

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství



Disertační práce

**Metodika hodnocení elektronických systémů
pro tajné vzdálené volby**

Autor: Ing. Tomáš Martínek

Školitel: doc. Ing. Jan Tyrychtr, Ph.D.

© 2024 ČZU v Praze

„Má-li naše demokracie své nedostatky, musíme překonávat ty nedostatky, ale ne překonávat demokracii.“

— Tomáš Garrigue Masaryk

Poděkování

Rád bych tímto poděkoval školiteli doc. Ing. Janu Tyrychtrovi, Ph.D. a dalším kolegům z Katedry informačního inženýrství, Provozně ekonomické fakulty ČZU v Praze i dalším výzkumníkům. Dále bych rád poděkoval zúčastněným expertům, respondentům a dalším odborníkům, kteří přinesli dodatečnou odbornost do přípravy práce. A především bych rád poděkoval, nejen za pomoc s výchovou našich dětí, manželce RNDr. Tereze Martínkové Bártlové, Ph.D., rodině, přátelům a známým, díky nimž mohla tato práce vzniknout.

Tomáš Martínek

ORCID: [0000-0002-4295-0886](https://orcid.org/0000-0002-4295-0886)

Metodika hodnocení elektronických systémů pro tajné vzdálené volby

Abstrakt

Tato disertační práce se zaměřuje na problematiku hodnocení elektronických systémů pro tajné vzdálené volby s důrazem na technické, bezpečnostní a demokratické aspekty. Cílem je navrhnout metodiku evaluace, která zohledňuje specifické požadavky hlasovacích systémů včetně možnosti ověření hlasů při zachování tajnosti volby. V úvodu je provedena literární rešerše zaměřená na problematiku elektronického hlasování včetně implementace v různých zemích. Práce analyzuje aktuální úroveň připravenosti České republiky na zavedení internetového hlasování a porovnává jej s příklady z praxe, jako jsou Estonsko a Francie. Výzkum zahrnuje analýzu názorů uživatelů i odborníků na problematiku internetového hlasování prostřednictvím dotazníkových šetření a rozhovorů. Klíčovým přínosem práce je návrh nového komplexního metodického postupu pro hodnocení elektronických systémů volby přes Internet (CoMEvIS), který také díky technickému pracovnímu listu umožňuje efektivní posouzení dodržení technických standardů a demokratických norem. Vyhodnocení úrovní požadavků je provedeno metodou BeCoMe. Práce také probírá bezpečnostní rizika spojená s internetovým hlasováním, včetně ochrany proti útokům a zabezpečení hlasovacích systémů. Závěrem jsou formulována konkrétní doporučení pro zavedení elektronického hlasování v České republice, včetně legislativních změn a technických opatření, která mají zajistit transparentnost a důvěryhodnost volebních procesů.

Klíčová slova: Internetové hlasování, E-voting, E-democracy, E-government, Open-Source, Hodnocení systémů, Online hlasování, Standardy, Kyberbezpečnost, Kryptografie, Elektronické hlasování

Methodology for evaluation of electronic systems for secret remote elections

Abstract

This dissertation focuses on the evaluation of electronic systems for secret remote elections with emphasis on technical, security and democratic aspects. The aim is to propose an evaluation methodology that takes into account the specific requirements of voting systems, such as the possibility to verify votes while maintaining the secrecy of the election. In the beginning, the literature review is carried out focusing on the issue of electronic voting and its implementation in different countries. The dissertation then analyses the current state of preparedness of the Czech Republic for the introduction of internet voting and compares it with practical examples such as Estonia and France. The research includes an analysis of the opinions of users and experts on the issue of i-voting through questionnaire surveys and interviews. A key contribution of the thesis is the proposal of a new comprehensive methodological procedure for the evaluation of electronic voting systems via the Internet (CoMEvIS), which not only through a technical worksheet allows for an effective assessment of compliance with technical standards and democratic norms. The evaluation of the requirement levels is performed using the BeCoMe method. The dissertation also discusses the security risks associated with Internet voting, including protection against attacks and security of voting systems. Finally, specific recommendations for the introduction of electronic voting in the Czech Republic are formulated, including legislative changes and technical measures to ensure transparency and credibility of the electoral processes.

Keywords: Internet voting, E-voting, E-democracy, E-government, Open-Source, System evaluation, Online voting, Standards, Cybersecurity, Cryptography, Electronic voting

Obsah

1 Úvod	10
1.1 Struktura disertační práce	11
1.2 Motivace	12
2 Cíle a metodika práce	14
2.1 Cíle práce	14
2.2 Metodika práce	15
2.2.1 Zpracování teoretických východisek	16
2.2.2 Bibliometrická analýza	17
2.2.3 Analýza názorů stávajících uživatelů internetového hlasování	18
2.2.4 Analýza názorů potenciálních uživatelů internetového hlasování	19
2.2.5 Rozhovory s odborníky a zainteresovanými osobami	21
2.2.6 Návrh metodického postupu provedení tajné internetové volby	22
2.2.7 Expertní určení úrovní požadavků	22
2.2.8 Metoda BeCoMe	24
2.2.9 Propojení stávajících metodik do doporučení Rady Evropy	28
2.2.10 Definování CoMEvIS	29
3 Teoretická východiska problematiky tajného elektronického hlasování	31
3.1 Kategorizace hlasování	31
3.1.1 Srovnání možností vzdáleného hlasování	36
3.2 Zkušenosti s elektronickým hlasováním	38
3.2.1 Estonsko	38
3.2.2 Norsko	40
3.2.3 Austrálie	41
3.2.4 Kanada	41
3.2.5 Spojené státy americké	42
3.2.6 Francie	43
3.2.7 Švýcarsko	43
3.2.8 Další státy	44
3.3 Standardizace	45
3.3.1 Doporučení CM/Rec(2017)5 výboru ministrů členským státům o standardech pro elektronické hlasování	45
3.3.2 Směrnice Výboru ministrů o používání informačních a komunikačních technologií (ICT) ve volebních procesech v členských státech Rady Evropy - CM(2022)10	46
3.4 Způsoby hlasování dle možností výběru	46
3.4.1 Alternativní volební systémy	47
3.4.2 Povinné hlasování	47
3.5 Legislativa	47
3.5.1 Volební právo v Česku	48
3.5.2 Digitální základy pro celonárodní internetové hlasování v Česku	50
3.6 Kryptografie	50

3.6.1 Homomorfnní šifrování	54
3.6.2 Mixnety	57
3.6.3 Slepé podpisy	60
3.7 Architektura vzdáleného elektronického volebního systému	60
3.7.1 Základní schéma vzdáleného elektronického hlasovacího systému	60
3.7.2 Schéma vzdáleného elektronického hlasování založené na blockchainu	62
3.7.3 Techniky autentizace a ověřování identity	64
3.7.4 Fáze volebního procesu vzdáleného elektronického hlasování	65
3.8 Bezpečnostní rizika	65
3.8.1 Zranitelnost software	66
3.8.2 Útoky na klienta voliče	66
3.8.3 Útoky na síťovou infrastrukturu	66
3.8.4 Korupce	67
3.8.5 Útoky sociálního inženýrství	67
3.8.6 Státní manipulace	68
3.9 Koncepty hodnocení systémů pro vzdálenou tajnou elektronickou volbu	68
4 Výsledky	75
4.1 Bibliometrická analýza	75
4.2 Analýza názorů stávajících uživatelů internetového hlasování	78
4.3 Analýza názorů potenciálních uživatelů internetového hlasování	80
4.4 Expertní určení úrovně požadavků Rady Evropy CM/REC(2017)5	81
4.5 Propojení metodiky s doporučením Rady Evropy CM/REC(2017)5	84
4.5.1 Všeobecné volební právo	84
4.5.2 Rovné volební právo	85
4.5.3 Svobodné volební právo	87
4.5.4 Tajné volební právo	89
4.5.5 Regulační a organizační požadavky	91
4.5.6 Transparentnost a pozorování	95
4.5.7 Odpovědnost	97
4.5.8 Spolehlivost a bezpečnost systému	99
4.5.9 Doplňující požadavky	104
4.6 CoMEvIS - metodika komplexního hodnocení systémů internetového hlasování v rámci tajných voleb	105
4.6.1 Hodnocení technických standardů a demokratických norem	106
4.6.2 Hodnocení regulace, předpisů a jiných norem užití	107
4.6.3 Hodnocení participace na hlasování	107
4.6.4 Hodnocení transparentnosti	109
4.6.5 Hodnocení nákladovosti, zajištění kontinuálního vývoje a podpory	109
4.6.6 Dodatečná hodnotící kritéria	110
5 Diskuze	111
5.1 Vyhodnocení výzkumných otázek	113
5.1.1 Jak se v České republice využívá tajné internetové hlasování? (VO1)	113
5.1.2 Jak je Česká republika digitálně připravena na zavedení internetového hlasování	

v rámci politicky závazných voleb? (VO2)	113
5.1.3 Mělo by dojít k regulaci internetového hlasování v rámci tajných voleb soukromých i veřejných institucí? (VO3)	115
5.1.4 Mělo by zavedení možnosti internetového hlasování v celonárodních volbách vliv na volební účast a strukturu volebních výsledků? (VO4)	116
5.1.5 Jakým způsobem snížit riziko nátlaku na voliče zahrnující i dobrovolnou spolupráci s korupčníkem v rámci vzdálených elektronických voleb? (VO5)	116
5.1.6 Jak zajistit dostupnost elektronických hlasovacích systémů pro vzdálenou volbu v době voleb? (VO6)	117
6 Závěr	119
6.1 Příležitosti budoucího výzkumu	120
6.2 Přínosy práce	121
6.3 Omezení výzkumu	122
7 Seznam použitých zdrojů	124
Přílohy	143
Příloha A: Požadavky na vzdálené hlasovací systémy dle Marcos del Blanco (2018)	143
Příloha B: Komparace software pro tajnou vzdálenou elektronickou volbu	150
Příloha C: Formulář pro experty s pokyny	155
Příloha D: Ukázka vyhodnocení dat metodou BeCoMe	157
Příloha E: Agregovaná data s určením úrovně požadavku	158
Příloha F: Vyplněný technický pracovní list pro hodnocení internetového hlasovacího systému pro tajnou volbu České pirátské strany	164
Příloha G: Vyplněný technický pracovní list pro hodnocení internetového hlasovacího systému pro tajnou volbu agrárních organizací	171
Příloha H: Článek Hodnocení i-voting systému pro vzdálené primární volby České pirátské strany	178
Příloha I: Článek Implementace tajné a ověřitelné personální elektronické volby na dálku agrární organizace dle doporučení Rady Evropy	202
Příloha J: Článek Digitální nástroje, demokratické affordance a participace v síťové straně: Česká pirátská strana	218
Příloha K: Preprint Hodnocení demokracie na českých vysokých školách používajících systém internetového hlasování pro volby do akademického senátu	241

Seznam tabulek

Tabulka 1: Porovnání požadavků na správu korespondenčního a internetového hlasování (strana 36)
Tabulka 2: Porovnání naplnění požadavků použitelnosti korespondenčního a internetového hlasování (strana 36)
Tabulka 3: Porovnání naplnění bezpečnostních požadavků korespondenčního a internetového hlasování (strana 37)
Tabulka 4: Statistiky prvního internetového hlasování a parlamentních voleb v Estonsku (strana 40)
Tabulka 5: Obce Ontario s individuální ověřitelností ve volbách v roce 2022 (strana 42)
Tabulka 6: Vyhodnocení dotazníkového šetření očekávaných vlastností i-voting systémů mezi studenty a absolventy vysokých škol (strana 81)

Seznam obrázků

- Obrázek 1: Postup zpracování disertační práce, zjednodušená metodika (strana 15)
- Obrázek 2: Vývojový diagram metody BeCoMe (strana 25)
- Obrázek 3: Schéma trojúhelníkové funkce příslušnosti fuzzy čísla (strana 25)
- Obrázek 4: Srovnání středu kružnice opsané / Circumcentrum - středu kružnice vepsané / (Orto)Centrum - těžiště / Centroid (strana 26)
- Obrázek 5: Typologie odevzdání hlasu (strana 32)
- Obrázek 6: Hlasování poštou v Evropě (strana 33)
- Obrázek 7: Elektronické hlasování ve světě (strana 35)
- Obrázek 8: Schéma podepsání a ověření digitálního podpisu (strana 53)
- Obrázek 9: Zpráva procházející množstvím mix serverů v mixnetu (strana 58)
- Obrázek 10: Komunikace mezi aktéry vzdáleného elektronického hlasovacího systému (strana 61)
- Obrázek 11: Struktura blockchainu (strana 63)
- Obrázek 12: Svoboda ve světě 2023 (strana 68)
- Obrázek 13: Na základě právnických kritérií (Bräunlich, 2013) odvozené technické požadavky (strana 69)
- Obrázek 14: Integrace Bräunlich (Bräunlich, 2013) v rámci evaluace Panizo (strana 71)
- Obrázek 15: Kompletní praktický hodnotící rámec (strana 72)
- Obrázek 16: Kompletní praktický hodnotící rámec s přidáním kritérií (strana 73)
- Obrázek 17: Kategorie článků ve Web of Science (strana 75)
- Obrázek 18: Země autorů článků ve Web of Science (strana 76)
- Obrázek 19: Vizualizace co-citací autorů (strana 76)
- Obrázek 20: Vizualizace analýzy klíčových slov (strana 77)
- Obrázek 21: Korelační matice otázek číslovaných v pořadí podle přílohy G (strana 80)
- Obrázek 22: Množina požadavků zahrnutých v hodnotící metodice CoMEvIS (strana 105)
- Obrázek 23: Počet odevzdaných hlasů v prvním kole českých prezidentských voleb v roce 2023 v jednotlivých zemích Evropy v zahraničí dle dat Českého statistického úřadu (strana 114)
- Obrázek 24: Počet odevzdaných hlasů v prvním kole českých prezidentských voleb v roce 2023 v jednotlivých zemích v zahraničí dle dat Českého statistického úřadu (strana 115)

