

You have downloaded a document from



The Central and Eastern European Online Library

The joined archive of hundreds of Central-, East- and South-East-European publishers, research institutes, and various content providers

Source: Politologica. Acta Universitatis Palackianae Olomucensis
Politologica. Acta Universitatis Palackianae Olomucensis

Location: Czech Republic

Author(s): Sylvie Reterová

Title: Alternativní formy hlasování z hlediska práva a bezpečnosti
Security and Legal Principles of Alternative Voting Methods

Issue: 6/2008

Citation style: Sylvie Reterová. "Alternativní formy hlasování z hlediska práva a bezpečnosti". Politologica. Acta Universitatis Palackianae Olomucensis 6:47-59.
<https://www.ceeol.com/search/article-detail?id=93368>

ALTERNATIVNÍ FORMY HLASOVÁNÍ Z HLEDISKA PRÁVA A BEZPEČNOSTI

Sylvie Reterová

SECURITY AND LEGAL PRINCIPLES OF ALTERNATIVE VOTING METHODS

ABSTRACT: This paper examines the issue of alternative voting methods – internet voting, telephone voting, postal voting and mail vote. The purpose is to provide the analysis of security and legal principles of election, which has to be fulfilled to the same extent as in case of traditional voting methods. The ensurance of these principles is necessary for democratic state functioning. Generally, the accent is put on voting procedures which are user-friendly and trustworthy at the same time.

KEYWORDS: Alternative Voting Methods, Electronic Voting, Internet Voting, Mail Vote, Postal Voting, On-line Voting, Telephone Voting

Úvod

Jak z názvu vyplývá, tento článek se soustředí na bezpečnostní a právní principy tzv. alternativních forem hlasování,¹ což je souhrnné označení pro netradiční způsoby výběru kandidátů ve volbách. Konkrétně se jedná o korespondenční hlasování, telefonní hlasování (s využitím pevné linky i mobilního telefonu), hlasování prostřednictvím digitální televize a internetové hlasování rozšířené také pod názvem elektronické volby nebo on-line volby. Tradiční volební postup spočívající ve vzhazování tištěných hlasovacích lístků do volebních urn totiž zdaleka nepředstavuje jedinou možnou cestu, jak určovat složení zastupitelského sboru, a mnoho demokratických států považuje používání této klasické metody ve 21. století spíše za překonané. V současné době jsou proto v popředí

¹ V textu používám pro alternativní formy hlasování synonymně také jiné přívlastky, jedná se o výrazy „inovativní“, „progresivní“, „moderní“, „nové“ nebo „pokrokové“ formy hlasování.

zájmu politologů, právníků a počítačových specialistů nové progresivní metody hlasování, jejichž rozšíření úzce souvisí s vývojem moderních komunikačních technologií. Vzhledem k tomu, že použití takových alternativních postupů není vázáno na konkrétní místo, není nikdo předem vyloučen z volebního procesu a hlasování je pohodlné, přístupné, rychlé a snadné. Výsledky jsou navíc známy okamžitě po skončení voleb a nemusíme se ani obávat chyb či omylů při jejich vyhodnocování. Teprve taková volební úprava je relevantním odrazem společenských podmínek ve 3. tisíciletí.

Faktem nicméně zůstává, že navzdory obrovskému technickému rozvoji v posledních letech je celosvětově nejrozšířenější formou volba pomocí jednotných kandidátních listin. Tedy procedura, která se od roku 1858, kdy byl poprvé použit papírový volební lístek, téměř nezměnila. Většina občanů je tak i nadále odkázána na tradiční prostředky hlasování – tužku a papír. Hlavním důvodem uvedené stagnace jsou právě bezpečnostní a právní úskalí, jež se mohou v souvislosti s prosazením volebních alternativ objevit. Největší obavy přitom vyvolává otázka, jak zajistit ochranu identity voliče a zároveň zabezpečit systém před vnějším zneužitím. V následujícím textu se proto zaměřím na analýzu nejčastějších sporných bodů a poté posoudím oprávněnost těchto obav.

Pohodlnost versus bezpečnost hlasování

Pohodlnost, respektive jednoduchost hlasovací procedury daná nezávislostí volebního úkonu na čase a místě, je stěžejním důvodem ukotvení nových alternativ v právních rádech jednotlivých států. Z legislativního hlediska je tím umožněn výkon hlasovacího práva nejen občanům žijícím v zahraničí, ale i všem voličům, kteří se ve stanovené dny nacházejí mimo příslušný okrsek nebo se nemohou osobně dostavit do volební místnosti. Přístupnost, pohodlnost a komfort hlasujících tak patří mezi nejvíce skloňované termíny zdůrazňované prakticky ve všech odborných i politických diskusích na toto téma. Stejně pozornosti se ovšem dostává také problematice bezpečnosti hlasování, jež tvoří základ většiny studií, úvah či rozhovorů analyzujících moderní způsoby výběru kandidátů do veřejných funkcí. Zde jsou klíčovými požadavky důsledná ochrana a zajištění systému po stránce organizačně-procesní i bezpečnostně-právní. Zásadní a dosud ne zcela přesvědčivě zodpovězenou otázkou přitom zůstává, jak propojit tyto dva aspekty a zároveň zachovat přednosti obou z nich, tedy snadnost hlasování a vysoký stupeň zabezpečení. Jinými slovy, zda lze zjednodušit volební proces a současně udržet stejnou míru důvěryhodnosti a spolehlivosti hlasování jako v případě tradičních postupů.² Před tím, než se pokusíme najít požadovaný kompromis, je třeba objasnit nejdůležitější bezpečnostní principy, jež musí být při hlasování garantovány.

Naplnění technických požadavků nutných pro realizaci alternativních volebních metod není jednoduché. Při vzdáleném hlasování, kdy občané nejsou v kontaktu se

² PRATCHETT, Lawrence a kol.: *Balancing security and simplicity in e-voting. Towards an effective compromise?* In: *The European Union and e-Voting. Addressing the European Parliament's internet voting challenge*. Sestavil Alexander H. Trechsel a Fernando Mendez. Londýn, New York 2005, s. 166–167.

