтни материјали што може да се разгледаат кога се размислува за измени во законската рамка. Извештајот на IFES за гласањето преку интернет во Норвешка нуди рамка за проверка на усогласеноста на гласањето преку интернет со меѓународните стандарди: https://www.regjeringen.no/globalassets/upload/krd/prosjekter/evalg/evaluering/topic7_assessment.pdf. Препораката на Советот на Европа од 2017 година е веројатно најважната збирка стандарди досега со над 49 елементи групирани според *универзално право на глас, еднакво право на глас, слобода на гласањето, тајност на гласањето, регулаторни и организациски услови, транспарентност и набљудување, отчетност и сигурност и безбедност на системот*: https://www.coe.int/en/web/electoral-assistance/-/council-of-europe-adopts-new-recommendation-onstandards-for-e-voting. Исто така се оформува сé пообемна збирка стандарди за електронски гласање од IFES, ОБСЕ/ОДИХР, Картер центарот и други, особено во делот на набљудување на избори, но применливи и како упатства за ИО.

- Тајност на гласањето: Едно од најконтроверзните прашања е дали гласањето во неконтролирано опкружување е во согласност со принципот на тајност на гласањето и како може да се обезбеди тајноста на гласањето кога гласањето се врши далечински од личен електронски уред.[13]
- Проверки, повторно пребројување и администрација: Треба да се поведе сметка за правната рамка со која се уредува проверката и организацијата на изборите и компетентноста на изборните органи, вклучително и сертифицирање на системите, ревизии, повторно пребројување, записи што може да бидат проверени од самите избирачи, и друго.
- Ефекти врз условите за транспарентност, како што е улогата на набљудувачите и партиските претставници
- Влијание на гласањето преку интернет врз неважечки и празни гласачки ливчиња

Најнакрај, воведувањето на електронско гласање од било каков вид бара значителни промени во државната правна рамка за избори.[14] Сепак, за првичните пилот-проекти можеби е оправдано да се донесуваат посебни одредби кои се однесуваат само на овие експериментални проекти, пред да се спроведе целокупната ревизија на правната рамка, доколку таквото гласање треба потоа да се воведе на ниво на целата држава.

Сеопфатна проверливост

Сеопфатна проверливост [End-to-end (E2E) verifiability] е предуслов за секој веродостоен систем за електронско гласање. Без тоа, речиси и да нема начин да се обезбеди доверба во процесот и да се изврши ревизорска проверка на гласачко ливче. СП користи криптографски функции за да му овозможи на гласачот да провери дали гласачкото ливче е испратено (евидентирано) и пресметано (изброено) онака како што е предвидено (индивидуална проверливост). СП исто така овозможува трети страни да ги проверуваат изборните резултатите за да ја потврдат нивната точност (општа проверливост). Ова значи дека резултатите може да бидат подложени на ревизија за проверка на точност, потенцијално од било кои засегнати страни: поединци или независни организации, како што се медиуми, политички партии или невладини организации. Како и сите системи отворени кон интернет, СП не штити од софистициран штетен софтвер (malware) што може да биде специјално изработен за да шпионира како избираат гласачите, да ја компромитира тајноста на гласачките ливчиња или лажно да гласа во име на легитимен гласач.

Освен тоа, тешко е да се обезбеди начин за гласачите да проверат како гласале без истовремено да се овозможи гласачите истото да го покажуваат на трети лица, што носи ризик од купување гласови или принуда. Со текот на годините, Естонија ги подобри техниките за да им овозможи на гласачите да го проверат својот глас пред да биде трајно евидентиран. После гласањето на

[13] Оваа дискусија се однесува и на гласање по пошта и можноста да се гласа повеќепати. Естонија го ублажува ова и потенцијалот за притисоци со тоа што се брои само последниот даден глас онлајн. Во Естонија може и секој што гласал преку интернет да гласа и лично во избирачко место на денот на гласање, со што се поништува евентуално претходно дадениот глас преку интернет.

[14] Кодексот на Венецијанската комисија за добри практики во изборната област укажува дека не би требало да има поголеми измени во изборното законодавство во периодот од една година пред избори; https://rm.coe.int/090000168092af01

компјутер, секој избирач добива QR код кој важи само 30 минути и му овозможува на гласачот да го провери гласањето од друг уред, на пр. смарт-телефон.[15] Ова, секако, подразбира гласачот да поседува повеќе уреди со интернет врска. Треба да се има на ум дека функцијата индивидуална проверливост на гласачко ливче испратено преку интернет исто така отвора можност за купување гласови, и во моментов нема технологија што може тоа ефикасно да го ублажи.