Seznam použitých zkratk

2FA	Dvoufaktorová autentizace - <i>Two-factor authentication</i>
AES	<i>Advanced Encryption Standard</i>
AI	Umělá inteligence - <i>Artificial Intelligence</i>
ASAP	Co nejdříve, jak je to možné - <i>As Soon As Possible</i>
BDŘ	(Kybernetická) Bezpečnost dodavatelského řetězce
BeCoMe	<i>Best Compromise Mean</i>
BFT	<i>Byzantine Fault Tolerance</i>
CAPTCHA	<i>Completely Automated Public Turing test to tell Computers and Humans Apart</i>
CAS	<i>Central Authentication Service</i>
CAWI	<i>Computer Assisted Web Interviewing</i>
CCA	<i>Chosen-Ciphertext Attack</i>
CNIL	Národní komise pro informatiku a svobodu (ve Francii)
CoE	Rada Evropy - <i>Council of Europe</i>
ČSÚ	Český statistický úřad
DIA	Digitální a informační agentura
DLT	<i>Distributed Ledger Technology</i>
DRE	<i>Direct Recording Electronic</i>
DDoS	<i>Distributed Denial of Service</i>

DoS	<i>Denial of Service</i>
E2Ev	E2E ověřitelnost - <i>End to End Verification</i>
EDR	<i>Endpoint Detection and Response</i>
EU	Evropská unie
FREAK	<i>Factoring RSA Export Keys</i>
GDPR	<i>General Data Protection Regulation</i>
HP	Hewlett-Packard
ID	Identifikátor
ICT	Informační a komunikační technologie
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
IT	Informační technologie
ISO	<i>International Organization for Standardization</i>
LWE	<i>Learning With Errors</i> (učení s chybami)
MaxAgM	<i>Maximum Agreement Mean</i>
NAKIT	Národní agentura pro komunikační a informační technologie, s. p.
NDA	<i>Non-disclosure agreement</i>
NDR	<i>Network Detection and Response</i>
NIA ID	Přihlášení jménem, heslem, SMS kódem via Národní Identitní Autorita
OCR	<i>Optical Character Recognition</i>
ODIHR	<i>Office for Democratic Institutions and Human Rights</i>
OHCHR	<i>Office of the High Commissioner for Human Rights</i>
OS	Operační systém
OTP	<i>One-Time Password</i>
PBFT	<i>Practical Byzantine Fault Tolerance</i>
PIN	Osobní identifikační číslo
PoA	<i>Proof of Authority</i>
PoS	<i>Proof of Stake</i>
PoW	<i>Proof of Work</i>
PKE	<i>Public Key Encryption</i>
RLA	<i>Risk Limit Audit</i>
RSA	<i>Rivest-Shamir-Adleman</i> (algoritmus)
QR kód	Kód rychlé odpovědi - <i>Quick Response</i>
SHA	<i>Secure Hash Algorithm</i>
SIM	Účastnická identifikační karta (v rámci mobilních sítí)
SOC	Security Operations Center
SPCSS	Státní pokladna Centrum sdílených služeb, s. p.
SSL	<i>Secure Sockets Layer</i>
UI	<i>User Interface</i>
UX	<i>User Experience</i>
UOCAVA	<i>Uniformed and Overseas Citizens Absentee Voting Act</i>
TDG	<i>Technical Design Goals</i>
TLS	<i>Transport Layer Security</i>
USA	Spojené státy americké
W3C	<i>World Wide Web Consortium</i>
WAI	<i>W3C Web Accessibility Initiative</i>
WCAG	<i>Web Content Accessibility Guidelines</i>
ZKP	<i>Zero-Knowledge Proof</i>

1 Úvod

Informační a komunikační technologie procházely od vzniku Internetu rychlým vývojem. Digitalizace procesů pomáhá zvyšovat efektivitu i komfort uživatelů. Na počátku tisíciletí se očekávalo, že dojde k digitalizaci demokratických procesů včetně voleb. V roce 2024 je využití elektronického hlasování přes Internet v právně závazných celonárodních volbách po světě stále minimální. Více než desetileté zkušenosti v rámci celonárodních voleb má pouze Estonsko, kde se zároveň, stejně jako jinde, řeší bezpečnostní rizika daného systému (Springall, 2014). S využitím hlasování přes Internet v politicky závazných volbách alespoň na komunální úrovni nebo u voličů pobývajících v zahraničí mají určité zkušenosti i země jako Kanada, Spojené arabské emiráty, Francie, Ekvádor, Spojené státy americké, Rusko, Austrálie, Švýcarsko, Finsko, Norsko a další. Poslední čtyři jmenované země ovšem mají stejně tak zkušenosti s ukončováním pilotních projektů elektronického hlasování. Využití elektronického hlasování v Rusku spíše přináší otázky ohledně integrity voleb a rizika státní manipulace.

Pandemie COVID-19 si vyžádala mnohem větší využití vzdálené komunikace, ačkoliv rozvoj vzdáleného elektronického hlasování se konal spíše ve volbách nižšího významu. V současné době je tajné vzdálené elektronické hlasování využíváno téměř po celém světě ve volbách do orgánů akademických institucí, komerčních společností, zemědělských družstev a podobně. Elektronické hlasování neustále řeší různé kryptografické výzvy, bezpečnostní hrozby, či vyvážení protichůdných požadavků, jakými jsou například požadavek na integritu voleb včetně ověřitelnosti a současně požadavek na zajištění soukromí voličů (Koitmäe, 2021).

V rámci elektronického hlasování přes Internet existuje mnoho částí celého systému hlasování, které musí být důvěryhodné a zabezpečené — od zařízení voliče, přes síťovou infrastrukturu po samotný hlasovací systém včetně zainteresovaných aktérů. Pokud by bylo narušení integrity útokem na systém odhaleno až po vyhlášení výsledků, je velmi obtížné situaci napravit. Vzdálené hlasování probíhá v nekontrolovaném prostředí, kde může snadněji dojít k ovlivnění voliče. Historické zkušenosti se snahami ovlivnit výsledky klasických (Transparency International, 2014) i elektronických voleb (Wolchok, 2012) neustále připomínají význam nutnosti pořád zlepšovat bezpečnostní opatření celého systému, kde by narušení integrity mohlo mít významné dopady na celou společnost.

Mezi základní požadavky na elektronický volební systém vzhledem k zajištění důvěryhodnosti patří ověřitelnost správného započítání hlasů i bezpečnostní nezávislý audit. Stejně tak je důležitá evaluace samotných hlasovacích systémů i postupů, podle kterých se volba provádí. I přesto se hodnocením systémů hlasování zabývalo pouze několik prací. V roce 2016 Neumann navrhl pravděpodobnostní rámec pro schémata elektronického hlasování (Neumann, 2016a). Následně Panizo a

Marcos del Blanco zavedli ucelenou metodiku s technickými a právními připomínkami i praktickými doporučeními ve svém systému hodnocení elektronických volebních systémů (Panizo Alonso, 2018). Zvažovali zejména požadavky Rady Evropy na elektronické hlasování (Council of Europe, 2017) a také soubor technických a praktických faktorů hodnocených mezinárodními odborníky v oblasti elektronického hlasování (Marcos del Blanco, 2018a). O další rozvoj metodik hodnocení internetových hlasovacích systémů se snaží některé státy včetně Francie (La Commission nationale de l'informatique et des libertés, 2019) a další akademici (Brunet, 2023). Tato práce na tyto studie navazuje a snaží se odstranit některé identifikované nedostatky současných konceptů hodnocení.

Stávající metodiky hodnocení nezahrnují nové poznatky, neposkytují jasnou informaci o splnění požadavků doporučení Rady Evropy (Council of Europe, 2017), nenabízí jednoduché technické pracovní listy pro provedení evaluace, nezahrnují určení minimálních požadavků v rámci různých úrovní hlasování nebo nehledí na další kritéria, která je vhodné při hodnocení těchto specifických systémů zvažovat. V rámci této práce je na základě výzkumu navržena nová komplexní metodika hodnocení elektronických systémů pro tajné vzdálené volby, která zahrnuje nové poznatky, umožňuje jasné a jednoduché vyhodnocení minimálních požadavků pomocí inovativního technického pracovního listu, včetně vyhodnocení splnění definované úrovně významnosti, a popsání postupu pro hodnocení dalších kritérií. Metodiku je možné použít pro vyhodnocení stávajících i připravovaných postupů provedení internetového hlasování s využitím různých volebních systémů.

1.1 Struktura disertační práce

Po úvodu, cílech a metodice práce je popsán základní rámec problematiky elektronického hlasování v rámci obsáhlé třetí kapitoly teoretických východisek. Disertační práce na základě rešerše odborné literatury z vědeckých databází Web of Science, Scopus a dalších dostupných vědeckých zdrojů, souvisejících odborných publikací a jiného přináší zpracování teoretických východisek, které zahrnují typologii hlasování, zkušenosti s elektronickým hlasováním jednotlivých zemí, standardizaci, způsoby hlasování, legislativu a digitální základy primárně v České republice, kryptografii, schéma vzdáleného elektronického volebního systému a bezpečnostní rizika. Poslední podkapitola obsahuje deskriptivní analýzu konceptů hodnocení splnění požadavků systémů pro tajné internetové hlasování. Primárně se soustředí na související práce Marcose del Blanca z let 2018-2020, Panizo Alonsa (2018), Neumanna (2016a) a další podobné studie.

Čtvrtá kapitola přináší popsané výsledky disertační práce. Vychází z bibliometrické analýzy významných vědeckých prací se zaměřením na elektronické volební systémy, jejich evaluaci a kryptografii. Následně analyzuje výsledky dotazníkových šetření provedených v rámci výzkumu (Martínek, 2024c; Martínek, 2024d; Martínek 2024g;

Martínek, 2024e). Další podkapitolu tvoří expertní určení úrovní požadavků Doporučení Rady Evropy CM/Rec(2017)5 (Council of Europe, 2017), která je založena na definování úrovní a následném expertním šetření vyhodnoceném pomocí rozhodovací metody BeCoMe. V následující podkapitole jsou do Doporučení Rady Evropy CM/Rec(2017)5 (Council of Europe, 2017) doplněny výsledné úrovně, autorské poznámky k evaluaci, propojení s metodikou Marcos del Blanco (2018a) a přidány doplňující požadavky. V poslední podkapitole je souhrnně popsán komplexní metodický postup evaluace s využitím technického pracovního listu (Martínek, 2024a) a dalších popisně hodnocených kritérií. Ukázku možnosti vyplnění technického pracovního listu lze nalézt v přílohách F a G.

V páté kapitole jsou diskutovány výsledky výzkumu a odpovědi na výzkumné otázky definované v kapitole Cíle práce.

Šestá závěrečná kapitola obsahuje shrnutí práce a vyhodnocení splnění cílů práce, definování příležitostí budoucího výzkumu, shrnutí přínosů práce a informace o omezeních výzkumu.

V příloze A je do češtiny přeložená hodnotící metodika od Marcos del Blanco (2018a), která je následně využita pro komparaci softwaru v příloze B.

Expertní šetření je dokumentováno přiložením formuláře předloženého expertům v Příloze C, ukázkou vyhodnocení získaných dat metodou BeCoMe na jedné z otázek v Příloze D a kompletními agregovanými daty od expertů včetně vyhodnocení v Příloze E.

Celý výzkum se opírá o řadu publikací autora (viz Seznam použitých zdrojů), kde hlavní související publikace často citované v práci jsou přiloženy v přílohách H, I, J a preprint v příloze K.

1.2 Motivace

Autor práce se tajnou vzdálenou elektronickou volbou dlouhodobě zabývá. Během působení v Poslanecké sněmovně se zabýval digitalizací veřejné správy jako člen podvýboru pro e-government i jako místopředseda volebního výboru. Zaváděním a provozem internetového hlasování se zabýval v rámci vnitrostranické demokracie České pirátské strany, integrací informačních systémů se zabýval v rámci působení na pozici Systémového integrátora Provozně ekonomické fakulty ČZU v Praze. V rámci svého doktorského studia oboru Informační management se autor věnoval pedagogické činnosti předmětů Systémová integrace, Interakce člověk počítač, Softwarového inženýrství, Moderní prostředky informatiky pro administrativu, provoz a řízení související s tématem disertační práce i výzkumu zaměřeného na personální volbu, informační systémy a jejich evaluaci.