členy volební komise, nelze zajistit bezprostřední kontrolu nad řádným průběhem voleb a vzhledem k vyloučení přímého dohledu úředníků je také velmi těžké zaručit nestranný, tajný, soukromý a demokratický výkon hlasovacího práva. Z hlediska bezpečnosti je důraz kladen na předcházení možnému systémovému zneužití ve všech čtyřech fázích volebního procesu, tedy při registraci, identifikaci, odevzdávání i počítání hlasů. V případě elektronických voleb je navíc nezbytné zamezit manipulacím během přenosu dat, vyhodnocování volebních výsledků a uchovávání konečných údajů pro eventuální přezkoumání. Technicky nejsložitější je pak situace u internetového hlasování, kterého se účastní nejvíce subjektů a každý z nich vyžaduje vysokou míru zabezpečení. Pokud posoudíme on-line volby komplexně, je třeba ochránit nejen voliče, počítače (hardwary) a programová vybavení (softwary), ale také internetová připojení uživatele k poskytovateli, propojení webového serveru s tímto poskytovatelem a konečně i hlasovací servery včetně uživatelského rozhraní a jiných aplikačních systémů.³ Je tedy zřejmé, že pro uplatnění inovativních metod musíme dodržet celou řadu bezpečnostních kritérií, která jsou nutná pro úspěšné fungování nastiněného mechanismu.

Obecně již taková kritéria existují a pořadatelé voleb se mohou při realizaci alternativních hlasovacích forem opřít o detailně vypracovaný teoretický koncept. Jeho součástí je seznam podmínek vytvářejících rámec pro právně, organizačně i procesně bezpečné volby, jež v praxi garantují veškeré zákonné atributy pro hlasování. Technické předpoklady pro uskutečnění popisovaných standardů přitom moderní demokracie splňují již několik let, a sice v podobě elektronického podpisu, jehož základní vlastností je nepopíratelnost.⁴ Uvedený návrh obsahuje podrobný popis deseti požadavků, z nichž prvním je důsledné zachování zásady, podle níž smí hlasovat pouze oprávněný volič. Stěžejní je zde zejména postup, jakým k identifikaci dochází, a v zásadě rozlišujeme čtyři způsoby vyznačující se různým stupněm zabezpečení. Nejjednodušší je ověření voliče prostřednictvím elektronického identifikátoru nebo zaručeného elektronického podpisu a jednotného registru obyvatel. Stejně jako u ostatních internetových služeb (například on-line bankovníctví) se volič při registraci autorizuje pomocí PIN kódu a čipové karty, jejíž data slouží k potvrzení totožnosti. Počítačový program provedenou verifikaci porovná s databází osobních dokladů a pokud vše odpovídá, запиše občana k volbám.⁵

Na opačném konci stojí fyzická registrace probíhající osobně a v dostatečném předstihu před vlastní volbou. Na jedné straně zajišťuje tato úprava větší míru jistoty a důvěryhodnosti systému, na straně druhé však výrazně omezuje výhodu vyššího pohodlí občanů. Zde je tedy dobře patrný onen rozpor mezi bezpečností a přístupností hlasovací

³ BURMESTER, Mike – MAGKOS, Emmanouil: *Towards Secure and Practical E-elections in the New Era*. In: *Secure Electronic Voting*. Sestavil Dimitris A. Gritzalis. Boston, Dordrecht, Londýn 2003, s. 63–65. ZÁLEŠÁK, Michal – MATEJKA, Ján: *Nové možnosti (e)demokracie*.

<http://park.logos.cz/article.asp?itm=203&ShowNoScriptVersion=True> (30. 1. 2007)

⁴ Princip nepopíratelnosti spočívá v tom, že nelze popřít využití elektronického podpisu daným občanem. Česká republika přistoupila na tuto možnost v roce 2000 na základě Zákona č. 227/2000 Sb., o elektronickém podpisu. *Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů*.

⁵ ŠINDELÁŘ, Petr: *Elektronické volby jako možný nástroj pro posílení demokracie*. System Integration 2006, s. 241–242. si.vse.cz/archiv/clanky/2006/sindelar.pdf (10. 2. 2007)

procedury, kdy se zvýšená ochrana poskytuje na úkor snížené pohodlnosti. Volič má povinnost dostavit se na příslušný úřad veřejné správy, kde je po fyzické kontrole identity zapsán k hlasovacímu procesu a současně je mu vygenerován kód pro elektronickou volbu. Jestliže musí občan iniciovat poslední krok potvrzující jeho oprávněnost volit sám, jedná se o tzv. on-line registraci, kterou dále dělíme na registraci s fyzickým předáním identifikátoru a registraci s elektronickým předáním identifikátoru. V prvním případě je občanům po ověření jejich identity na serveru registrační služby doručeno potvrzení spolu s kódem poštou, při druhé možnosti je voličům tento identifikátor zaslán elektronicky například formou SMS zprávy do mobilního telefonu. Pozitivem dvou posledně jmenovaných postupů je jednak eliminace nutnosti fyzické přítomnosti na příslušných úřadech a jednak prodloužená lhůta pro registraci. Z hlediska státního zájmu je jistě příznivá i redukce nákladů na poštovné.⁶