Ограничена можност за ревизорска проверка на резултатите

Ревизорски проверки за ограничување на ризикот, како и можноста за спроведување на какво било повторно пребројување на гласовите, се мошне ограничени, ако не и невозможни, кога гласачките ливчиња се испраќаат преку интернет. За разлика од некои современи машини за електронско гласање, не се изработува запис (ревизорска трага) на хартија. Ова ја отежнува можноста ИО да вршат ревизорски проверки на изборните резултати доколку настане спор. Во политичко и социјално опкружување условено од доверба и транспарентност, ова е веројатно најважниот недостаток на гласањето преку интернет.

При постизборна ревизорска проверка за ограничување на ризикот рачно се проверува случаен, статистички релевантен примерок на (физички/хартиени) гласачки ливчиња за да се види дали електронските апарати за гласање и скенерите на гласачки ливчиња правилно функционирале.[16] Ревизорска проверка со споредување на гласачките ливчиња опфаќа и независно пребројување на сите гласачки ливчиња, не само статистички примерок, за да се провери дали апаратите точно ги пресметале збировите. Постизборните ревизорски проверки се од огромно значење за избори со електронско броење на гласовите и претставуваат дел од добрата практика ширум светот.[17] Нивните придобивки ги истакнуваат политолози, статистичари и експерти за безбедност на избори.[18]

[15] QR код е еден вид тродимензионален бар-код, претежно се користи за претставување на информации (URL или контакт информации) и се чита/дешифрира со наменска апликација на мобилен телефон; https://en.wikipedia.org/wiki/QR_code

[16] Mark Lindeman and Philip B. Stark, *A gentle introduction to Risk Limiting Audits*, *2012*; https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

[17] The Belfer Center, *State and Local Election Cybersecurity Playbook, 2016*; https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

[18] The Brennan Center, *America's Voting Machines at Risk, 2015*; https://www.brennancenter.org/sites default/files/publications/Americas_Voting_Machines_At_Risk.pdf

Доверба и транспарентност

Изборните процеси мора да дадат резултати што ја одразуваат волјата на гласачите во средина што воспоставува доволна доверба за тие резултати да бидат прифатени како валидни. Впечаток дека се случува изборна измама може да биде исто толку штетен по веродостојноста на изборите како и вистинска измама. Голем број фактори придонесуваат за оваа доверба, вклучувајќи ја и перцепцијата на јавноста за самиот ИО, политичкото опкружување, историјата на измами или злоупотреби во одредена држава, и довербата во самиот систем и алатките што се користат во изборниот процес. ИО мора да бидат будни во одржувањето на транспарентен процес што ќе им овозможи на сите засегнати страни да веруваат дека гласањето, процесот на броење и самите резултати се легитимни.

Секое воведување на нова технологија во изборен процес треба внимателно да се испланира[19]. Негативно прво искуство – или разоткривање на слабост во системот – може да ги сврти изборните чинители против технологијата, и потоа тешко се враќа довербата. За ова има бројни примери: Референдумот во Барселона в Шпанија[20] беше спорен на повеќе нивоа, вклучително и самото гласање, со пријави за случаи на лажно претставување упатени до суд; изрази на загриженост во јавноста во Норвешка[21] и Франција.[22] Покрај гласачите, раководствата и персоналот во изборните органи исто така мора да ја разбираат и да имаат доверба во технологијата што ја употребуваат во нивното работење. Тоа може да се постигне само со

Поуки од Швајцарија

Кантоните во Швајцарија експериментираа со гласање преку интернет, но бројот на валидни и излезени гласачи остана маргинален заради тестовите и ревизорските проверки, трошоците и довербата на јавноста. Паралелно се испробани два системи. Системот sVote од Swiss Post е комерцијален, обелоденет софтвер развиен од Scytl. Нуди опција за гласачите кои живеат во Швајцарија и оние во странство да гласаат преку мобилна апликација и веб-страница. Методот за автентикација на гласачите суштински се разликува од системот во Естонија. Не се заснова на софистицирана лична карта, туку на уникатен безбедносен код испратен по пошта; потребна е претходна регистрација за гласачите да ги добијат безбедносните шифри. Избирачите потоа треба да го внесат своите својот гласачки број, безбедносниот код, датум на раѓање и матична општина. Гласањето преку интернет беше предмет на жестока дебата во Швајцарија кога властите организираа „награда за наоѓање грешки“ (bug bounty), при што беа утврдени и јавно обелоденети критични слабости. Овој систем сега е напуштен од швајцарските власти. Вториот систем - Женевскиот систем - исто така неодамна беше запрен. Според тоа, иднината на гласањето преку интернет во Швајцарија во моментов не е јасна.