Autor si je vědom rizik spojených s nedodržením demokratických norem a technických standardů (Kapitola 2.2.10) při zavádění systémů pro vzdálenou volbu, které mohou mít neblahý vliv na celou společnost. Z toho důvodu se snaží přinést do této aktuální problematiky odborný vhled, který má pomoci zavádět a provozovat systémy pro vzdálenou elektronickou volbu správně. Za lepší považuje systémy nezavádět, pokud by hrozilo nedodržení demokratických norem a technických standardů. Tato práce by proto měla tuto multidisciplinární problematiku komplexně pojmout, zlepšit možnosti evaluace těchto specifických systémů a přiblížit problematiku všem čtenářům.

2 Cíle a metodika práce

2.1 Cíle práce

Hlavním cílem disertační práce (HC) je navrhnout metodiku evaluace elektronických systémů pro tajné vzdálené online volby zahrnující hodnocení celého postupu s ohledem na standardizované požadavky jako je verifikace hlasovacího lístku při zachování tajnosti hlasování.

V rámci návrhu bude analyzován současný technologický pokrok, srovnány stávající elektronické volební systémy pro vzdálenou volbu i připravenost České republiky na zavedení elektronických voleb.

Mezi **dílčí cíle** práce patří:

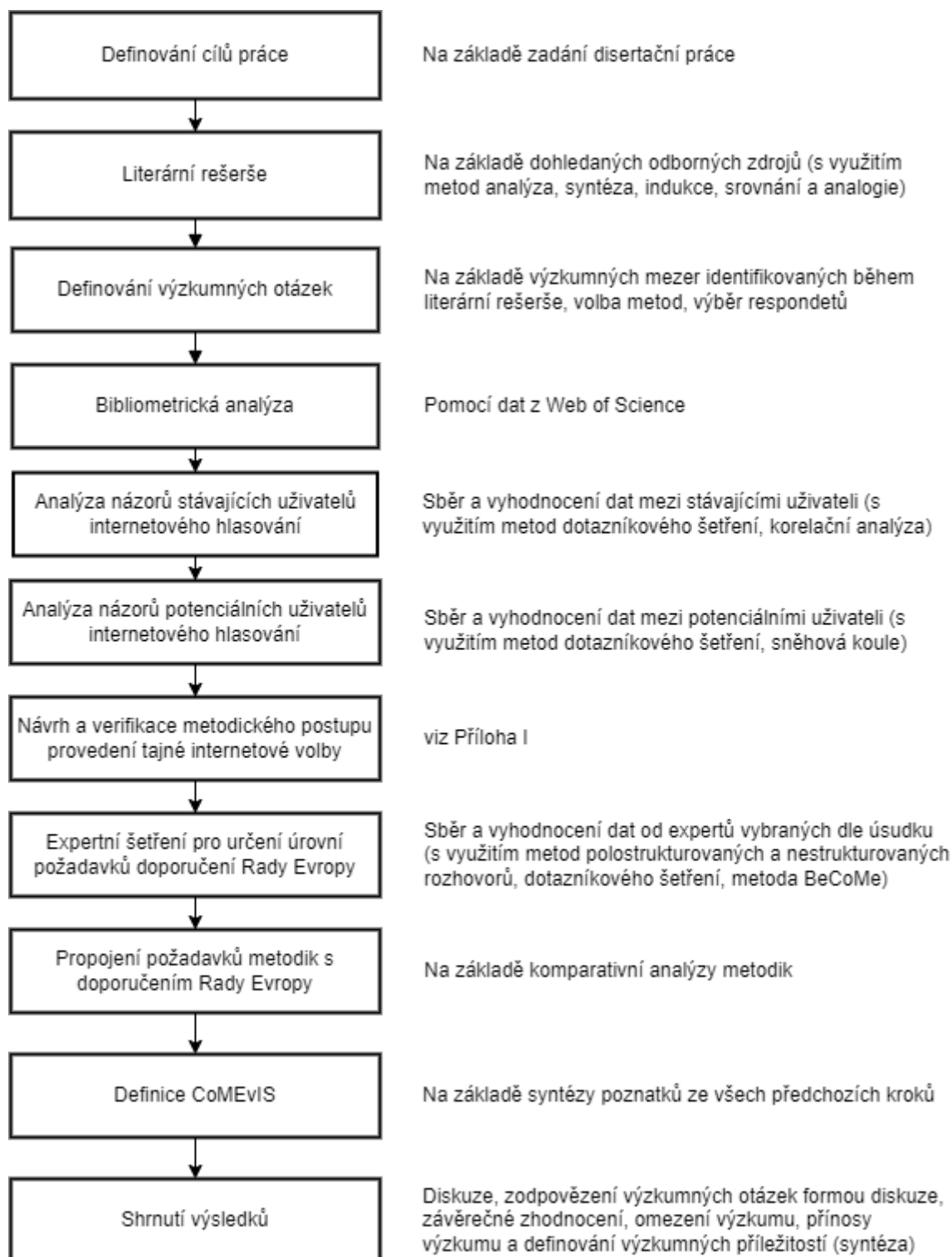
- prozkoumat současný stav poznání v oblasti tajné elektronické vzdálené volby a dostupné open-source systémy, které umožňují tajnou elektronickou vzdálenou volbu (DC1),
- prozkoumat stav digitalizace veřejné správy v oblasti voleb (DC2),
- zpracovat komplexně problematiku tajných internetových voleb, zhodnotit přínosy a rizika provedení tajné ověřitelné vzdálené elektronické volby (DC3),
- analyzovat názory stávajících a potenciálních uživatelů internetového hlasování (DC4),
- navrhnout a ověřit nový metodický postup provedení vzdálené elektronické volby (DC5),
- expertně určit úrovně požadavků na systémy internetového hlasování (DC6),
- provést syntézu dosažených výsledků a formulovat závěry a doporučení pro další výzkum (DC7).

Na základě výzkumu by se mělo v rámci diskuze odpovědět také na několik formulovaných **výzkumných otázek**:

- Jak se v České republice využívá tajné internetové hlasování? (VO1)
- Jak je Česká republika digitálně připravena na zavedení internetového hlasování v rámci politicky závazných voleb? (VO2)
- Mělo by dojít k regulaci internetového hlasování v rámci tajných voleb soukromých i veřejných institucí? (VO3)
- Mělo by zavedení možnosti internetového hlasování v celonárodních volbách vliv na volební účast a strukturu volebních výsledků? (VO4)
- Jakým způsobem snížit riziko nátlaku na voliče zahrnující i dobrovolnou spolupráci s korupčníkem v rámci vzdálených elektronických voleb? (VO5)
- Jak zajistit dostupnost elektronických hlasovacích systémů pro vzdálenou volbu v době voleb? (VO6)

2.2 Metodika práce

Metodika práce se skládá z několika postupných kroků, které znázorňuje následující obrázek 1.



Obrázek 1: Postup zpracování disertační práce, zjednodušená metodika (vlastní zpracování)

2.2.1 Zpracování teoretických východisek

Základem disertační práce je systematické prozkoumání oblasti vzdálené tajné a ověřitelné elektronické volby a souvisejících technologických a legislativních pokroků formou literární rešerše. Aktuální poznatky v této oblasti jsou shromážděny analýzou sekundárních dat z vědeckých publikací indexovaných v databázích Web of Science a Scopus, případně dalších databází a publikací v renomovaných časopisech nebo přednesených na mezinárodních konferencích a jiných vědeckých zasedáních. Konkrétně se pro hledání využily klíčová slova související s tématem práce jako *internet voting*, *e-voting*, *system evaluation* a další včetně různých kombinací. Mezi další využití databáze patří SpringerLink, IEEE Xplore Digital Library nebo ACM Digital Library a využití citačních AI nástrojů Elicit, Dimensions a návrhů ChatGPT. Sekundárně se využívají odborné weby, odborné knihy, akademické práce, materiály vývojářů souvisejících informačních systémů, podklady odborných pracovních skupin ve veřejné správě i legislativa České republiky, Evropské unie či podklady Rady Evropy. Reference byly spravovány pomocí nástroje CitacePRO, kdy se využívá citační styl ČSN ISO 690 (autor, datum), který pro citace v textu generuje formát: První autor (Rok vydání) s případným písmenným rozlišením v případě více referencí hlavního autor v daném roce.

Analýza stavu připravenosti České republiky byla učiněna zkoumáním stávajícího stavu digitalizace veřejné správy pomocí neformálního a nestrukturovaného interview s osobami v rámci Státní pokladny Centra sdílených služeb a jiných institucí. Informace byly také čerpány z materiálů a neformálních a nestrukturovaných rozhovorů s účastníky konference E-Vote-ID, která je pravděpodobně nejvýznamnější konferencí se zaměřením na elektronické volební systémy a které se autor práce zúčastnil (Martínek, 2022). Autor také čerpá ze svých zkušeností se systémy pro internetové hlasování, z působení v Poslanecké sněmovně, ve volební komisi nebo z dalších navštívených odborných konferencí. Výzkum je smíšený, protože kombinuje kvantitativní i významněji kvalitativní část (Molnár, 2012).

Pro vytvoření teoretických východisek disertační práce byly použity obecné teoretické metody: analýza, syntéza, indukce, srovnání a analogie (Ochrana, 2019). Součástí výzkumu bylo také zkoumání dostupných informačních systémů, které umožňují tajnou vzdálenou elektronickou volbu, i formou vlastní instalace systému a zkoumání zdrojového kódu. Práce byla během její přípravy formou neformálních a nestrukturovaných rozhovorů konzultována s odborníky na digitalizaci, rozvoj, provoz a legislativu z veřejné správy i akademického prostředí. Kvalitativní výzkum je charakteristický tím, že jeho průběh se formuje během sběru dat. Tento typ výzkumu zkoumá realitu velmi detailně a do hloubky, což znamená, že lze získat mnoho informací od relativně malého počtu osob. O tom, které informace jsou relevantní, rozhodují sami respondenti, nikoli výzkumník. Díky tomu je výzkum velmi validní,

protože se minimalizuje zkreslení dat, jelikož data procházejí méně transformacemi. Hlubkový charakter zkoumání také umožňuje lépe porozumět zkoumanému jevu. Na druhou stranu, kvalitativní výzkum má nízkou reliabilitu, protože závěry jsou ovlivněny individuálním pohledem výzkumníka. Jiný výzkumník by mohl dojít k odlišným výsledkům (Olecká, 2010).

2.2.2 Bibliometrická analýza

Na základě prvotní literární rešerše byla provedena bibliometrická analýza. Bibliometrická analýza se uplatňuje v širším akademickém výzkumu, kdy je jejím cílem hodnotit kvalitu, dopad a vliv autorů i dalších subjektů v dané výzkumné oblasti (Hassan, 2017). Kromě toho nabízí bibliometrická analýza další výhody, jako je identifikace trendů, podpora spolupráce, srovnávání s kolegy, podpora rozhodování nebo odhalování mezer ve znalostech. Díky těmto výhodám je bibliometrická analýza cenným nástrojem pro výzkumníky, kteří usilují o informovaná rozhodnutí založená na datech a efektivní řízení výzkumu.

V rámci výzkumu bylo analyzováno 106 prací z databáze Web of Science, vybraných na základě vyhledání "*e-voting system evaluation*" se zahrnutím referencí dohledaných prací se související tematikou zaměřenou na kryptografii, elektronické hlasovací systémy a jejich hodnocení. Zdrojová data analýzy jsou veřejně dostupná na Zenodo (Martínek, 2024h). Bibliometrická analýza se zaměřuje na kategorie zkoumaných prací a země autorů vizualizovaných pomocí nástroje Clarivate a Microsoft Excel. Pomocí nástroje VOSviewer 1.6.20 byla provedena vizualizace klíčových slov a co-citací, která znázorňuje vazby pomocí vzdáleností, velikosti uzlů a barev.

Barvy na mapě označují různé tematické klastry. V analýze klíčových slov barvy představují skupiny klíčových slov, která se často objevují společně v textech, zatímco v analýze co-citací autorů barvy reprezentují autory, kteří jsou často citováni ve stejném kontextu. **Velikost uzlů** reflektuje jejich důležitost. U klíčových slov velikost uzlu ukazuje, jak často se dané klíčové slovo vyskytuje, a u autorů velikost uzlu značí počet citací daného autora. **Vzdálenost mezi uzly** pak odráží sílu vztahu — v případě klíčových slov to znamená, že čím blíže jsou k sobě, tím častěji se vyskytují společně v dokumentech, a u co-citací autorů to naznačuje, že čím blíže jsou autoři k sobě, tím častěji jsou citováni společně (Van Eck, 2010).

Bibliometrická analýza se zaměřuje také na celkový počet citací. Data byla platná k 2. červenci 2024. Bibliometrická analýza pomohla určit významné vědecké práce, na které bral autor větší zřetel během finalizace disertační práce, pomohla určit klíčová slova spojená s výzkumem a především pomocí kategorií článků přispěla k následnému výběru expertů na základě jejich specializací.

2.2.3 Analýza názorů stávajících uživatelů internetového hlasování

Pro zjištění názorů stávajících uživatelů systému tajného internetového hlasování bylo se souhlasem předsednictva České pirátské strany provedeno anonymní dotazníkové šetření mezi členy České pirátské strany.