Pokud se vrátíme zpět k seznamu podmínek, které musí být při prosazování alternativních modelů respektovány, je třeba zdůraznit, že se jejich vymezení nijak neliší od nároků kladených na klasické volební metody. Z toho vyplývá, že inovativní techniky nabízejí srovnatelnou míru bezpečnosti a spolehlivosti jako tradiční systémy hlasování. Vzhledem k tomu, že zbývající standardy jsou převážně právního charakteru, budou podobněji zkoumány v následující části textu a na tomto místě uvádím pouze jejich taxativní výčet. Druhým kritériem je pravidlo, podle něhož každý volič disponuje jedním a pouze jedním hlasem a není tedy možné, aby přípustnost několika volebních alternativ zakládala oprávnění hlasovat vícekrát. Každý volič je dále chráněn před zneužitím osobních údajů, což je garantováno tajným, soukromým a anonymním výkonem hlasovacího práva. Významným principem je také požadavek správnosti, úplnosti a ověřitelnosti sčítacího procesu, přičemž možnost kontroly má po skončení hlasování i samotný volič. Celý proces musí být dále odolný vůči chybám, a to včetně chyb náhodných, a nikdo nesmí duplikovat či jinak manipulovat cizí hlasy. Tento atribut je promítnut do všeobecné zásady, podle níž obsah volby nesmí být modifikovatelný či odposlechnutelný. Systém také nesmí přijímat hlasy mimo zákonem stanovený čas voleb a konečně posledním kritériem je zákaz zveřejňování průběžných volebních výsledků, a to i v případě, že korespondenční a elektronické hlasování trvá několik týdnů.⁷

Vedle naplnění těchto obecných standardů je pro aplikaci elektronických voleb rozhodující též technické zabezpečení hlasování, jehož náročnost bývá v praxi nejčastější příčinou oddalování realizace i-voleb. Odborníci v této souvislosti upozorňují na riziko výskytu softwarových selhání a především počítačových virů, s nimiž má zkušenosti takřka každý uživatel internetu. Velmi obávané jsou ty, které se aktivují k určitému datu a v den voleb ochromí nemalé procento počítačů. Viry přitom mohou být šířeny buď jednorázově na vybrané e-mailové adresy určité skupiny obyvatel, nebo hromadně s cílem

⁶ ALVAREZ, Michael, R. - HALL, Thad, E.: *Point, Click, and Vote. The Future of Internet Voting*. Washington 2004, s. 95-96. ŠINDELÁŘ, P.: *c. d.*, s. 242-243.

⁷ ZIMMERMANN, Frank: *Anonymous code lists for secure electronic voting over insecure mobile channels*. 2003. Citováno podle: ŠINDELÁŘ: *c. d.*, s. 241-242. RADWIN, Michael, J.: *An untraceable, universally verifiable voting scheme*. 1995, s. 1-3. <http://www.radwin.org/michael/projects/voting.html> (8. 3. 2007)

zasáhnout co největší počet hlasujících. Aktivují se zpravidla přečtením elektronické zprávy, popřípadě přiloženého souboru, nebo již otevřením e-mailové schránky. Obtížněji odhalitelnou formou je pak aktivace viru návštěvou některých internetových stránek, při jejichž otevření se spustí nežádoucí proces. V neposlední řadě mohou být virem napadeny také oblíbené soubory. Negativním dopadům způsobeným těmito útoky však lze účinně zabránit, ať už speciálními antivirovými programy, jejichž obsah není předem znám, nebo intenzivní osvětou informující voliče o tom, jak postupovat při obdržení viru.⁸

Vážným nebezpečím při provádění elektronických voleb jsou dále individuální pokusy hackerů, jež usilují o nezákonné proniknutí do hlasovacího programu, nebo závažné systémové útoky financované prakticky kýmkoliv. Ke zneužití přitom může dojít již v samotném počítači u voliče, tedy ještě předtím, než se jedinec připojí na webovou stránku hlasovacího serveru. „V současné době existuje několik programů, jejichž prostřednictvím lze spravovat a ovládat vybraný počítač připojený k síti v podstatě stejně, jako kdyby útočník seděl u dotyčného počítače.“⁹ Tímto způsobem lze tedy snadno hlasovat za daného občana či jinak na dálku manipulovat jeho rozhodnutí. Z technického hlediska sice zatím nejsou softwarová vybavení na takové úrovni, aby tyto pokusy zcela vyloučila, nicméně jejich správným nainstalováním je možné eliminovat negativní dopady na minimum. Pro specialisty v oboru počítačových technologií rovněž není problém útoky zpětně odhalit a viníky potrestat.¹⁰

V souvislosti s dostupností oficiálního volebního serveru se další riziko vyskytuje v podobě tzv. DDoS útoků (distributed denial of service attacks), jejichž záměrem je vyvolat přetížení hlasovacího programu. Konkrétní postup spočívá ve vysílání množství požadavků v jednom okamžiku s úmyslem způsobit neúnosnou zátěž, čímž dojde nejprve k omezení a následně i úplnému selhání mechanismu. Voličům v takovém případě není umožněno připojit se k požadované internetové stránce a odevzdat elektronicky svůj hlas. I přes vysokou výkonnost počítačového serveru trvá vždy několik hodin, než se program opět podaří zprovoznit, přičemž v průběhu této opravy nelze přijímat žádosti občanů o volbu. V praxi jsou popisované snahy hackerů poměrně běžnou záležitostí, ovšem ne vždy k zamýšlenému selhání dojde. Případů dokončených útoků je nicméně mnoho, což lze deklarovat například americkou studií z roku 2001, v níž se zjistilo, že v průběhu pouhých tří týdnů bylo takto ohroženo 10 tisíc počítačů.¹¹ V současné době ještě nelze DDoS útokům zcela předcházet, avšak vzhledem k technicky vyšší kvalitě počítačových serverů by k systémovému přetížení bylo zapotřebí vyvinout enormní úsilí.

Z uvedeného vyplývá, že alternativní volbu je nutné důkladně promyslet a státy by neměly její realizaci uspěchat. Na druhou stranu ale již dnes existuje pro většinu zmíněných problémů řešení a důkazem je nemálo úspěšně provedených pilotních projektů

⁸ RUBIN, Aviel, D.: *Security Considerations for Remote Electronic Voting over the Internet*. New Jersey 2001. <http://avirubin.com/e-voting.security.htm> (8. 3. 2007). ZÁLEŠÁK, M. - MATEJKA, J.: c. d.