[19] ACE Project, *Guiding principles for election technology – trust and transparency*; http://aceproject.org/main/english/et/et20.htm

[20] *Информативна статија за референдумот во Барселона*, стр. 124; https://www.regjeringen.no/globalassets/upload/krd/prosjekter/e-valg/evaluering/topic6_assessment.pdf

[21] https://www.bbc.com/news/technology-28055678

[22] https://www.reuters.com/article/us-france-election-cyber/france-drops-electronic-voting-for-citizens-abroadover-cybersecurity-fears-idUSKBN16D233

ригорозни постапки за оценка и делотворни стратегии за обука. Надворешните даватели на услуги вклучени во реализација на изборите, исто така, мора да ги исполнуваат законските и други услови; ако постои впечаток дека овие даватели на услуги го прекршуваат законот, довербата кај засегнатите чинители се урива. Изборните органи треба да извршат посебна проценка на ризикот во врска со потенцијалните поврзаности и зависности на надворешните даватели на услуги, бидејќи овие врски може да ја поткопаат веродостојноста на новиот систем. Ова не важи само за добавувачите од приватниот сектор, туку се однесува и на зависностите од другите државни институции.

Покрај можностите за измама, кои се изложени поподробно во делот „Безбедносни аспекти“ подолу, слабо обучените администратори може ненамерно да создадат грешки кои брзо ја ослабнуваат јавната доверба. Гласачи што не разбрале како правилно се употребува системот може самите да направат грешки, а подоцна тоа да го припишат на намерна злоупотреба од страна на ИО. Пилот-проби и воведување на проекти за гласање преку интернет треба да се прават само во политички и општествен контекст кога веќе постои високо ниво на доверба во изборниот систем. Гласањето преку интернет само по себе не значи дека ќе се зајакне довербата – всушност, може и да ја намали,[23] или може партиски/политички да се инструментализира. Слично, недостатокот на јавна доверба во непристрасноста на персоналот во изборните органи нема да се подобри со воведување повеќе технологија во процесот; наместо тоа, оваа доверба се гради со активна борба против коруптивните постапки и зголемување на транспарентноста. Овие прашања на доверба треба сеопфатно да се решат пред да се воведува технологијата во изборниот процес.

Безбедносни аспекти

Во текот на изминатата деценија се појавија бројни познати напади на интернет портали, вируси што блокираа веб-страници на државни/владини институции и големи корпорации, и софтвер за уцена (ransomware) што ги парализира организациите со шифрирање на нивните податоци. Со оглед на важноста на изборите, разумно може да се претпостави дека злонамерни актери - особено во земји со специфични геополитички противници - може намерно да осмислат и реализираат напади или штетен софтвер (malware) за манипулирање со гласањето.

Компјутерски вирус, доколку не го откријат антивирусните мерки на компјутерот од кој се гласа, може да манипулира со гласот на жртвата во корист на партијата што ја фаворизира напаѓачот. Напаѓачите би можеле и да изработат лажна клиент-апликација за гласање, што може да ги измами корисниците да мислат дека уредно гласале, а всушност никогаш не пристапиле до официјалниот систем или не го испратиле својот глас. Доколку некој ваков напад се случи во голем обем, може да ја поткопа валидноста на изборите или целиот изборен систем.

Потенцијалните штетни активности би можеле да вклучуваат спречување на гласачот да го испрати своето ливче, менување на гласачкото ливче, следење како гласа гласачот, искористување

[23] Презентација за наградата за наоѓање пропусти (bug bounty) во Швајцарија; https://www.theverge.com/2019/2/12/18221570/swiss-eelectronic-voting-public-intrusion-test-hacking-white-hack-bug-bounties

на електронските легитимации на гласачот за да добие пристап и да го прошири тој пристап со цел да нанесе штета на изборниот систем, да ги измени изборните резултати, или да наштети на веродостојноста на изборните резултати. Кражба на електронски легитимации, неовластен упад со лажно претставување (phishing) и "социјален инженеринг" се други можни начини за напад врз изборниот систем, иако можеби не би влијаеле врз голем број гласачи.