Metoda dotazníkového šetření je kvantitativní výzkumný nástroj, který se používá k získání dat od velkého počtu respondentů prostřednictvím standardizovaných otázek. Dotazníky mohou být distribuovány různými způsoby, včetně tištěných formulářů, online dotazníků, telefonických rozhovorů nebo poštovních zásilek. Hlavní výhodou této metody je možnost získat strukturovaná data, která jsou snadno analyzovatelná a umožňují srovnávání mezi různými skupinami respondentů. Metodika navrhování dotazníků zahrnuje formulaci otázek, které jsou jasné, nezavádějící a přiměřené pro cílovou skupinu. Klíčovými zdroji pro návrh a administraci online dotazníků jsou práce Dillmana (2011) a Fowlera (2013), které poskytují detailní pokyny a osvědčené postupy. Dotazníkové šetření se často používá v sociálních vědách, marketingovém výzkumu a veřejném mínění. Jeho spolehlivost a platnost jsou však závislé na kvalitě dotazníku a na reprezentativnosti vzorku respondentů.

Návrh dotazníku byl před jeho finalizací testován se skupinou respondentů a na základě zpětné vazby byl upraven do finální podoby. Sběr dat proběhl pomocí metody CAWI. **Metoda CAWI** je technika sběru dat, která využívá Internet k provádění dotazníkových šetření. Respondenti odpovídají na otázky prostřednictvím webového rozhraní, což umožňuje efektivní a rychlý sběr dat. Výhodou této metody je její dostupnost, nízké náklady a možnost oslovit široké spektrum respondentů. Díky automatizaci je také snadné výsledky okamžitě analyzovat. Nicméně nevýhodou může být omezený přístup k respondentům, kteří nemají internet, a riziko nízké míry návratnosti. Metoda je vhodná pro průzkumy trhu, sociální výzkumy nebo hodnocení veřejného mínění (Bethlehem, 2009).

Pro průzkum byla využita platforma *ankety.pirati.cz* založená na aplikaci LimeSurvey, kam měli přístup k dotazníku pouze členové Pirátské strany prostřednictvím unikátní URL adresy zaslané v e-mailové pozvánce, která členům umožnila dotazník jednorázově vyplnit. Odpovědi na dotazník byly dobrovolné a anonymní, jak bylo uvedeno na úvodní stránce dotazníku a v e-mailové pozvánce. Průzkum probíhal od 22. února do 14. března 2024. Z celkového počtu 1 179 členů strany vyplnilo anketu s 19 otázkami v plném rozsahu 213 členů, což představuje 18,6 % ze všech členů strany. Na 16 výzkumných otázek bylo možné odpovědět ano nebo ne, 3 otázky byly sociodemografické a zaměřovaly se na pohlaví, věk a dosažené vzdělání. Podrobně je dotazníkové šetření vyhodnoceno v článku autora v Acta Informatica Pragensia (Martínek, 2024d).

K účasti na dotazníkovém šetření byli vyzváni všichni členové České pirátské strany, vzhledem k nízkému počtu členů není řešena reprezentativnost respondentů vůči celé populaci. Data průzkumu jsou veřejně přístupné na Zenodo (Martínek, 2024c). Pro další zjištění byly analyzovány agregované skupiny odpovědí u daných otázek ve vztahu k odpovědím na ostatní otázky. Pro výsledky je použita výzkumná metoda popisné statistiky s čísly. Údaje jsou agregovány a následně slovně interpretovány. Výsledky průzkumu jsou prezentovány v procentech zaokrouhlených na jedno desetinné místo.

K analýze závislostí mezi otázkami v souboru dat byla použita **korelační analýza** (Lee Rodgers, 1988). Odpovědi Ano byly převedeny na hodnotu 1 a odpovědi Ne na hodnotu 0. Korelační matice byla vypočtena pomocí Pearsonova korelačního koeficientu (Pearson, 1895). Tento koeficient měří sílu lineárního vztahu mezi dvěma proměnnými. Výsledný koeficient může nabývat hodnot od -1 do 1, kde:

- 1 znamená dokonale pozitivní lineární závislost,
- 0 znamená žádnou lineární závislost,
- -1 znamená dokonale zápornou lineární závislost.

Vzorec pro Pearsonův korelační koeficient r je:

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}} \quad (1)$$

Kde:

- n je počet párů hodnot,
- x a y jsou jednotlivé hodnoty dvou proměnných.

K interpretaci výsledků slouží heatmapa korelační matice pro 16 výzkumných otázek z datového souboru, která poskytuje přehled o vzájemných závislostech mezi odpověďmi, které jsou očíslovány podle pořadí uvedeného v článku (Martínek, 2024d). K analýze dat byla použita knihovna Pandas 1.4.0 pro programovací jazyk Python a heatmapa byla vytvořena pomocí knihovny Python Matplotlib 3.4.3 s využitím knihovny Seaborn 0.11.2.

2.2.4 Analýza názorů potenciálních uživatelů internetového hlasování

Za účelem zjištění názorů potenciálních uživatelů na vlastnosti dálkového elektronického hlasování bylo provedeno dotazníkové šetření mezi studenty a absolventy českých vysokých škol zemědělského zaměření. I když pro výběr byla použita metoda sněhové koule, lze předpokládat, že se jedná o osoby s vyšší technickou gramotností, kteří mohou být v blízké budoucnosti potenciálními uživateli systémů internetového hlasování. **Metoda sněhové koule** (Goodman, 1961; Biernacki, 1981) je technika výběru respondentů, která se často používá v sociálním

výzkumu, zejména tam, kde je přístup k vhodným respondentům obtížný. Tento postup je založen na tom, že výzkumník nejprve identifikuje malé množství respondentů, kteří splňují kritéria výzkumu, a poté požádá tyto jedince, aby doporučili další osoby, které také splňují tato kritéria.

Pro skladbu otázek byl použit framework od Agbesi (2023) pro zkoumání dimenzí transparentnosti internetového hlasování, doplněný o několik specifických otázek. Agbesi (2023) s kolegy identifikuje pět základních dimenzí, a to Dostupnost informací, Srozumitelnost, Monitorování a ověřitelnost, Nápravná opatření, Testování, přičemž tyto dimenze ovlivňují vnímání transparentnosti, což následně ovlivňuje důvěryhodnost celého systému. Anonymní dotazníkové šetření bylo provedeno metodou CAWI online prostřednictvím platformy LimeSurvey na webu *Dotaznik.czu.cz* provozovaném Českou zemědělskou univerzitou v Praze. Pozvánka k účasti v průzkumu byla určena především českým studentům a absolventům zemědělských vysokých škol. Průzkum probíhal od 24. října 2023 do 12. května 2024. Účastníkům byly veškeré informace včetně souhlasu se zpracováním dat zobrazeny na úvodní stránce průzkumu.

Respondenti odpovídali na otázky na sedmibodové Likertově škále od rozhodně nesouhlasím (0) po rozhodně souhlasím (6) v pěti definovaných dimenzích. Dotazník vyplnilo celkem 177 osob. Celkem 108 dotazníků bylo vyplněno v plném rozsahu. Z nich bylo odstraněno dalších 8 dotazníků, protože kontrolní otázka "Tato otázka není součástí průzkumu a pouze nám pomáhá odhalit boty a automatizované skripty. Chcete-li potvrdit, že jste člověk, zvolte zde prosím možnost 'Rozhodně souhlasím'" byla zodpovězena jinak než "Rozhodně souhlasím". Ze 100 odpovědí bylo 64 mužů, 35 žen a 1 respondent neuvedl své pohlaví. Ve věku 18-30 let je 72 respondentů, ve věku 31-40 let 18 respondentů, ve věku 41-50 let 5 respondentů, ve věku 51-60 let 2 respondenti a ve věku 61-70 let 3 respondenti. Středoškolské vzdělání má 72 respondentů, 10 má bakalářský titul, 12 magisterský titul a 6 doktorský titul.

Dotazníkové šetření je vyhodnoceno souhrnně podle stanovených dimenzí a transparentnosti, které se skládají z jednotlivých otázek. Hodnocení popisuje průměrnou četnost odpovědí na Likertově škále a míru očekávání naplnění dané dimenze na škále od 0 (vůbec se neočekává) do 1 (plně se očekává), přičemž od výše 0,5 se daná charakteristika očekává. Míra očekávání pro danou vlastnost je poměr průměrného hodnocení k maximálnímu možnému hodnocení v rámci souhrnu celé dimenze. Výpočet vychází ze zjištění průměrné odpovědi $\bar{X}_d$ (0 až 6) pro jednotlivou dimenzi

$$\bar{X}_d = \frac{\sum_{j=1}^m \left(\frac{\sum_{i=1}^n x_{ij}}{n} \right)}{m} \quad (2)$$

Kde:

- $\bar{X}_d$ je průměrná odpověď pro dimenzi d ,
- x_{ij} je hodnota odpovědi respondenta i na otázku j v dimenzi d ,
- n je počet respondentů,
- m je počet otázek v dimenzi d .

Výpočet míry očekávání naplnění dané dimenze E_d se provádí:

$$E_d = \frac{\bar{X}_d}{X_{max}} \quad (3)$$

Kde:

- E_d je míra očekávání naplnění dimenze d ,
- X_{max} maximální možná hodnota na Likertově škále (6).

K popisné statistice byl použit software Statistica 14, kdy byly dopočítány základní údaje, jako jsou průměrné, minimální a maximální hodnoty, různé míry variability a údaje týkající se tvaru rozdělení proměnné (včetně směrodatné odchylky a směrodatné chyby). Důležitým aspektem popisu proměnné byl tvar jejího rozdělení, který udává četnost hodnot v různých rozsazích proměnné. Přesnější informace byly získány provedením testů normality pro určení pravděpodobnosti, že vzorek pochází z normálně rozdělené populace pozorování, konkrétně pomocí Shapiro-Wilkova testu (Shapiro, 1965). Tyto statistiky byly zahrnuty do veřejně přístupného souboru dat (Martínek, 2024g). Podrobněji jsou výsledky vyhodnoceny v článcích autora (Martínek, 2024e; Příloha K). Na základě analýz názorů stávajících i potenciálních uživatelů internetového hlasování bylo zjištěno, které kategorie požadavků jsou považovány za významné.

2.2.5 Rozhovory s odborníky a zainteresovanými osobami

V rámci disertační práce bylo provedeno několik rozhovorů s odborníky na IT, kybernetickou bezpečnost, právo, politologii, volební problematiku a další příbuzné obory (Příloha D, Příloha J). V příloze K podrobněji autor rozebírá provedené polostrukturované rozhovory se systémovými integrátory a dalšími zástupci vysokých škol. V příspěvku (Martínek, 2024b) byly provedeny nestrukturované rozhovory s českými krajany v zahraničí.

Metoda interview (rozhovoru) je klíčovým nástrojem v kvalitativním výzkumu, který umožňuje hlubší porozumění subjektivním zkušenostem, názorům a motivacím respondentů. Rozhovory mohou mít různé formy, přičemž polo-strukturované a

nestrukturované rozhovory jsou mezi výzkumníky velmi populární. Polostrukturované rozhovory jsou charakteristické tím, že výzkumník má předem připravený soubor otázek nebo témat, které chce probrat, avšak ponechává prostor pro spontánní odpovědi a otázky podle průběhu rozhovoru. To umožňuje získat hlubší vhled do zkoumaného problému, zatímco zároveň zajišťuje určitou míru konzistence mezi různými rozhovory. Klasické práce jako od Kvaleho (2009) a Brinkmanna nebo od Brymana (2016) poskytují podrobné návody a teoretické rámce pro vedení polostrukturovaných rozhovorů.

Nestrukturované rozhovory jsou ještě flexibilnější a často se používají v explorativních studiích, kde je cílem objevit nové koncepty nebo porozumět komplexním fenoménům bez předem dané struktury. Výzkumník zde nepracuje s pevně stanovenými otázkami, ale spíše s obecným tématem, kolem kterého se rozhovor volně točí. Tato metoda je zvláště užitečná v etnografickém výzkumu, kde je potřeba získat detailní a autentický pohled na životní zkušenosti respondentů. Kniha *The Ethnographic Interview* od Spradleyho (2016), která byla původně publikována v roce 1979, je považována za zásadní zdroj pro pochopení nestrukturovaných rozhovorů a jejich aplikace v terénu. Dalším důležitým zdrojem je práce Corbina (2015) a Strause, která nabízí vhled do využití nestrukturovaných rozhovorů v rámci zakotvené teorie, což je metoda analýzy dat, která často čerpá právě z nestrukturovaných rozhovorů.

2.2.6 Návrh metodického postupu provedení tajné internetové volby

Na základě zjištěných požadavků byl následně navržen metodický volební postup (Martínek, 2024e) s využitím systému Belenios (Belenios team, 2023), který by splňoval do určité míry požadavky Rady Evropy (Council of Europe, 2017). Metodický postup zahrnuje i procedury nesouvisející přímo s volebním software, jako je například způsob určení volební komise, způsob určení pravomocí, možnost klasické papírové volby a podobné. Systém byl autorem samostatně testován v rámci experimentálního hlasování na vlastní instalaci systému Belenios dostupné na volba.odvolit.cz, kdy došlo současně ke kontrole zdrojového kódu i testování systému za účelem ověření jeho správné funkčnosti. Navržený postup byl následně slovně verifikován na základě evaluace dle požadavků Rady Evropy (Martínek, 2024e).