⁹ ZÁLEŠÁK, M. - MATEJKA, J.: c. d.

¹⁰ JEFFERSON, David a kol.: *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*. 2004, s. 12–18. www.servesecurityreport.org/paper.pdf (8. 3. 2007)

¹¹ Příkladem, kdy k uvedenému útoku došlo v průběhu hlasování, jsou kanadské on-line volby v roce 2003. Zde byl systém napaden přímo v den oficiálního konání voleb. JEFFERSON, D. a kol.: c. d., s. 18.

v čele s estonským hlasováním z března 2007. Z pohledu uživatele a volebního serveru jsou nejbezpečnější elektronické čipové karty, jejichž zavedení není pro vyspělé státy nijak obtížné. Karta spolu se speciální čtečkou zaručí, že hlasující subjekt je u počítače opravdu přítomen a nikdo jiný tedy nemůže z jiného místa vykonat neoprávněnou volbu. Programová selhání a počítačové viry lze pak vyloučit pomocí nejmodernější zabezpečovací technologie, což se velmi dobře podařilo například ve Švýcarsku (elektronické volby se zde konají od roku 2003). Ve spojitosti s technickým pokrokem lze v budoucnu navíc očekávat aplikaci nových nezpochybnitelných metod, mezi něž patří jednak biometrické techniky měřící fyziologickou charakteristiku dané osoby (otisky prstů, snímání duhovky, geometrie cév apod.) a dále behaviorálně založené techniky, jež mohou být uplatněny mimo jiné při ověřování podpisů (měří se dynamika podpisu či síla úderů do klávesnice).¹²

Kvalitní zabezpečení hlasovacího systému však není spjata pouze s těmito pro nás vzdálenými technologiemi. Hlasovat bezpečně a zároveň pokrokově lze již dnes a přesvědčit se o tom mohli občané řady států, jejichž právní systém ukotvuje institut alternativní volby. Hledaný kompromis mezi snadností a důvěryhodností hlasování můžeme spatřovat například v legislativní a praktické úpravě Estonska (úspěšné internetové volby proběhly v roce 2007) a Švýcarska, kde bezproblémový průběh voleb vyvrátil domněnky mnoha odpůrců inovativních způsobů hlasování. Pokud tedy zvažujeme, zda umožnit výkon volebního práva milionům potenciálních voličů nebo podlehnout obavám z případného selhání či zneužití systému, měli bychom se přiklonit k alternativě první. V praxi se totiž jasně ukázalo, že nezbytnou ochranu ve volbách zajistit lze, kdežto zpřístupnit hlasovací proces všem voličům s tradičními postupy nelze.

Ne/soulad alternativních voleb se základními hlasovacími principy

S vyřešením bezpečnostních problémů však obavy části odborné veřejnosti nekončí. Možná úskalí totiž nespočívají pouze v technickém a organizačním ukotvení hlasovací procedury, ale mohou se dotýkat i samotné podstaty demokratického uspořádání země. Podkladem pro toto tvrzení je skutečnost, podle níž volby (a referenda) jsou pro občany v zastupitelských demokraciích prakticky jedinou příležitostí, jak se jednorázově podílet na politickém rozhodování, a pokud by došlo k úpravě tohoto způsobu participace, mohlo by to ovlivnit vlastní fungování státu. Případnou změnu volebních pravidel směrem k umožnění alternativního hlasování je tedy nutné velmi dobře zvážit, a to jak z pohledu vnitrostátních právních předpisů, tak z hlediska souladu s mezinárodními normami. Zásady pro hlasování jsou promítnuty v ústavách všech vyspělých zemí a rovněž v řadě nadnárodních ustanovení, která zahrnují volební právo mezi základní politická práva. V Evropě se jedná zejména o Úmluvu o ochraně lidských práv a základních svobod

¹² ZÁLEŠÁK, M. - MATEJKA, J.: c. d. DICTSON, Derek - RAY, Dan: *The Modern Democratic Revolution: An Objective Survey of Internet-Based Elections*. White Paper, The Internet Voting Portal, 2000, s. 9. www.SecurePoll.com (10. 2. 2007)

schválenou v roce 1950 na půdě Rady Evropy, celosvětovou konvencí je pak Všeobecná deklarace lidských práv přijatá Valným shromážděním Organizace spojených národů v roce 1948.¹³

Obecně je demokratičnost voleb založena na čtyřech zásadních principech – všeobecnosti, přímosti, rovnosti a tajnosti hlasování, přičemž jejich existence musí být zachována kumulativně, a nelze tedy omezit nebo dokonce vyloučit byť jen jedno z nich. Při nahrazení tradičních volebních forem inovativními technikami jsou přitom ohrožena všechna uvedená práva a dle mínění některých vědců by proto nové volební postupy neměly vystřídat, nýbrž pouze doplnit ty současné. V takovém případě by digitální a elektronické hlasování tvořilo pouze doplněk ke klasické volbě a pokud by lidé neměli důvěru k moderním mechanismům, odevzdali by svůj hlas prostřednictvím tištěného volebního lístku. Druhá skupina specialistů nicméně tvrdí, že k takovému rozhodování nebudou mít voliči důvod, jelikož alternativní volby nejenže zaručují srovnatelnou míru právní jistoty, ale zároveň poskytují množství výhod, kterými vysoce převyšují kvalitu tradičních hlasovacích systémů.¹⁴ Pro posouzení oprávněnosti obou názorů věnuji následující text těm právním otázkám, které v souvislosti s alternativní volbou vyvolávají největší rozpory. V tabulce č. 1 nejprve uvádím jejich přehled a poté zhodnotím, zda odporují ústavně zakotveným principům či nikoliv.