Службените лица во изборните органи обично имаат овластувања од повисоко ниво да додаваат валидни гласачи во базата на податоци за регистрација на гласачи, да бришат невалидни гласачи, да конфигурираат гласачки ливчиња, да ги дефинираат времето и датумот на гласање, да поставуваат правила за пресметување на изборните резултати и да генерираат извештаи за изборите. Овие чинители би можеле злонамерно да го компромитираат системот или ненамерно да овозможат напад преку заразен компјутер. Автоматизацијата и компјутеризацијата на работата на службените лица во изборните органи треба да бидат придружени со збирка протоколи што би спречиле скриени напади врз системот, соодветни нивоа на профили за најава, лозинки и проверки, како и програми за обука и свесност за ризици по информатичката безбедност.

Систем-администраторите имаат највисоко ниво на овластувања за управување со сервер и други информатички системи за избори. Најчесто тие имаат и физички пристап до опремата и овластени се да инсталираат, конфигурираат и следат различни компоненти на системот за гласање за да обезбедат негово правилно функционирање. Овие лица може намерно или случајно да олеснат напад ако употребат заразени USB мемориски уреди, на пример, или намерно или ненамерно да ја ослабнат заштитата на системите. Во одредени околности, треба да се има предвид можноста од лични закани кон клучниот персонал за информатичка и комуникациска технологија, бидејќи така би можеле да се обезбедат информации што би биле искористени од страна на напаѓачите.

Пауки од Вашингтон, D.C.

Во 2010 година, Одборот за избори на Округот Колумбија (District of Columbia Board of Elections) објави отворена покана кон сите заинтересирани хакери да најдат слабости во пилот-програма за гласање преку интернет наменета за воен персонал и гласачи во странство. Екипа предводени од истражувачи од Универзитетот на Мичиген успеа да упадне во системот за помалку од 36 часа и оствари пристап до сите идентификациски елементи и лозинки за валидните гласачи. Ги сменија сите гласови да одат за непостоечки кандидат без тоа воопшто да биде забележано од администраторите на програмата, и дури успеаја да пристапат до системот за видео надзор на изборната комисија. Низ бројни написи и интервјуа, овој случај предизвика широки јавни дискусии и стана пример за тоа колкави штети може да се нанесат врз веродостојноста на една изборна комисија кога се разоткрива небезбеден информатички систем. Во САД, гласање преку интернет се користи во повеќе од 30 сојузни држави, претежно за воен персонал и гласачи во странство, и покрај предупредувањата и препораките од различни експерти и комисии.

Рамката за информатичка безбедност изготвена од Националниот институт за стандарди и технологија (NIST)[24] нуди неколку препораки за ублажување на овие ризици во однос на овие актери. Овие препораки треба да се примат со претпазливост - не ја елиминираат потребата од темелно моделирање на закани и план за управување со ризици, бидејќи ниту една стратегија за информатичка безбедност не е целосно делотворна. Меѓу другите препораки, NIST препорачува примена на криптографска заштита (при пренос на податоци и за податоци во мирување), напредни техники за криптографско гласање, употреба на наменски и сигурен хардвер (како е-лична карта), безбедносно скенирање на крајната точка (за да се потврди дека софтверски елемент што се користи за гласање не е изменет), околина за стартување на системот што може претходно да се конфигурира или технологија за виртуелизација (тешко применливо за сите уреди на сите гласачи, но може потенцијално да запре штетен софтвер) и секундарни канали за комуникација (како што е QR-кодот што им овозможува на гласачите во Естонија да го проверат својот глас преку друг уред).

Гласање преку интернет со примена на блок-верига (blockchain)

Во изминативе три години се забележуваат напори за промовирање на гласање онлајн. Напоредно со овој наплив комерцијалните компании почнаа да промовираат и примена на блок-верига (blockchain) како "платформа" за пренос на гласовите од личните уреди на гласачите до централна постројка за пребројување/ пресметување, наводно со карактеристики на СП.