2.2.7 Expertní určení úrovní požadavků

Na základě provedené rešerše, analýz názorů uživatelů internetového hlasování, nestrukturovaných rozhovorů s odborníky a pomocí určení kritérií ovlivňujících významnost voleb bylo stanoveno 6 úrovní voleb. Pro určení úrovní požadavků byly provedeny polostrukturované rozhovory s několika experty z oblastí IT, AI, kyberbezpečnosti, práva, politologie, volební politiky, veřejné správy apod.

vybranými úsudkem na základě kategorizace provedené v rámci bibliometrické analýzy. **Metoda úsudku** (úvahy) při výběru expertů je proces, během kterého se zvažují různé faktory, jako jsou odborné znalosti, zkušenosti, relevantní dovednosti a osobní vlastnosti kandidátů. Tento postup zahrnuje nejen formální hodnocení kvalifikací, ale také subjektivní posouzení vhodnosti konkrétního experta pro danou úlohu. Klíčové je při tomto přístupu zohlednit schopnost experta přinést hodnotný přínos na základě kontextu, ve kterém bude působit (Ericsson, 2012).

Experti vyplňovali dotazník vytvořený v aplikaci Google Tabulky (Příloha C), který obsahoval úvodní informace k povaze šetření. Každý expert je ve výzkumných datech, dostupných u autora práce, označen jménem i kontaktním e-mailem, v příloze D jsou s ohledem na ochranu osobních údajů u expertů uvedeny pouze jejich specializace.

Expertům byl způsob vyplňování vysvětlen na začátku formuláře (Příloha C), ve zvací zprávě i v rámci možného osobního neformálního rozhovoru. Celkem bylo nutné vyplnit optimální úroveň u 143 požadavků dle doporučení Rady Evropy (Council of Europe, 2017). Každý expert vyplnil optimální - Nejlepší návrh úrovně, od které má být daný požadavek vyžadován jako minimální základ. Pokud si nebyl jist optimální úrovní, mohl vyplnit Dolní a Horní mez úrovní, mezi kterými se rozhoduje. Každý požadavek byl popsán zkráceným i plným popisem. Každý expert měl vyplňovat vždy pouze hodnotu 1 až 5. Pokud některý z expertů vyplnil hodnotu 0, byla daná hodnota přepsána na hodnotu 1, protože dle definice úrovně 0 nevyžaduje splnění žádného požadavku. Pokud některý z expertů naopak vyplnil číslo vyšší než 5 nebo nevyplnil žádné číslo, protože považoval daný požadavek za nepodstatný, byla hodnota přepsána na číslo 5, protože tato úroveň má dle definice Doporučení CM/Rec(2017)5 výboru ministrů členským státem Rady Evropy o standardech pro elektronické hlasování (Council of Europe, 2017) plnit všechny požadavky. Každý expert mohl doplnit i slovní komentář. Aby nedošlo ke zkreslení výsledků měli experti dostatek času na případné vyplnění formuláře, konkrétně první oslovení expertů proběhlo v červenci 2024, deadline pro vyplnění byl 8. září 2024.

Celkem formulář vyplnilo 13 expertů z různých oblastí, jejich specializace je popsána v Příloze D, a čtrnáctý expert na kybernetickou bezpečnost poskytl alespoň slovní komentáře. Odpovědi expertů byly přeneseny do agregovaného listu odpovědí (Příloha E). Následně byly odpovědi transponovány tak, aby je bylo možné snadno vkládat do technického listu intervalového nástroje rozhodovací metody BeCoMe (Příloha D). V technickém listu metody BeCoMe tak bylo postupně vyhodnoceno všech 143 požadavků. Výsledné hodnoty Nejlepšího kompromisu a Maximální chyby odhadu byly následně přeneseny zpět do agregovaného listu odpovědí (Příloha E). Protože je potřeba pro jednotlivé požadavky určit minimální úroveň, od kterých má být daný požadavek povinný, tak byla určena minimální hodnota odečtením maximální možné chyby od nejlepšího kompromisu, čímž byla dána z hlediska

bezpečnosti přednost určení nižší úrovně před prostým určením vyšší úrovně. Tato hodnota byla následně zaokrouhlena na celé číslo, čímž byla určena konkrétní úroveň daného požadavku.

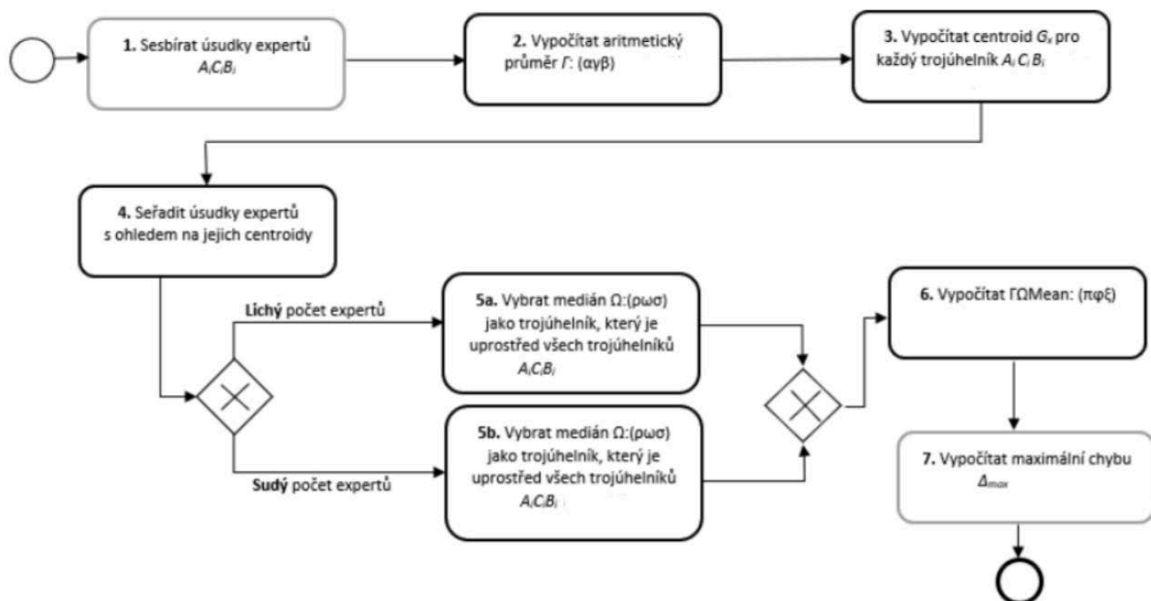
2.2.8 Metoda BeCoMe

Metoda BeCoMe (*BestCompromise-Mean*) zjednodušuje proces skupinového rozhodování tím, že se zaměřuje na nalezení co nejlepšího kompromisu mezi všemi zúčastněnými. Tyto osoby mohou zahrnovat například odborníky nebo uživatele určitého systému, kteří se mohou kvůli svým rozdílným specializacím výrazně lišit v názorech (Vrana, 2021). Pro schopnost matematicky vypočítat nejlepší možný kompromis expertů různých specializací je tato rozhodovací metoda použita pro vyhodnocení i v této práci. Metoda je postavena na open-source softwaru, přičemž zadávání i vyhodnocení dat lze provádět prostřednictvím tabulek v Microsoft Excel. BeCoMe také poskytuje grafické zobrazení výsledků, což usnadňuje jejich vizualizaci a interpretaci. Díky této metodě lze efektivně posoudit odpovědi odborníků na kvantitativní i kvalitativní parametry navrhovaného řešení (Vrana, 2021; Ander, 2022).

Metoda BeCoMe (Vrana, 2021) je založena na dříve publikované metodě MaxAgM (Vrana, 2012), přičemž přináší úpravy, které zachovávají výhody původní metody. Zároveň odstraňují nebo snižují její omezení. Mezi tyto nedostatky patřila především vysoká výpočetní a koncepční náročnost, složitá interpretace výsledků, absence ukazatelů přesnosti a nutnost používat specializovaný software (Vrana, 2021; Ander, 2022).

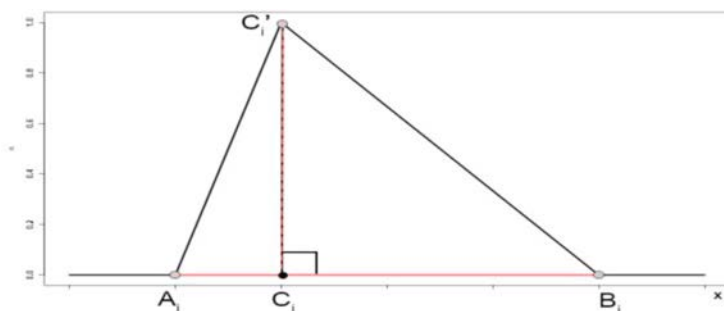
Metoda BeCoMe a její nástroje poskytují řešení pro dva klíčové aspekty: rychlost a spolehlivost rozhodování v nejasných situacích. Odborníci by měli posoudit určité kvantitativní nebo kvalitativní aspekty navrhovaného řešení. Svá stanoviska mohou vyjádřit třemi způsoby: 1) jako jednoduché číslo; 2) jako fuzzy číslo s preferovanou hodnotou, dolní a horní hranicí; a 3) jako hodnocení na Likertově škále s možnostmi jako „Rozhodně nesouhlasím“, „Spíše nesouhlasím“, „Neutrální“, „Spíše souhlasím“, „Rozhodně souhlasím“ nebo na podobné lingvistické stupnici (Vrana, 2021). V rámci této práce bylo zvoleno vyjádření úrovně formou fuzzy čísla s preferovanou hodnotou vyjádřenou celým číslem úrovně, případně také dolní a horní hranicí. Metoda byla použita při určování optimálního řešení expertů ve složitých situacích (Vrana, 2021) nebo také v rámci interakčního designu v prostředí ambientní inteligence (Ander, 2022).

Konkrétně lze využití metody BeCoMe znázornit tímto vývojovým diagramem a konkrétním postupem v 7 krocích (Vrana, 2021; Ander, 2022):



Obrázek 2: Vývojový diagram metody BeCoMe / vlastní úprava Ander (2022) na základě Vrana (2021)

1. Shromáždění úsudků expertů vyjádřených pomocí fuzzy čísel s trojúhelníkovou funkcí příslušnosti $A_i C_i B_i$, kde $A_i B_i$ je základnou trojúhelníku umístěného na reálné ose x a C_i je projekcí vrcholu trojúhelníku C'_i na osu x :



Obrázek 3: Schéma trojúhelníkové funkce příslušnosti fuzzy čísla (Vrana, 2021)

Vrchol trojúhelníku C odpovídá střední hodnotě názoru experta. To znamená, že hodnota $x=C$ je preferovanou hodnotou expertního návrhu. Míra preference pro určitou hodnotu x je úměrná souřadnici y na straně trojúhelníku. To znamená, že navrhovaná hodnota nesmí být menší než A ani větší než B .

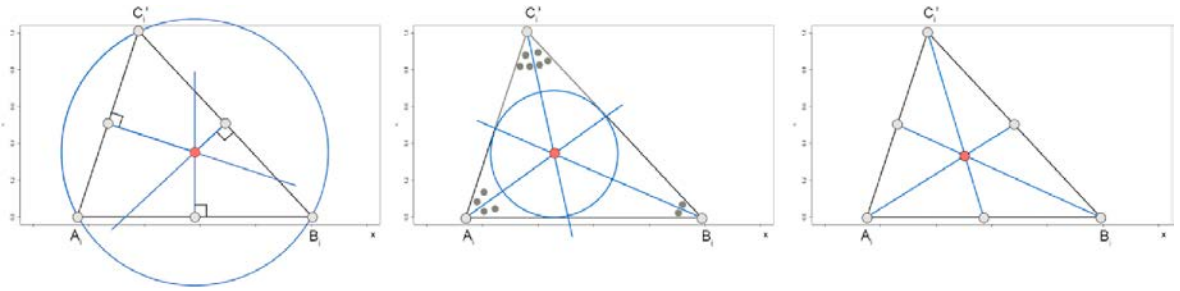
2. Vypočítat aritmetický průměr $\Gamma: (\alpha\gamma\beta)$ posudků M expertů je opět fuzzy číslo s trojúhelníkovou funkcí příslušnosti, kde jednotlivé vrcholy α , γ a β výsledné funkce příslušnosti jsou aritmetické průměry vrcholů dílčích funkcí příslušnosti A_i , C_i , B_i :

$$\alpha = 1 / M \sum_{k=1}^M A_k \quad (4)$$

$$\beta = 1 / M \sum_{k=1}^M B_k \quad (5)$$

$$\gamma = 1 / M \sum_{k=1}^M C_k \quad (6)$$

3. Vypočítat centroid G_x pro každý trojúhelník $A_i C_i B_i$:



Obrázek 4: Srovnání středu kružnice opsané / Circumcentrum - středu kružnice vepsané / (Orto)Centrum - těžnice / Centroid (Vrana, 2021)

$$G_x = \frac{(A + B + C)}{3} \quad (7)$$

4. Seřadit úsudky expertů s ohledem na jejich centroidy.
5. Vybrat medián $\Omega: (\rho\omega\sigma)$ jako trojúhelník, který je uprostřed všech trojúhelníků $A_i C_i B_i$:

- a) Je-li počet M expertů lichý, tj. $M = 2n + 1$, střed množiny trojúhelníkových fuzzy čísel $A_i C_i B_i$ patří tomu i , kde $z_i = n + 1$. Toto středové i se označuje jako q . V tomto případě je statistický medián $\Omega: (\rho\omega\sigma)$ naší množiny M fuzzy čísel $\{A_i C_i B_i\}$, $i = 1 \dots M$, fuzzy číslo $A_q C_q B_q$, kde:

$$\rho = A_q, \omega = C_q, \sigma = B_q \quad (8)$$

- b) Je-li $M = 2n$ sudé číslo, střed množiny trojúhelníkových fuzzy čísel $A_i C_i B_i$ leží mezi fuzzy čísly $A_p C_p B_p$ a $A_r C_r B_r$, kde p odkazuje na $z_i = n$ a r označuje $z_i = n + 1$. Medián je aritmetický průměr fuzzy čísel $A_p C_p B_p$ a $A_r C_r B_r$, kde:

$$\rho = \frac{(A_p + A_r)}{2} \quad (9)$$

$$\sigma = \frac{(B_p + B_r)}{2} \quad (10)$$

$$\omega = \frac{(C_p + C_r)}{2} \quad (11)$$

6. Vypočítejte $\Gamma\Omega Mean: (\pi\phi\xi)$, kdy se optimální hodnota skupinového rozhodnutí nachází mezi aritmetickým průměrem $\Gamma: (\alpha\gamma\beta)$ všech expertních rozhodnutí $\alpha\gamma\beta$ a jejich statistickým mediánem $\Omega: (\rho\omega\sigma)$. Optimální kompromis leží uvnitř intervalu (Γ, Ω) . Aritmetický průměr těchto dvou mezí intervalu $\Gamma\Omega Mean$ je definován aproximací $\Gamma\Omega Mean: (\pi\phi\xi) = (\Gamma + \Omega)/2$, tj.:

$$\pi = (\alpha + \rho)/2 = 1/2M \sum_{k=1}^M A_k + \rho/2 \quad (12)$$

$$\phi = (\gamma + \omega)/2 = 1/2M \sum_{k=1}^M B_k + \omega/2 \quad (13)$$

$$\xi = (\beta + \sigma)/2 = 1/2M \sum_{k=1}^M C_k + \sigma/2 \quad (14)$$

kde:

- M je počet expertů,
 - $A_i B_i$ jsou základny trojúhelníku,
 - C_i je vrchol trojúhelníkové funkce příslušnosti i -tého úsudku experta ($i=1, \dots, M$),
 - $\rho \omega$ jsou základny,
 - σ je vrchol statistického mediánu příslušnosti funkce.
7. Vypočítat maximální chybu Δ_{max} , která nemůže překročit polovinu rozdílu mezi krajními hodnotami, kterými jsou aritmetický průměr všech rozhodnutí expertů $\Gamma: (\alpha\gamma\beta)$ a jejich statistický medián $\Omega: (\rho\omega\sigma)$, tj.:

$$\Delta_{max} = \frac{abs(\alpha\gamma\beta - \rho\omega\sigma)}{2} \quad (15)$$

Metoda BeCoMe je lepší než metody využívající zobecněné průměrovací operátory a nabízí několik klíčových výhod (Vrana, 2021; Ander, 2022):

1. Dokáže přinést nejlepší možný teoretický kompromis.
2. Kromě kvantitativních výsledků umožňuje také kvalitativní posouzení aspektů problému, které nelze snadno kvantifikovat. Je také užitečná pro výběr nejvhodnějšího řešení z několika možností.
3. Odborníci mohou vyjádřit své názory pomocí reálných čísel, fuzzy čísel nebo Likertových škál.
4. Časové náklady jsou minimální, protože konečné řešení lze získat okamžitě po zadání proměnných.
5. Hlavní výhodou metody BeCoMe ve srovnání s původní metodou MaxAgM je její jednoduchost. Všechny parametry rozhodovacího procesu lze snadno spočítat pomocí tabulek v Microsoft Excel, bez nutnosti využívat specializovaný software. Tato jednoduchost přispívá také k větší koncepční přehlednosti, což zajišťuje snadnější interpretaci výsledků. Kromě toho je možné výsledky graficky zobrazit, což dále zjednodušuje jejich vizualizaci a pochopení.
6. Software metody BeCoMe je open source.

V této práci je také novinkou použití metody BeCoMe pro řešení velkého množství otázek.

2.2.9 Propojení stávajících metodik do doporučení Rady Evropy

Expertně určené úrovně jsou následně doplněny k jednotlivým požadavkům Doporučení Rady Evropy (Council of Europe, 2017) v hranatých závorkách v kapitole 4.5. Na základě komparativní analýzy Doporučení Rady Evropy (Council of Europe, 2017) s požadavky metodiky Marcos del Blanco (2018a) uvedených v příloze A jsou následně propojeny související požadavky a identifikovány požadavky, které Doporučení Rady Evropy (Council of Europe, 2017) a Marcos del Blanco (2018a) neobsahují. **Komparativní analýza metodik hodnocení informačních systémů** se zaměřuje na systematické porovnávání různých metodik používaných k hodnocení kvality informačních systémů (ISO, 2023). Tento přístup je důležitý zejména pro určení toho, jak různé metodiky definují různé kvalitativní atributy, jako je bezpečnost, použitelnost, výkonnost nebo spolehlivost systémů. Cílem této analýzy je zjistit, jaké rozdíly existují mezi metodami ve způsobu, jakým hodnotí systémové požadavky, a jaké postupy jsou vhodnější pro konkrétní typy informačních systémů nebo jejich kontexty použití. Propojené požadavky z metodiky Marcos del Blanco (2018a) jsou doplněny za název požadavku Doporučení Rady Evropy (Council of Europe, 2017) v kapitole 4.5.

Analyzovány jsou také další odborné práce zabývající se konkrétními požadavky na elektronické volební systémy (Panizo Alonso, 2018; Cucurull, 2019; Marcos

del Blanco, 2019; Marcos del Blanco, 2020; Brunet, 2023). Na základě analýzy jsou následně přidány pod číslem 50 doplňující minimální požadavky. Doplněny jsou také poznámky autora k jednotlivým požadavkům za účelem usnadnění vyhodnocení jejich splnění při provádění evaluace systému pro tajnou vzdálenou volbu.

2.2.10 Definování CoMEvIS

Na základě předchozích kroků, syntézou poznatků výzkumu zahrnující provedené analýzy, je souhrnně definována nová metodika komplexního hodnocení systémů internetového hlasování CoMEvIS (*Comprehensive Methodology of Evaluating I-voting Systems*).

Metodika reflektuje specifické požadavky na internetové hlasování, mezi které patří **regulace** (Von Nostitz, 2021; Deseriis, 2021; Council of Europe, 2017; Marcos del Blanco, 2018a), **technické standardy** (Von Nostitz, 2021; Council of Europe, 2017; Marcos del Blanco, 2018a; Curucull, 2019) mezi které se řadí bezpečnost, integrita, ověřitelnost a utajení hlasování, zajištění vlastnictví dat, kontrola, a **demokratické normy** (Von Nostitz, 2021; Council of Europe, 2017), mezi které patří:

- **Participace** voličů na hlasování, která je ovlivňována mírou inkluзивity a přístupnosti. Hlasování některým z volebních kanálů má být umožněno všem oprávněným voličům při dodržení ústavních zásad jako je všeobecnost, či tajnost.
- **Reprezentace** znamená, do jaké míry výsledky voleb odrážejí různorodé složení voličské komunity. Systém internetového hlasování by měl zajistit rovný přístup pro všechny oprávněné voliče i kandidáty bez ohledu na jejich socioekonomický status, technické prostředky nebo jiné překážky, aby výsledky voleb skutečně reprezentovaly hlasy všech skupin, včetně menšinových voličů.
- **Konkurenceschopnost** zajišťuje, aby volby umožňovaly spravedlivou soutěž mezi kandidáty a aby všichni kandidáti měli rovné příležitosti k účasti. V systémech internetového hlasování je zásadní zajistit, aby systém nezvýhodňoval určité skupiny nebo jednotlivce, čímž se podpoří spravedlivý volební proces.
- **Transparentnost a odpovědnost** znamená, že celý proces elektronického hlasování je přístupný nezávislému auditu a ověření. V systémech internetového hlasování může být transparentnost zajištěna prostřednictvím použití softwaru s otevřeným zdrojovým kódem nebo nezávislými audity, které umožní ověřit, že volby nebyly zmanipulované a že výsledky přesně odrážejí vůli voličů. Transparentnost a odpovědnost má garantovat legitimitu volebních výsledků. To zajišťuje důvěru voličů v systém a akceptaci internetového hlasování jako demokratické a legitimní metody hlasování.

- **Schopnost reakce** se týká toho, jak rychle a efektivně jsou řešeny problémy a jak jsou volenými zástupci reprezentovány preference voličů.

Základem pro hodnocení regulace, technických standardů i demokratických norem je vytvořený inovativní **technický pracovní list** (Martínek, 2024a), který umožňuje vyhodnotit splnění požadavků Doporučení Rady Evropy (Council of Europe, 2017) i doplněné minimální požadavky s ohledem na definovanou úroveň významnosti voleb v rámci bezplatné aplikace vytvořené pro Microsoft Excel, případně využitelné v jiném tabulkovém editoru. Dále metodika obsahuje popisné hodnocení dalších kritérií, které na základě komparativní analýzy (Von Nostitz, 2021; Deseriis, 2021; Council of Europe, 2017; Marcos del Blanco, 2018a) nejsou obsaženy v technickém pracovním listu (Martínek, 2024a) a které jsou zároveň dle analýz uživatelů internetového hlasování považovány za významné pro evaluaci.

Ověření funkčnosti technického pracovního listu je provedeno v přílohách F a G, kdy jsou hodnoceny systémy internetového hlasování evaluované v článcích autora (Martínek, 2024d; Martínek, 2024e). V prvním případě se jedná o evaluaci existujícího systému internetového hlasování (Martínek, 2024d; Příloha F), ve druhém případě se jedná o hodnocení prototypu, který je navržen formou nového metodického postupu implementace tajného vzdáleného elektronického hlasování s využitím konkrétního softwaru (Martínek, 2024e; Příloha, G).

Dle navržené metodiky je možné hodnotit nejen volební software, ale také celý postup konkrétní implementace nebo navrženého metodického postupu volby s využitím konkrétního software. Metodika se snaží formalizovat kroky hodnocení dodržení technických standardů a demokratických norem tak, aby mohlo dojít k objektivní kvantifikaci evaluace. Metodika doplňuje dané hodnocení o další kritéria popisným způsobem.

3 Teoretická východiska problematiky tajného elektronického hlasování

3.1 Kategorizace hlasování

Od veřejného hlasování pomocí slov a gest se postupně vyvinuly i další způsoby hlasování, které umožňují i zachování soukromí. Demokratický proces je dnes chápán ve spojitosti s volbami, které většinou stále probíhají klasicky pomocí papíru a volebních urn před volební komisí. Volkamer (2009) definuje 3 základní rozměry hlasování. První rozměr hlasování je dle **média**, na kterém je uložen. Může se tak jednat o uložení na:

- *papír*,
- *elektronické médium v bitech*,
- *mechanické médium využívající například dřerných štítků*.

Druhým rozměrem je **prostředí**, ve kterém se odevzdává hlas:

- *kontrolované prostředí*, kde volební pracovníci mají zajistit přesnost, soukromí a integritu procesu odevzdání hlasu (například ve volební místnosti před volební komisí),
- *nekontrolované prostředí*, kde není kontrola volebními pracovníky (například vzdálené hlasování z domova).

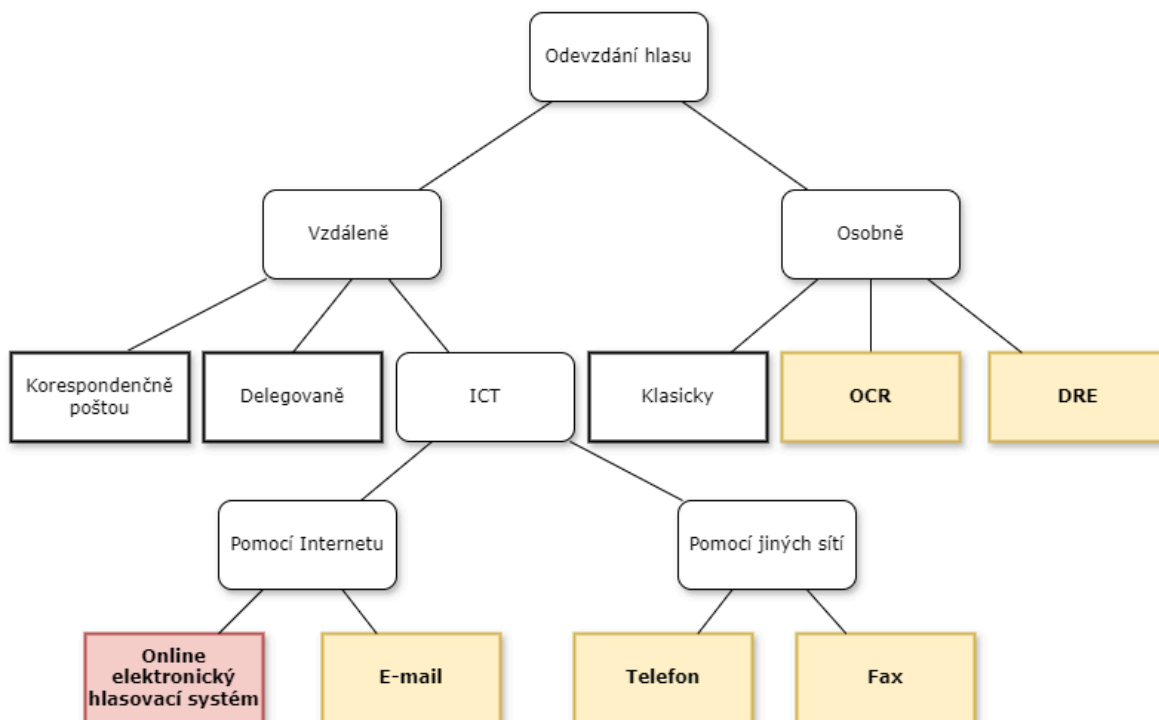
Třetím rozměrem je **okamžik** možného odevzdání hlasu:

- *ve volební den*,
- *přede dnem voleb* (tzv. předčasné hlasování).