Tabulka č. 1: Ohrožení základních hlasovacích práv při zavedení alternativní volby

Ústavní principy hlasování	Problémy vyskytující se při alternativním hlasování (podle odpůrců)
všeobecnost	digitální propast (ne každý má přístup a schopnosti používat technologie)
rovnost	<p>dvouj volba (více hlasovacích způsobů umožňuje odevzdat více hlasů)</p> <p>porušení rovnosti hlasujících (elektroničtí voliči jsou zvýhodněni oproti tradičním, jelikož mohou hlasovat vícekrát)</p>
tajnost	<p>volba není tajná (nehlasuje se za plentou)</p> <p>volba není anonymní (lze zjistit, jak kdo hlasoval)</p> <p>volba je ovlivnitelná (možnost nátlaku)</p>
přímost	volba není přímá (hlasuje se prostřednictvím pošty, telefonu, TV, internetu)

Zdroj: autorka

Klíčovým předpokladem demokratického volebního procesu je dodržení zásady všeobecného hlasování, podle níž má každý člověk právo volit, a tím se nepřímo podílet na politickém řízení společnosti. Toto oprávnění se vztahuje na každého dospělého občana bez rozdílu věku, pohlaví, rasy, národnosti, původu nebo přesvědčení a žádná skupina obyvatel tedy nesmí být pozitivně či negativně diskriminována. S realizací elektronického hlasování však vyvstává otázka, jak zajistit všeobecný přístup voličů k informačním

¹³ KLÍMA, Michal: *Volby a politické strany v moderních demokraciích*. Praha 2003, s. 184.

¹⁴ MITROU, Lilian - GRITZALIS, Dimitris - KATSIKAS, Sokratis: Revising legal and regulatory requirements for secure e-voting. http://www.instore.gr/evote/evote_end/htm/3public/doc3/public/evote_paper_SEC_2002_2.doc (5. 2. 2007)

technologiím a zároveň jak rozšířit počítačové dovednosti na všechny věkové kategorie. Rozdíl mezi těmi, kteří moderní komunikační prostředky používají, a těmi, kteří s nimi nemají žádnou zkušenost, se nazývá digitální propast, postihující nejvíce starší vrstvy obyvatel, občany s nižším stupněm dosaženého vzdělání nebo nízkými příjmy. Při zavedení univerzálního alternativního hlasování by tak značná část voličů byla omezena ve výkonu svého práva, což by znamenalo takové porušení základního ústavního principu, které nelze v demokratickém státě akceptovat.¹⁵

V současné době vykazují nejvyšší počet obyvatel s počítačovými znalostmi a připojením k internetu skandinávské země a Nizozemsko, nicméně ani zde se problém digitální propasti nepodařilo zcela překonat a zákonodárci nemohli k ukotvení moderních hlasovacích způsobů přistoupit. Případná stížnost u Evropského soudu pro lidská práva by totiž s největší pravděpodobností byla shledána oprávněnou.¹⁶ Pro tuto chvíli lze tedy konstatovat, že dokud bude společnost rozdělená na ty, kteří schopnostmi a přístupem k nejmodernějším technologiím disponují a na ty, kteří tyto možnosti ani dovednosti nemají, nemůžeme přikročit k uzákonění elektronických voleb na všeobecné úrovni. Nic však nebrání jejich integraci do stávajícího právního řádu, kde by tvořily alternativu k tradičním, popřípadě korespondenčním volbám, jež požadavek všeobecnosti splňují. Taková legislativní úprava by vyhovovala jak občanům preferujícím klasické hlasovací lístky, tak těm, kteří se z pracovních či osobních důvodů nemohou do volebních místností dostavit.

Druhým kritériem demokratičnosti voleb je garance rovného hlasovacího práva, kde rovnost vyjadřuje především tu skutečnost, že každý občan má pouze jeden hlas se stejnou hodnotou. Tato zásada se obecně týká i rovnoprávného postavení politických stran a jiných kandidujících subjektů, na které však prosazení progresivních metod nemá žádný vliv.¹⁷ Rovněž při teoretické neexistenci digitální propasti by inovativní postupy nezpůsobily porušení pravidla rovnosti hlasujících, jelikož by všichni občané měli stejný přístup k volební proceduře. Rozpor ovšem nastává v případě, kdy je zákonem povoleno využití více hlasovacích technik a současně připuštěna možnost opakovaného výkonu volebního práva. Na jedné straně taková úprava eliminuje vynucené či podvodné hlasování, na straně druhé ale zvýhodňuje elektronické voliče, kteří mohou, narozdíl od tradičních voličů, odevzdat (ve smyslu opravit) svůj hlas několikrát.

Vzhledem k tomu, že je posledně jmenovaná varianta předpokládaným řešením pro většinu zemí, je nutné stanovit přesné priority pro posuzování platnosti hlasů, přičemž musí být zřejmé, jaký hlas je při opakovaném provedení závazný. Systém musí spolehlivě rozpoznat, zda volič nehlasoval oběma způsoby, a případnou duplicitní volbu odstranit. „Toto rozpoznání může být buď synchronní (i-volby a papírové volby probíhají souběžně), nebo asynchronní (papírové volby začínají v okamžiku ukončení i-voleb).“¹⁸ Obvykle je

¹⁵ ALVAREZ, M. R.: *c. d.*, s. 48–53. MITROU, L.: *c. d.*

¹⁶ Tento závěr mimo jiné vyplývá z odborné studie právních expertů britské univerzity v Leicesteru, kteří problematiku alternativních forem hlasování zkoumali podrobně. ZÁLEŠÁK, M. – MATEJKA, J.: *c. d.*

¹⁷ MITROU, L.: *c. d.*

¹⁸ ŠINDELÁŘ, P.: *c. d.*, s. 243.

příznán klasické volbě v porovnání s elektronickými hlasy větší stupeň závaznosti, jelikož lístek odevzdaný tradiční cestou již nemůžeme po jeho vhození do volební urny opravit, a tím zneplatnit. V zákoně lze tento aspekt upravit například elektronizací seznamu voličů ve volebních místnostech nebo ukotvením povinnosti hlasovat alternativně pro ty občany, kteří se pro takovou volbu předem zaregistrují. V prvním případě by volební komisaři zaznamenali do elektronického seznamu každého občana, který by se rozhodl hlasovat prostřednictvím papírových kandidátních listin, čímž by se automaticky zamezil jeho přístup k digitálnímu a internetovému hlasování. U druhé eventuality by pak záleželo na způsobu provedení registrace, na jejímž základě by se voliči rozdělili do dvou skupin bez možnosti pozdějšího přechodu.¹⁹ Výsledkem obou těchto legislativních úprav je jednak odstranění duplicitní volby a jednak spolehlivé zajištění rovného hlasovacího práva, kdy každý volič disponuje jedním hlasem se stejnou váhou.