Блок-верига претставува еден вид дистрибуирана база на податоци. Обично е во сопственост и управување на неколку независни субјекти што делуваат како содружници (peers). Секој содружник (peer) евидентира нови трансакции, кои криптографски се шифрираат со потпис од претходната трансакција. Блок-веригата според своето устројство е отпорна на измена од страна на еден од содружниците – особина што се нарекува неменливост. На избори со ваква технологија, блок-веригата служи како дистрибуирана гласачка кутија што ги содржи гласачките ливчиња, иако понекогаш содржи и други информации.

Поуки од Германија

Уставниот суд на Германија смета дека секаков вид електронско гласање е противуставно од повеќе причини: од гласачите се бара слепо да веруваат во технологијата, и немаат начин да знаат како компјутерите ги бројат гласовите, а секој електронски или нов систем треба да биде подеднакво разбирлив и употреблив за лаици како системот што го заменува (пенкало и хартија за стандардно гласање). Со тоа во суштина се оневозможува воведување на нов електронски систем на гласање во Германија при сегашното ниво на технологија.

Еден од темелните елементи на блок-веригата е да се потпира врз поголем број содружници (peers). Ако има само еден содружник – изборниот орган – тогаш нема гаранција за неменливост на податоците и придобивката од користењето на блок-верига исчезнува.

[24] The National Institute of Standards and Technology at the request of the U.S. Election Assistance Commission, *The Security Considerations for Remote Electronic UOCAVA Voting*, *2011;* https://www.nist.gov/sites/default/files/documents/itl/vote/NISTIR-7700-feb2011.pdf

За жал, најсериозните слабости кои се заканууваат на интегритетот и тајноста на гласањето се случуваат пред гласовите воопшто да стигнат до блок-веригата.[25] Повеќето од овие решенија не го решаваат проблемот со идентификација/ легитимација на избирачот, на пример. Ова е клучно за веродостојноста на изборите. Естонија, на пример, го реши ова прашање без блок-верига, со примена на електронска лична карта. Освен тоа, безбедноста на уредот од кој гласачите гласаат онлајн е во голема мерка надвор од опсегот на овие системи на блок-верига. Технологијата блок-верига исто така не овозможува заштита од дистрибуиран напад за попречување на опслужувањето (distributed-denial-of-service attack) што ја блокира работата на серверите, не ги заштитува информациите додека патуваат преку интернет, и не ја зајакнува отпорноста на серверите и инфраструктурата кон напредните постојани закани.

Заклучок

Воведувањето на нова технологија, како што е гласање преку интернет, произлегува од потреба да се одговори на определен проблем. Пред да се размислува за далечинско гласање преку интернет, или кое било друго технолошко решение, клучно е изборниот орган најпрвин да ги утврди проблемите во изборниот процес што се обидува да ги ублажи или надминува. Доколку се смета дека со далечинско гласање преку интернет се надминуваат проблеми, тогаш мора внимателно да се обмисли пред да се спроведе. Секако дека новата технологија нуди можности, но недоволна подготовка или внимателност може да нанесе голема штета на јавната доверба и интегритетот на самите избори. Постојат различни начини на вградување на технологија за далечинско гласање, од определување на ограничен сегмент од населението што се соочува со потешкотии при гласањето, до амбициозни обиди за подобрување на излезноста и намалување на трошоците за избори. Далечното гласање преку интернет е една опција; постојат бројни други можности за електронски решенија. Оние што го сметаат гласањето преку интернет за глобално решение треба внимателно да ги проценат потенцијалните влијанија во однос на трошоците, учеството, ефикасноста, довербата и безбедноста.

Овој документ претставува преглед на клучните размислувања од постојната литература истакнати во различни студии на случаи. Целта е да се поттикне понатамошно проучување на оваа тема пред да се носат одлуки, и да се изложи широк дијапазон на прашања и аспекти за разгледување. Овие глобални искуства со себе носат и поуки за претпазливост:

- Политичките и општествените контексти се разликуваат помеѓу државите. Успешно искуство во Естонија не значи дека овој модел ќе прилега на друга земја. Неуспешна пилот-проба во некоја држава, исто така, може долгорочно да ги одврати сопствените чинители од технолошки решенија.