Čtvrtým rozměrem by mohla být **hlasující osoba**:

- *volič*, kdy odevzdává hlas sám volič,
- *delegát*, kdy odevzdává hlas voličem pověřená osoba.

Řada států umožňuje více volebních kanálů odevzdání hlasu. Schéma na obrázku 5 zobrazuje možné způsoby hlasování, tučně zvýrazněné jsou elektronickými hlasováními (e-voting, e-hlasování) podle Rady Evropy (Council of Europe, 2004).



Obrázek 5: Typologie odevzdání hlasu (vlastní zpracování)

Klasické hlasování

Za klasické (případně *tradiční*, *papírové*) hlasování se považuje papírová volba voličem do volební urny v kontrolovaném prostředí před volební komisí.

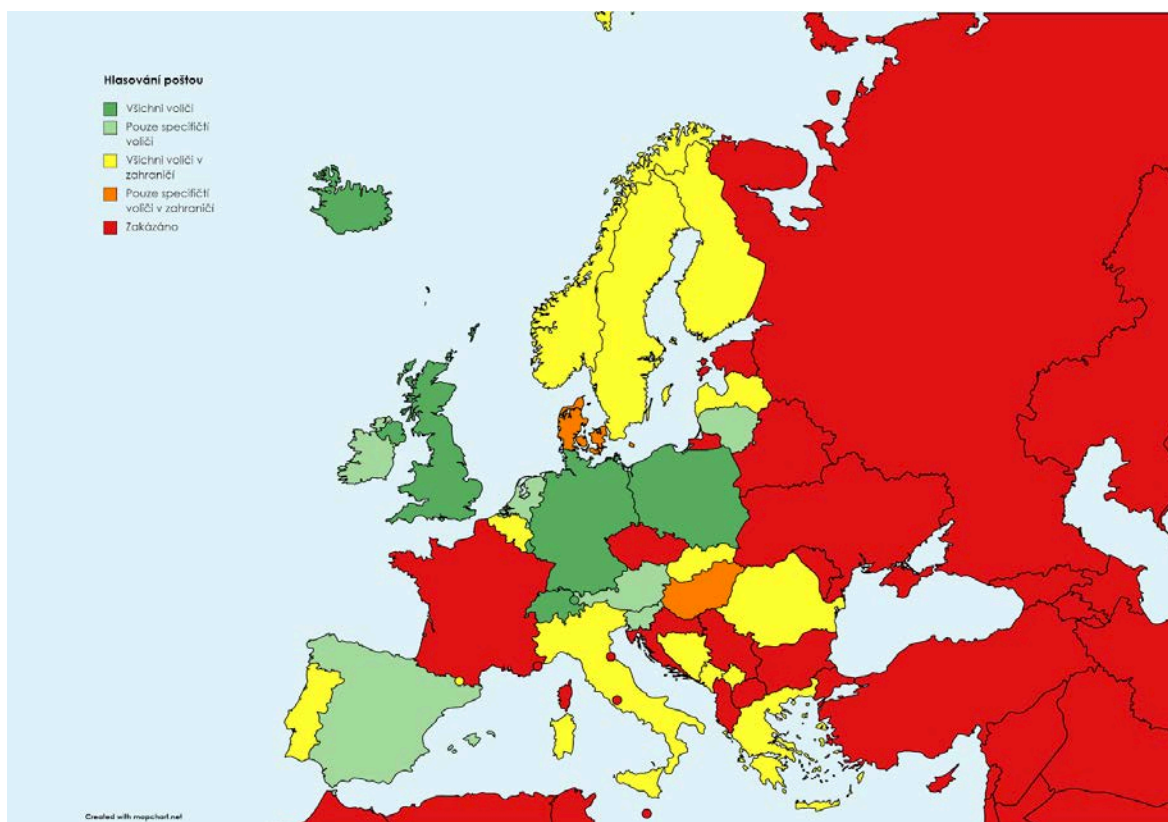
Některé země také umožňují předčasné odevzdání hlasu voličům, kteří by se v době voleb nemohli dostavit do volební místnosti.

Korespondenční hlasování

Za korespondenční hlasování se považuje vzdálené hlasování, kdy volič odesílá svůj hlas prostřednictvím papírové pošty. Existují různé varianty obdržení hlasovacích lístků, kde kromě pošty mohou být zapojeny i ICT například pro vyžádání hlasovacích lístků.

Hlasování poštou je povoleno pro určité voliče v mnoha zemích EU, jak zobrazuje následující Obrázek 6. Některé státy umožňují volit poštou pouze specifickým občanům, kteří dovršili určitý věk nebo se nemohou dostavit do volebních místností ze zdravotních důvodů, kvůli službě v armádě či uvěznění a podobně (Heinmaa, 2020).

Mnoho zemí umožňuje hlasování poštou alespoň voličům v zahraničí. Například Maďarsko povoluje poštou hlasovat pouze voličům bez adresy v Maďarsku, což jsou především etničtí Maďaři žijící v sousedních zemích, kde má vysokou podporu vládní strana Fidesz (Rupnik, 2022).



Obrázek 6: Hlasování poštou v Evropě / vlastní zpracování dle (Heinmaa, 2020)

Ve světě je korespondenční hlasování umožněno ve Spojených státech amerických, Kanadě, Japonsku, Indii či Austrálii (International IDEA, 2024).

Hlasování delegováním pravomoci

V tomto procesu volič předává své volební právo jiné osobě, která může hlasovat za voliče. Při tajné volbě je nezbytné delegovat toto právo na důvěryhodnou osobu, protože zvolenou možnost hlasování obvykle nelze zpětně ověřit. Volit přes delegovanou osobu lze například v Belgii, Francii, Nizozemí, Norsku, Polsku, Švédsku, Švýcarsku či Spojeném království (Heinmaa, 2020).

OCR (Optical Character Recognition)

V tomto případě se pro voliče jedná o formu klasického hlasování, kde si ovšem musí dát záležet na vyplněném papírovém hlasovacím lístku, protože lístek následně zpracovává technologie, která rozeznává vybranou volbu strojově.

DRE (Direct Recording Electronic)

V tomto případě odevzdává volič svůj hlas osobně přímo elektronickému hlasovacímu zařízení ve volební místnosti. Zpravidla jsou instrukce pro voliče zobrazeny na displeji zařízení, zařízení je ovládáno dotykově nebo pomocí klávesnice, volební data jsou zpravidla ukládána do paměti jednotek. Hlasovací

záznamy jsou následně bezpečně odeslány do sčítacího zařízení, to může zahrnout vyjmutí dat a jejich fyzické doručení do sčítací volební komise. DRE může umožnit i tisk stvrzenky pro možnost ověření hlasování voličem.

Hlasování e-mailem

Vzdálené hlasování prostřednictvím e-mailu těžko naplní všechny ústavní požadavky včetně zachování utajení hlasujícího. Tento způsob je v omezené míře nabízen v některých státech USA pro volbu nerezidentům a vojenskému personálu (Puiggalí, 2007). Protože nelze naplnit požadavek tajnosti, volič podepisuje dokument, kde se vzdává soukromí a práva na tajnost hlasování.

Hlasování faxem

Vzdálené hlasování pomocí faxu má obdobná omezení jako hlasování e-mailem. Tento způsob je v omezené míře také nabízen v několika státech USA pro volbu specifickým voličům (Puiggalí, 2007). Protože nelze naplnit požadavek tajnosti, volič podepisuje dokument, kde se vzdává soukromí a práva na tajnost hlasování.

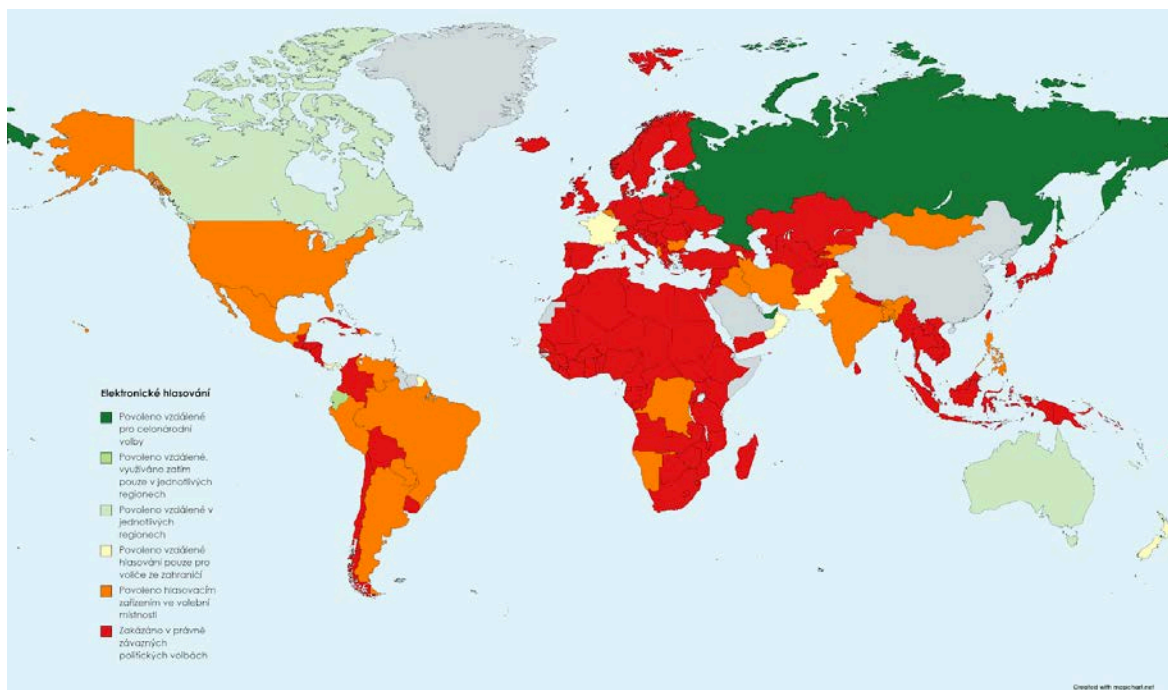
Hlasování po telefonu

Hlasování pomocí telefonního hovoru sice umožňuje vzdáleně hlasovat i méně technicky gramotné populaci, ale na druhou stranu má velké nedostatky v ochraně soukromí. Hlasovat po telefonu bylo umožněno v australském státě Victoria jako doplňková možnost k vzdálenému elektronickému hlasování prostřednictvím online elektronických volebních systémů. Využívá se například pro nevidomé nebo slabozraké voliče (Australian Electoral Commission, 2023).

Online elektronický hlasovací systém

V následujícím textu se bude práce zabývat primárně právě elektronickými systémy pro vzdálené hlasování (i-voting, i-hlasování), kde lze odevzdat hlas přes Internet pomocí připojeného zařízení, kterým může být počítač, chytrý telefon, tablet nebo jiné obdobné zařízení (dále také "internetové hlasování").

Internetové hlasování se v současné době používá pro celonárodní volby v Estonsku, Spojených arabských emirátech a Rusku, kde někteří účastníci jednání ODIHR NAM vyjádřili četné obavy týkající se celkové důvěry v elektronický volební systém a jeho transparentnost, jakož i nedostatků záruk pro ověřování ruských voličů a jasnosti ohledně možnosti podávat související stížnosti. Francie, Pákistán, Omán a Nový Zéland umožňují využít internetové hlasování pro voliče v zahraničí. Kanada, Austrálie, Švýcarsko či Ekvádor mají zkušenosti s využitím internetového hlasování v regionálních volbách, jak znázorňuje obrázek 7 (International IDEA, 2023).



Obrázek 7: Elektronické hlasování ve světě / vlastní zpracování dle (International IDEA, 2023)

Mezi silné stránky internetového hlasování se dle Ministerstva vnitra ČR (2012) zpravidla uvádí:

- možnost zvýšení volební účasti,
- větší komfort pro voliče,
- větší atraktivita zejména pro mladší voliče,
- eliminace chyb při vyplňování hlasovacích lístků,
- rychlejší zpracování výsledků voleb, pokud je možné hlasovat pouze elektronicky,
- usnadnění hlasování pro voliče v zahraničí,
- usnadnění hlasování pro voliče s hendikepy, jako jsou slabozrací a nevidomí voliči nebo voliči bez končetin.

naopak mezi slabé stránky se zpravidla uvádí (Ministerstva vnitra ČR, 2012) :

- zvýšené riziko ovlivňování výsledků voleb,
- snížení důvěry a ohrožení legitimacy volených orgánů,
- finanční zatížení státního rozpočtu,
- vyšší náklady na zajištění bezpečnosti systému proti manipulacím během i mimo volební období,
- možná nižší transparentnost oproti tradičnímu způsobu hlasování,
- složitější pochopení fungování systému pro běžného občana, který není odborníkem v IT,
- omezené možnosti zpětného přepočítání hlasů v případě soudního přezkumu,

- hrozba tzv. „digitální propasti“ — nerovný přístup k hlasování podle věku a příjmů voliče, zejména pokud by bylo možné hlasovat pouze elektronicky,
- možné narušení principu anonymity voleb.