Ve spojitosti s rovností hlasů je nezbytným předpokladem také tajnost při jejich odevzdávání, což znamená, že nesmí být zjistitelné, jak kdo hlasoval. Rozhodující je přitom vytvoření podmínek pro svobodný a anonymní výkon volebního práva, jakož i dodržení pravidla nezveřejňovat výsledky hlasování před zahájením sčítacího procesu z důvodu potenciálního ovlivňování voličů. Odpůrci alternativních metod však moderní hlasovací postupy spojují spíše s termíny, jako jsou „veřejná volba“, „manipulace s hlasy“ nebo „nedostatečné zaručení soukromí“, a poukazují rovněž na špatné zabezpečení ochrany voličů. Jejich argumenty se opírají o zjevnou skutečnost, že k vlastnímu úkonu hlasování nedochází za plentou ve volebních místnostech, nýbrž na jakémkoliv veřejně přístupném místě, kde je umístěn počítač s připojením na internet. Zdůrazňují také, že při elektronické formě nelze zcela oddělit identitu voliče od samotného obsahu hlasování a není tak zachována požadovaná anonymita.²⁰ Taková tvrzení ale nemůžeme vzhledem k dalším informacím a zkušenostem jednotlivých zemí považovat za opodstatněná. Fakt, že k odevzdání hlasu nedochází za plentou, ještě neznámá, že volba není vykonána na základě soukromého a svobodného rozhodnutí občanů. Navíc pojem „veřejná volba“ se netýká hlasovacích prostorů otevřených pro širokou veřejnost, těmi jsou ostatně i volební místnosti a tradiční volbu bychom tedy také museli klasifikovat jako veřejný projev. Termín „veřejný“ se přesněji vztahuje k hromadnému a viditelnému vyjádření souhlasu nebo nesouhlasu, který probíhá zpravidla pod dohledem všech přítomných. Alternativní volba je oproti tomu individuálním aktem, který nijak nepodléhá kontrole ostatních hlasujících a není tedy přípustné považovat ji za volbu veřejnou.

Jiná je situace u případného ovlivňování voličů rodinnými a jinými příslušníky, což představuje výrazný zásah do soukromých práv občana. Tento negativní jev může samozřejmě nastat i při klasickém způsobu hlasování, nicméně u elektronických voleb je

¹⁹ Vyloučit dvojí volbu lze také důslednou kontrolou odevzdaných hlasů dle seznamu oprávněných voličů, což úspěšně praktikuje například Estonsko. Tamtéž, s. 243.

²⁰ KITCAT, Jason: *Electronic Voting. A challenge to democracy?* Open Rights Group 2007. www.openrightsgroup.org/wp-content/uploads/org-evoting-briefing-pack-final.pdf (1. 3. 2007).
GARRONE, Pierre: *Fundamental and political rights in electronic elections*. In: *The European Union and e-Voting. Addressing the European Parliament's internet voting challenge*. Sestavil Alexander H. Trechsel a Fernando Mendez. Londýn, New York 2005, s. 117-118.

riziko nesrovnatelně vyšší, jelikož dotyčného je možné při vlastním úkonu pozorovat, a tím nátlak vystupňovat. Jedná se tedy o porušení zásady svobodného výkonu hlasovacího práva, kdy občanům není garantováno volit podle jejich nejlepšího svědomí a politického přesvědčení. Mezi nejčastější hrozby patří kupování hlasů nebo vynucená volba určitého politického subjektu či kandidáta, pro něhož by občan za normálních (svobodných) okolností nehlasoval.²¹ Faktem zůstává, že finanční motivace obyvatel (a tedy prodávání hlasů) nepomine ani při ponechání osvědčených mechanismů, ani při prosazení alternativní volby, a pozornost se proto soustředí na druhý aspekt soukromého vyjádření vůle. Efektivní řešení přitom existuje a v praxi se úspěšně aplikovalo například v Estonsku během komunálních (2005) i parlamentních (2007) voleb. Občané zde měli možnost odevzdat elektronický hlas několikrát, čímž ve chvíli, kdy nebyli pod dohledem, automaticky změnili své původní nedobrovolné rozhodnutí na volbu dle vlastního výběru. Možností opakovaného výkonu volebního práva byl minimalizován tlak na voliče a svobodná povaha hlasování tím nebyla dotčena.

Co se týká posledního kritického momentu, jenž odpůrci progresivních volebních forem v souvislosti s rovností voleb vyzdvihují, nejsou ani zde jejich argumenty zcela odůvodněné. Z technického hlediska totiž není problém oddělit identitu voliče, popřípadě jeho elektronického klíče, od samotného obsahu hlasování, a anonymita občanů je tak i nadále garantována. Konkrétně je zabezpečení dáno tím, že ve fázi, kdy je hlas voliče propojen s jeho identifikátorem, systém neumožní otevřít obálku s obsahem jeho volby. Po skončení hlasování je pak tato vazba přerušena a údaje jsou následně drženy odděleně. V žádné fázi volebního procesu tak není možné zjistit, jak kdo hlasoval, čímž základní princip tajných voleb zůstává zachován. Nezbytnou součástí ochrany identity občanů je rovněž vyhrazení přístupových práv k rozšifrování obálek kompetentnímu technickému personálu, vnitřní audit a nezávislá kontrola systému v průběhu celé hlasovací procedury. V neposlední řadě musí být volby zabezpečeny taktéž fyzickou přítomností státních kontrolních orgánů, které dohlížejí nad počítači shromažďujícími a vyhodnocujícími výsledky hlasování.²²