[25] David Jefferson (Verified Voting), *The Myth of "Secure" Blockchain Voting*; https://www.verifiedvoting.org/wpcontent/uploads/2018/10/The-Myth-of-_Secure_-Blockchain-Voting-1002.pdf

- Трошоците се важен фактор. Сите трошоци треба да бидат соодветно пресметани на почетокот на дискусиите за да се утврди дека чинителите целосно ги разбираат критериумите врз кои ги засноваат нивните одлуки.
- Досега нема ниту еден пример во кој гласање преку интернет ја зголемило излезноста на изборите.
- Ќе има потреба од приспособување на законската рамка за да се овозможи примена на нова технологија за гласање. Ова може да има влијание во однос на времето потребно за целосно воведување на технологијата на правно обврзувачки избори.
- Воведувањето технологија не ја зголемува автоматски довербата. Довербата може да се стекне само преку воспоставување соодветни процедури, проверки/ревизија и обезбедување на транспарентност и доволно пристап и информации за чинителите целосно да го разберат редоследот и механизмите на процесот на гласање. Довербата се гради од самиот почеток - ИО мора да обезбеди консултации со надворешни чинители во фазите на пилот-проби и изработка.
- Далечинското гласање може да влијае врз тајноста на гласањето. Без личен надзор врз процесот на гласање од страна на службени лица на избирачките места, на пример, ИО мора да бидат свесни за можностите за надворешни притисоци, купување гласови или злоупотреба, и да преземат соодветни противмерки.
- Безбедноста, како и (еднакво важно) перцепциите за безбедноста, се клучен фактор што треба да бидат водечки теми во дискусиите околу гласањето преку интернет.

Иако има придобивки што државите можат да ги остварат со пилот-проби за гласање преку интернет, особено за одредени групи избирачи како што се лица со попреченост, внатрешно раселени лица, гласачи на окупирани територии или дијаспора, потребно е внимателно да се проценат ризиците. Голем број земји го напуштија гласањето преку интернет - и електронското гласање поопшто - заради безбедносни проблеми и прашања поврзани со довербата на јавноста.

Успешните примери на воведување на вакви технологии покажаа дека треба да се изградат врз силна постоечка инфраструктура што им е позната на граѓаните бидејќи ја користат и за други услуги, како што е примерот во Естонија, наместо целосно нова платформа наменски изработена за гласање преку интернет.

Сите напори за дигитализација на изборниот процес во една држава - вклучително и гласање преку интернет - треба внимателно да се обмислат преку физибилити студија која опфаќа меѓународни истражувања и домашен контекст. Ова е во согласност со европските добри практики и треба да претходи на потенцијални пилот-проби и последователно воведување во поширок обем.

Анекс 1 – Дополнителни ресурси и документација

Клучни ресурси

1. Securing the Vote, Protecting American Democracy by the National Academies of Sciences, Engineering, and Medicine, 2018: https://www.carnegie.org/media/filer_public/34/9d/349d3207d994-4838-8b79-5f8d88e0e412/nas_report.pdf
2. Bruce Schneier essay on Voting Security, 2004: https://www.schneier.com/essays/archives/2004/07/voting_security.html
3. International Foundation for Electoral Systems and National Democratic Institute guide for *Implementing and Overseeing Electronic Voting and Counting Technologies*, 2013: https://www.ndi.org/sites/default/files/Implementing_and_Overseeing_Electronic_Voting_and_Counting_Technologies.pdf

Други важни ресурси и документација

1. Online Voting: Rewards and Risks, Report from The Atlantic Council and McAfee, 2014: https://www.verifiedvoting.org/wpcontent/uploads/2014/10/Online_Voting_Rewards_and_Risks.pdf
2. "Internet Voting: Past, Present and Future," International Foundation for Electoral Systems, Ben Goldsmith, 2013: https://www.ifes.org/news/Internet-voting-past-present-and-future
3. European Parliament Brief, *Digital Technology in Elections: Efficiency Versus Credibility*, 2018, https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625178/EPRS_BRI(2018)625178_EN.pdf
4. *Introducing Electronic Voting: Essential Considerations*, International IDEA, 2011: https://www.idea.int/sites/default/files/publications/introducing-electronic-voting.pdf
5. *Email and Internet Voting: The Overlooked Threat to Election Security*, Susan Greenhalgh - National Election Defense Coalition, Susannah Goodman - Common Cause Education Fund, Paul Rosenzweig, R Street Institute, Jeremy Epstein, ACM US Technology Policy Committee, 2016: https://www.acm.org/binaries/content/assets/public-policy/jtreportemailInternetvoting.pdf 6. *Feasibility Study on Internet Voting for the Central Electoral Commission of the Republic of Moldova*, 2016: https://www.undp.org/content/dam/moldova/docs/Publications/MD-IVOTE-FSand-Roadmap_cleanENG.pdf
7. Hacking the D.C. Internet Voting Pilot, 2010 by J. Alex Halderman, https://jhalderm.com/pub/papers/dcvoting-fc12.pdf, https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-offeronline-voting-but-experts-warn-it-isnt-secure/, https://www.youtube.com/watch?v=tHJlRkwOd4U and https://www.youtube.com/watch?v=G4myYkbtkuk
8. Organization for Security and Co-operation in Europe needs assessment mission report for the November 2019 Federal Assembly elections, providing an analysis of the issues recently identified

and further recommendations and context on internet voting, https://www.osce.org/odihr/elections/switzerland/425009?download=true

9. Evaluation of the e-voting pilot program by the Ministry of Local Government of Norway: https://www.regjeringen.no/en/historical-archive/Stoltenbergs-2nd-Government/Ministry-ofLocal-Government-and-Regiona/tema-og-redaksjonelt-innhold/kampanjesider/e-votetrial/evaluations-of-the-e-voting-trials/evaluation-of-the-e-voting-trials-in-201/summary-of-theisf-report/id685824/
10. International Foundation for Electoral Systems, "International Experience with E-Voting, Norwegian E-Vote Project" by Jordi Barrat i Esteve, Ben Goldsmith and John Turner, 2012: https://www.regjeringen.no/en/historical-archive/Stoltenbergs-2nd-Government/Ministry-ofLocal-Government-and-Regiona/tema-og-redaksjonelt-innhold/kampanjesider/e-votetrial/evaluations-of-the-e-voting-trials/evaluation-of-the-e-voting-trials-in-201/id684642/

Анекс 2 – Држави што применуваат гласање преку интернет (гласање преку интернет надвор од избирачки места во политички обврзувачки избори)

Во целата држава	Во некои делови од државата или за одредени категории гласачи	Се планира пробно гласање, или направено е пробно гласање и со тоа е запрено, или никогаш не е применето
Естонија е единствената држава што на сите граѓани им нуди можност да гласаат преку интернет на локални, државни и европски избори.	**Ерменија**: Дипломатскиот персонал и членовите на нивните семејства може да гласаат онлајн.	**Франција**: Применето за гласачи што престојуваат во странство на парламентарните избори во 2012 година, но запрено во 2017 година поради безбедност; владата планира повторно да го воведе во 2022 година. Лицата што престојуваат во странство исто така гласаа преку интернет на внатрепартиските избори во Републиканската партија во 2016 година.
	Австралија: пробно гласање преку интернет се понуди за воениот персонал надвор од земјата во 2017 година, но не продолжи понатаму. Нов Јужен Велс им овозможува на некои групи - гласачи со посебни потреби, жители на оддалечени подрачја, надвор од сојузната држава - да гласаат преку интернет, но нема планови оваа опција да се прошири во други сојузни држави.	**Индија**: Во 2010 година се спроведе пробно гласање преку интернет за локални избори во сојузната држава Гуџарат.
	Канада: гласање преку интернет е можно за локални избори во некои изборни единици во Онтарио и Нова Шкотска. Канада разгледуваше можност да воведе гласање преку интернет на федералните избори.	**Норвешка:** можност за гласање преку интернет се понуди за локалните избори во 2011 и државните избори во 2013 година во некои изборни единици. Во 2014 година можноста за гласање преку интернет беше укината поради безбедносни причини.