Abychom se vypořádali se všemi obavami odborné veřejnosti, je třeba objasnit i zbývající spornou otázku spočívající v potenciálním ohrožení zásady přímých voleb. Někteří kritici upozorňují, že hlasování pomocí počítače, pošty, telefonu nebo televize těžko můžeme pokládat za volbu přímou. Takové tvrzení však naprosto nevystihuje význam přímého hlasovacího práva vyjádřeného v ústavách a jiných ustanoveních demokratických zemí. Institut přímých voleb se totiž vztahuje k přímému výběru kandidátů do státních funkcí, což znamená, že občané volí své zástupce přímo, a nikoliv prostřednictvím sboru, který následně rozhoduje o konečném složení zastupitelských orgánů. Opakem je volba nepřímá uplatňovaná od konce 18. století ve Francii,²³ kdy občané nejprve vybírali jednot-

²¹ BIRCH, Sarah - WATT, Bob: *Remote Electronic Voting: Free, Fair and Secret?* The Political Quarterly, 75, 2004, č. 1, s. 62-64. ZÁLEŠÁK, M. - MATEJKA, J.: *c. d.*

²² CRANOR, Lorrie F.: *Electronic Voting. Computerized polls may save money, protect privacy.* <http://www.acm.org/crossroads/xrds2-4/voting.html> (14. 3. 2007). ŠINDELÁŘ, P.: *c. d.*, s. 243.

²³ Institut nepřímých voleb zavedla francouzská ústava v roce 1791. KLÍMA, M.: *c. d.*, s. 188.

livé volitele, kteří poté dle vlastní vůle určovali podobu národních shromáždění. V jistých oblastech se tento nepřímý způsob hlasování zachoval až do současnosti, a to především u voleb do druhých komor parlamentů (například do německé Spolkové rady) nebo do funkce prezidenta (v České republice).²⁴ Z uvedeného jasně vyplývá, že alternativní formy hlasování nijak neomezují volební právo občanů zvolit si přímo svého zástupce a nemůže se tedy jednat o omezení principu přímého hlasování.

Pokud jde o celkové zhodnocení právní problematiky, lze po provedené analýze konstatovat, že zpochybňování inovativních volebních postupů z důvodu jejich rozporu s ústavně zakotvenými hlasovacími právy není opodstatněné. Jedinou oblastí, kde se riziko porušení právních předpisů podařilo částečně prokázat, je oblast všeobecného přístupu občanů k volebnímu procesu, jež by nebyl vzhledem k trvající digitální propasti zcela zaručen. Je tedy pravděpodobné, že na všeobecné úrovni by se prosazení alternativních metod setkala s oprávněnými námitkami. Ty však nelze vznést v případě aplikace moderních postupů jako doplňku k tradičnímu hlasování. Uzákonění korespondenční, elektronické a digitální volby v kombinaci se stávajícími hlasovacími technikami totiž neodporuje žádnému legislativnímu pravidlu a zákonodárci tak mohou bez obav přistoupit k jejich realizaci.

Závěr

Není pochyb o tom, že ukotvení alternativních forem hlasování představuje významný krok směrem k modernizaci demokracie. Lze dokonce říci, že vzhledem k intenzivnímu rozvoji nových komunikačních technologií v posledních desetiletích je tento krok nejen potřebný, ale také nevyhnutelný. Jen těžko si dokážeme představit, že by procedura výběru reprezentantů, i přes výrazný posun ve vývoji společnosti, zůstala neměnná. Navíc, ani osvědčené mechanismy nejsou zárukou spolehlivosti a pokud budou státy trvat na zachování tištěných volebních listků, i nadále se budeme setkávat s množstvím negativních jevů charakteristických pro tuto tradiční formu. Těmi jsou především četné hlasovací podvody, záměrná manipulace s kandidátními listinami či nepřesné výsledky způsobené chybami během zdlouhavého ručního počítání. Po každých volbách tak můžeme být svědky zpochybňování konečných údajů, ať už ze strany nespokojených kandidátů, kteří budou s poukazem na lidskou omylnost vyžadovat jejich opětovnou kontrolu, nebo z iniciativy státních orgánů majících na starosti zajištění řádného průběhu hlasování. Jistě bychom se nevyhnuli ani soudnímu přezkumu volebních výsledků a jiným nárokům uplatňovaným soudní cestou. Vážným problémem, se kterým se klasický způsob hlasování nedokáže vypořádat, je rovněž fenomén klesající participace. Východiskem přitom mohou být právě alternativní metody hlasování, které prostřednictvím informačních technologií umožňují větší podíl přímého rozhodování občanů na politice. Na rozdíl od

²⁴ KLÍMA, M.: *c. d.*, s. 188–189. AMBROŽ, Jan: *E-volby jsou v ČR vzdálenou budoucností*. <http://www.lupa.cz/clanky/e-volby-jsou-v-cr-vzdalenou-budoucnosti/> (30. 1. 2007)

klasických postupů mají totiž potenciál posílit občanskou angažovanost a podnitit zájem obyvatel o veřejné dění.²⁵

V současné době proto většina vyspělých států upřednostňuje pokrokové způsoby hlasování, které nejenže překonávají jmenované obtíže, ale také přinášejí řadu výhod, jež tradiční hlasovací postupy nemohou a nikdy ani nebudou schopny nabídnout. Patří mezi ně především výrazné zvýšení pohodlnosti hlasování, zvýšení rychlosti a přesnosti zpracování volebních výsledků, zjednodušení volebního procesu, snížení náročnosti při vyhodnocování hlasů a s tím související eliminace chyb vzniklých při jejich počítání. Dále pak odstranění možnosti manipulace s volebními listky a vzhledem k nainstalovanému kontrolnímu mechanismu také minimalizace množství neplatných hlasů. Významným přínosem je rovněž podpora prvků přímé demokracie a již zmíněné podnětí participace občanů dané přístupností a jednoduchostí volební procedury. Nesporný je v neposlední řadě také fakt, že pouze alternativní způsob hlasování relevantním způsobem odráží požadavky a životní styl obyvatel ve 3. tisíciletí.