	Мексико: Некои сојузни држави дозволуваат гласање преку интернет за гласачи што се наоѓаат во странство.	Во 2004 година **Холандија** реализираше гласање преку интернет за водостопанскиот одбор *Rijnland* и во 2006 за гласачи во странство на државните избори. Гласањето преку интернет престана во 2017 година поради безбедноста.
	Нов Зеланд: Гласачите во странство може да гласаат онлајн.	**Шпанија**: Во 2010 година Барселона одржа онлајн референдум за проект за
		урбан развој. Гласањето беше еднократна пилот-проба само на интернет, многу контроверзна.[26]
	Панама: Гласачите во странство може да гласаат онлајн.	**Обединето Кралство**: Пробно гласање онлајн се реализира на локални избори меѓу 2002 и 2007 година.
	Швајцарија: Некои кантони нудат гласање преку интернет на гласачите во странство - во неколку случаи и на локално присутните гласачи - на избори и референдуми. Декларирана цел е да се воведе гласање преку интернет за целата земја.	**Русија** се подготвува да го воведе својот прв систем за гласање преку интернет. Системот ќе се тестира во московски кварт од кој ќе се избере еден член на градскиот совет за главниот град во септември 2019 г. Еден од првите експерименти со воведување на гласање преку интернет го реализираше Изборната комисија на Волгоградскиот регион за избори во Урјупинск во 2009 година, и во округот Одинцово во 2010г.

[26] Градот Барселона во Шпанија наиде на проблеми во делот на идентификација на гласачите и кражба на идентитет, со пример на позната личност што откри дека некој друг веќе се најавил во системот со неговите елементи за автентикација и гласал наместо него;
https://www.regjeringen.no/globalassets/upload/krd/prosjekter/evalg/evaluering/topic6_assessment.pdf

	САД: И покрај загриженоста изразена по хакерскиот упад во пробното гласање преку интернет во Округот Колумбија, повеќе од 30 сојузни држави во САД овозможуваат воен персонал и лица што престојуваат во странство да гласаат онлајн. Гласачите што користат онлајн или гласање по пошта се откажуваат од правото на тајност на гласањето.	**Финска** назначи работна група за проучување на техничката изводливост на систем за гласање преку интернет. Утврди дека технологијата сè уште не ги исполнува доволно сите услови, наведувајќи проблеми со компромисот меѓу проверливоста и тајноста на гласањето

Извор: http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625178/EPRS_BRI(2018)625178_EN.pdf

За авторите

Meredith Applegate, Програмски советник на IFES – Украина

Meredith Applegate е програмски советник за IFES во Украина со повеќе од 10 години искуство во развој, управување и спроведување на програми за избори и демократија во централната канцеларија и на терен. Особено се фокусира кон родовата еднаквост, застапувањето и развојот на граѓанското општество, едукација на гласачите и граѓаните и правата на лицата со попреченост. Applegate била назначувана на долгорочни функции во Индонезија, Мјанмар и Украина. Исто така работела и на краткорочни до среднорочни задачи за изборни активности, едукација на гласачите и граѓаните и ставање крај на насилствата врз жените на избори, вклучително и ангажмани за Субјектот на ООН за родова еднаквост и зајакнување на жените во Сиера Леоне, Програмата на Обединетите нации за развој во Молдавија, и програмите на IFES во Камбоџа, Доминиканска Република, Непал и Источен Тимор.

Vladlen Basysty, Раководител за технологија и информатичка безбедност во IFES – Украина

Vladlen Basysty раководител за технологија и информатичка безбедност во IFES – Украина. Basysty има 16-годишно искуство во управување со проекти за информатичка технологија со организации меѓу кои Меѓународната организација за миграции, CGI Federal, Амбасадата на САД во Украина, Бирото на Министерството за домашна безбедност на САД, Федералниот центар за обука за полициски службеници, проектот на Институтот Џон Сноу и Американската агенција за меѓународен развој “СИДА Фондација Исток-Запад” и Мировниот корпус на САД во Украина.

Thomas Chanussot, Виш експерт за технологија и информатичка безбедност

Thomas Chanussot работи во областа на изборите од 2004г. Со претходно искуство во информатичката технологија, учествувал во повеќе од 12 изборни активности ширум светот, особено во областа технологија за управување со избирачки списоци и изборни резултати, каде работел во различни улоги вклучително и развој на системи, ревизорски проверки на безбедноста и раководење на тим. Има опсежно работно искуство на критична изборна инфраструктура, проектирање и безбедност на биометриски и небиометриски бази на податоци за избирачки списоци, како и системи за управување со резултати. Сега управува со неколку иницијативи за критична информатичка безбедност на изборни процеси во Азија и Источна Европа, и во IFES води оценки на информатичка безбедност.

Global Expertise. Local Solutions.
Sustainable Democracy.

IFES | 2011 Crystal Drive | 10th Floor | Arlington, VA 22202 | www.IFES.org