Naopak problematickým bodem moderní hlasovací úpravy jsou analyzované pochyby týkající se bezpečnosti a zákonnosti celého konceptu. V článku jsem proto prováděla rozbor jednotlivých právních institutů, na základě něhož se potvrdilo, že ukotvení a aplikace alternativních způsobů hlasování ve formě doplňku k tradičním volebním technikám není v rozporu se základním ústavním principem všeobecného, rovného, přímého a tajného hlasovacího práva. Co se týká bezpečnosti hlasování, je nutné zdůraznit, že naplnění technických požadavků není snadné, nicméně ne nemožné. Přestože výskyt systémových chyb, a zejména pak vnějších útoků, nelze stoprocentně eliminovat, v praxi se jasně ukázalo, že pro většinu problémů již řešení existuje, a tedy nezbytnou ochranu zaručit lze. Navíc, určité obavy jsou v pozadí každého pokroku a pokud by společnost tato únosná rizika nenesla, vývoj by těžko mohl postupovat dále. Závěrem proto můžeme konstatovat, že s realizací elektronických voleb by se nemělo čekat na absolutní neomylnost technologii (té ani nelze dosáhnout), nýbrž že klíčovým argumentem by v tomto směru mělo být dosažení snadnějšího a efektivnějšího přístupu občanů k hlasovací proceduře.²⁶ A toho dosáhneme pouze zavedením alternativních způsobů hlasování.

LITERATURA

- ALVAREZ, Michael R. – HALL, Thad E.: *Point, Click, and Vote. The Future of Internet Voting*. Washington, Brooking Institution Press 2004. 204 s.
- BIRCH, Sarah – WATT, Bob: *Remote Electronic Voting: Free, Fair and Secret?* The Political Quarterly, 75, 2004, č. 1, s. 60–72.

²⁵ ŠINDELÁŘ, P.: c. d., s. 235–236.

²⁶ ZÁLEŠÁK, M. – MATEJKA, J.: c. d. JONES, Douglas W.: *The Evaluation of Voting Technology*. In: *Secure Electronic Voting*. Sestavil Dimitris A. Gritzalis. Boston, Dordrecht, Londýn 2003, s. 3.

- BURMESTER, Mike - MAGKOS, Emmanouil: *Towards Secure and Practical E-elections in the New Era*. In: *Secure Electronic Voting*. Sestavil Dimitris A. Gritzalis. Boston, Dordrecht, Londýn, Kluwer Academic Publishers 2003. s. 63-76.
- CRANOR, Lorrie F.: *Electronic Voting. Computerized polls may save money, protect privacy*. <http://www.acm.org/crossroads/xrds2-4/voting.html>
- GARRONE, Pierre: *Fundamental and political rights in electronic elections*. In: *The European Union and e-Voting. Addressing the European Parliament's internet voting challenge*. Sestavili Alexander H. Trechsel a Fernando Mendez. Londýn, New York, Routledge 2005. s. 111-123.
- JEFFERSON, David a kol.: *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*. 2004. 34 s. www.servesecurityreport.org/paper.pdf
- JONES, Douglas W.: *The Evaluation of Voting Technology*. In: *Secure Electronic Voting*. Sestavil Dimitris A. Gritzalis. Boston, Dordrecht, Londýn, Kluwer Academic Publishers. 2003. s. 3-16.
- KITCAT, Jason: *Electronic Voting. A challenge to democracy?* Open Rights Group 2007. www.openrightsgroup.org/wp-content/uploads/org-evoting-briefing-pack-final.pdf
- KLÍMA, Michal: *Volby a politické strany v moderních demokraciích*. Praha, Radix 2003. 273 s.
- MITROU, Lilian - GRITZALIS, Dimitris - KATSIKAS, Sokratis: *Revising legal and regulatory requirements for secure e-voting*. http://www.instore.gr/evote/evote_end/htm/3public/doc3/public/evote_paper_SEC_2002_2.doc
- PRATCHETT, Lawrence a kol.: *Balancing security and simplicity in e-voting. Towards an effective compromise?* In: *The European Union and e-Voting. Addressing the European Parliament's internet voting challenge*. Sestavili Alexander H. Trechsel a Fernando Mendez. Londýn, New York, Routledge 2005, s. 166-184.
- RADWIN, Michael J.: *An untraceable, universally verifiable voting scheme*. 1995. 9 s. <http://www.radwin.org/michael/projects/voting.html>
- RUBIN, Aviel D.: *Security Considerations for Remote Electronic Voting over the Internet*. New Jersey 2001. <http://avirubin.com/e-voting.security.htm>
- ŠINDELÁŘ, Petr: *Elektronické volby jako možný nástroj pro posílení demokracie*. System Integration 2006. si.vse.cz/archiv/clanky/2006/sindelar.pdf
- ZIMMERMANN, Frank: *Anonymous code lists for secure electronic voting over insecure mobile channels*. 2003.

ZDROJE

- AMBROŽ, Jan: *E-volby jsou v ČR vzdálenou budoucností*. <http://www.lupa.cz/clanky/e-volby-jsou-v-cr-vzdalenou-budoucnosti/>
- DICTSON, Derek - RAY, Dan: *The Modern Democratic Revolution: An Objective Survey of Internet-Based Elections*. White Paper, The Internet Voting Portal, 2000. www.SecurePoll.com
- Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů.*
- ZÁLEŠÁK, Michal - MATEJKA, Ján: *Nové možnosti (e)demokracie*. <http://park.logos.cz/article.asp?itm=203&ShowNoScriptVersion=True>