Obdobné faktory internetového hlasování potvrzuje i studie Licht (2021).

3.1.1 Srovnání možností vzdáleného hlasování

Tabulky 1, 2 a 3 porovnávají korespondenční hlasování poštou a internetové hlasování pomocí elektronického systému pro vzdálenou volbu. Každý srovnávací faktor je hodnocen na úrovni Nízká, Střední, nebo Vysoká podle toho, jak je možné při nejlepší možné míře dosáhnout naplnění daného faktoru.

Srovnávací faktor	Korespondenční hlasování	Internetové hlasování
Příprava voleb	Střední - Snadné zosobnění odevzdat hlas. Ručně psané podpisy je obtížné přesně ověřit nebo nejsou vždy ověřeny.	Vysoká - Použití silného ověřování, jako jsou digitální certifikáty, znamená, že hlasovat mohou pouze oprávnění voliči.
Volební management hlasovacího období	Střední - Správa poštovních hlasů je většinou manuální.	Vysoká - Správa může být automatizována. Pouze správa bezpečnostních opatření (např. správa volebních kryptografických klíčů) by mohla přidat určitou složitost.
Proces sčítání	Střední - Hlasy se musí počítat ručně nebo je volební úředníci musí umístit do optického počítačového zařízení.	Vysoká - Proces počítání je automatizovaný.
Kontrola výsledků voleb	Nízká - Neexistuje žádná záruka, že odevzdaný hlas je přítomen během procesu sčítání. Hlasovací kanál (poštovní službu) je prakticky nemožné kontrolovat.	Vysoká - Voliči si mohou správnost voleb individuálně zkontrolovat na svých účtenkách. Auditoři mohou kontrolovat hlasovací aplikaci.

Tabulka 1: Porovnání požadavků na správu korespondenčního a internetového hlasování (Puiggalí, 2007)

Srovnávací faktor	Korespondenční hlasování	Internetové hlasování
Prevence chyb při hlasování	Nízká - Voliče nelze upozorňovat na nechtěné chyby při hlasování, které mohou zneplatnit jejich hlasy.	Vysoká - Hlasovací aplikace dokáže odhalit jakoukoliv chybu během výběrového procesu a upozornit voliče před tím, než odevzdají svůj konečný hlas. To umožňuje voličům provést příslušné opravy.
Snadnost použití	Střední - Většina voličů zná papírové hlasovací lístky. Mladí voliči mohou mít problém s hlasováním poštou.	Střední - Volební terminály mohou poskytovat intuitivní a snadno použitelné rozhraní voličům s jasnými pokyny. Někteří voliči však tento druh zařízení neznají.
Přístupnost	Nízká - Papírové hlasovací lístky mají vážné problémy u zrakově postižených a některých tělesně postižených voličů. Podpora více jazyků může způsobit problémy s ochranou soukromí.	Vysoká - Používání osobních počítačů usnadňuje interakci zdravotně postiženým voličům. Podpora více jazyků nevyžaduje odevzdání hlasu v tomto jazyce.

Tabulka 2: Porovnání naplnění požadavků použitelnosti korespondenčního a internetového hlasování (Puiggalí, 2007, Martínek, 2024b)

Srovnávací faktor	Korespondenční hlasování	Internetové hlasování
Způsobnost	Střední - Snadné zosobnění odevzdat hlas. Ručně psané podpisy je obtížné přesně ověřit nebo nejsou vždy ověřeny.	Vysoká - Použití silného ověřování, jako jsou digitální certifikáty, znamená, že hlasovat mohou pouze oprávnění voliči.
Soukromí	Střední - Existuje riziko, že obsah poštovních hlasů bude zpřístupněn během jejich přepravy nebo při otevírání poštovních obálek.	Vysoká - Hlasy jsou před odevzdáním zašifrovány. Kryptografická opatření, jako jsou procesy míchání, lze implementovat k přerušení jakéhokoli spojení mezi hlasem a voličem. Voliči mohou chránit svůj počítač před malware.
Integrita	Nízká - Neexistuje žádný způsob, jak prokázat, že odevzdaný hlas zůstane během volebního procesu nezměněn.	Vysoká - Hlasy mohou být digitálně podepsány, čímž se zabrání jakékoliv manipulaci. Navíc při použití potvrzení o hlasování by mohl být jakýkoliv pokus o smazání hlasování odhalen při ověření potvrzení.
Ověřitelnost voličem – během volby	Střední - Existují nástroje pro sledování hlasování zaslaného poštou. Nelze však zaručit, že obálka doručená volebním úředníkům obsahuje stejný hlas odevzdaný voličem.	Vysoká - Ověřovací proces může být implementován jako nezávislý proces na hlasování.
Ověřitelnost voličem – během sčítání	Střední - Volič si může ověřit, že je jeho hlasovací lístek přítomen během procesu sčítání prostřednictvím sledovače hlasovacích lístků.	Vysoká - Potvrzení o hlasování umožňuje voličům jednotlivě ověřit, zda jsou jejich hlasy přítomny v procesu sčítání.
Zabezpečení průběžných výsledků	Střední - Obsah hlasování a tedy průběžné výsledky mohou být přístupné během přepravy.	Vysoká - Hlasy jsou před odevzdáním zašifrovány. Na konci voleb je mohou dešifrovat pouze autorizovaní členové volební komise.
Přesnost volební urny	Střední - Je možné přidat falešné hlasovací lístky bez odhalení. Hlasy mohou být také během přepravy vyloučeny. Ručně psané podpisy lze ověřit, aby bylo možné odhalit masivní podvody.	Vysoká - Každý zašifrovaný hlas může být digitálně podepsán pomocí jedinečného digitálního voličského certifikátu, aby se zabránilo přidávání falešných hlasů. Kromě toho mohou být voličům poskytnuty potvrzení o hlasování, aby mohli zjistit, že jejich hlasy byly odstraněny.
Odolnost nátlaku a odporu ke kupování hlasů	Nízká - Voliči mohou před odevzdáním svých hlasů ukázat vybrané možnosti hlasování třetím stranám, což umožňuje nátlak a prodej hlasů.	Střední - Pokud je volič donucen přítomností korupčníka k ovlivněné volbě, může odevzdat nový hlas později, pokud je povoleno vícenásobné hlasování.
Spolehlivost kanálu	Nízká - Tento hlasovací kanál závisí na spolehlivosti poštovního systému země, ze které se hlasuje. Dostat hlasy po datu uzávěrky není nic neobvyklého a voliči s tím nemohou nic dělat.	Střední - Voliči si uvědomí, že jejich hlas nedorazil k volebnímu orgánu, dojde-li k chybě při odevzdání hlasu. Proto lze použít pohotovostní opatření (např. zkusit hlasovat později nebo použít jiný hlasovací kanál), aby se zabránilo ztrátě jejich hlasů.

Tabulka 3: Porovnání naplnění bezpečnostních požadavků korespondenčního a internetového hlasování (Puiggalí, 2007)

Některé faktory jdou svými požadavky proti sobě, například Odolnost nátlaku a Ověřitelnost se musí určitým způsobem vyvážit, proto vysoká úroveň v obou faktorech najednou je složitě dosažitelná. Na základě provedené komparace vychází, že elektronická volba může být v mnoha ohledech lepší i než korespondenční hlasování, které je přitom umožněno v mnoha zemích nejen Evropské unie.

3.2 Zkušenosti s elektronickým hlasováním

Historicky za první využití hlasovat elektronicky přes Internet v politických právně závazných volbách jsou považovány volby přes e-mail a fax v některých státech USA primárně pro vojenský personál v zahraničí, které jsou považovány za problematické vzhledem k ochraně soukromí (Puiggalí, 2007). Použití systémů pro vzdálené elektronické hlasování začalo po roce 1990, kdy americká federální volební komise vydala volební systémové standardy (FEC, 2002). Vzdálené elektronické hlasovací systémy byly využívány pro primárky politických stran (Martínek, 2024d).

3.2.1 Estonsko

První celonárodní politicky závazné volby s využitím elektronického systému pro vzdálené hlasování proběhly roku 2005 v estonských komunálních volbách. Volbám předcházela potřebná změna legislativy včetně zavedení elektronických občanských průkazů a národního ID pro autentizaci v elektronickém hlasovacím systému (Valimised.ee, 2024a).

V Estonských volbách se zpravidla volí vzdáleně elektronicky sedm dní přede dnem konání papírových voleb, elektronický hlas může odeslat volič vícekrát, platný je poslední odeslaný. Pro hlasování je kromě Internetu potřeba občanský průkaz, mobilní ID nebo digitální doklad totožnosti s platnými certifikáty a PIN kódy. Hlasovat lze pouze pomocí počítače, kde volební program pro autentizaci vyžaduje čtečku karet pro občanský průkaz nebo podporu Mobile-ID na SIM kartě v mobilním telefonu voliče. Volba se provádí pomocí stažené volební aplikace, která automaticky kontroluje způsobilost voliče. Volič může zkontrolovat, zda byl jeho hlas správně předán a přijat pomocí samostatné aplikace pro chytré zařízení po dobu 30 minut od hlasování, kde mu je zobrazen QR kód pro možné ověření. Po ukončení elektronických voleb může volič svůj elektronický hlas přepsat klasickým papírovým hlasováním ve volební místnosti, což výrazně zvyšuje odolnost vůči nátlaku. Při sčítání e-hlasů po skončení papírových voleb se s hlasy provádějí tyto úkony (Valimised.ee, 2024b):

1. Všechna i-hlasování, která musí být anulována z důvodu změny i-hlasů, jsou anulována.
2. Osobní údaje (digitální podpisy) voličů jsou odděleny od elektronických hlasování. Anonymní hlasy se sčítají. I-hlas obsahuje pouze volební identifikátor a registrační číslo kandidáta.

3. I-hlasy se otevírají pomocí klíče pro otevření hlasování. Přístup ke klíči je rozdělen mezi členy Národní volební komise.
4. Sečtou se hlasy a zjišťuje se počet odevzdaných hlasů pro kandidáty.
5. Výsledky hlasování jsou vkládány do volebního informačního systému.

Po sečtení i-hlasů probíhá kontrola integrity systému. Aby bylo sčítání hlasů veřejně ověřitelné, jsou elektronické hlasy smíchány a přeskupeny. Míchání musí být provedeno takovým způsobem, aby dešifrování vstupu i výstupu poskytlo stejný výsledek. V rámci datového auditu kontroluje auditor také neporušenost i-volební schránky, správnost anulování opakovaných hlasování a anonymizaci hlasování. Na stejném základě jako auditor mohou podobné kontrolní postupy provádět také pozorovatelé (Valimised.ee, 2024b).

Bylo spočítáno, že vzdálené elektronické hlasování je nejlevnějším způsobem odevzdání hlasu v estonských volbách (Krimmer, 2018). Elektronické hlasování má v průměru také nižší environmentální dopady než cestování do volebních místností (Willemson, 2023). Estonský volební systém prochází neustálým vývojem (Solvak, 2016), který systém aktualizuje o nová bezpečnostní zjištění před každými volbami.

Od roku 2005 byl v Estonsku elektronický volební systém využit ve 13 celonárodních volbách, v posledních parlamentních volbách 2023 využilo možnost volit vzdáleně elektronicky 51,1 % voličů (Valimised.ee, 2023).

Aktuální verze estonského volebního systému napsaná především v programovacích jazycích Java, Go a Python je z velké části zveřejňována jako open source (Valimised, 2024). Bezpečnostní analýzy estonských voleb (Springall, 2014; Heiberg, 2015a) popisují možná rizika hlasování. Studie (Springall, 2014) ve své kritičnosti požadovala vzhledem k objeveným potenciálním hrozbám systém hlasování ukončit. Studie o volbách (Heiberg, 2015b) z let 2013 až 2015 obsáhle popisovala rizika včetně chyb neplatnosti certifikátu v případě jeho aktualizace v den volby, na druhou stranu uvádí, že k žádnému rozsáhlému útoku nedošlo. Dva ze spoluautorů dané studie byli napojeni na společnost Cybernetica, která se podílela na vývoji estonského systému, proto je nutné zvážit míru nezávislosti dané studie (Marcos del Blanco, 2018a). I aktuální studie poukazuje na riziko porážení individuální ověřitelnosti systému v případě kompromitace voličského zařízení (Pereira, 2023).

Porovnat vývoj volební účasti v prvních digitalizovaných komunálních volbách v Estonsku v roce 2005 a v následujících parlamentních volbách od roku 2007 do roku 2023 lze pomocí tabulky číslo 4. Od roku 2005 byl v Estonsku elektronický volební systém využit ve 13 celonárodních volbách, v posledních parlamentních volbách 2023 využilo možnost volit vzdáleně elektronicky 51,1 % voličů (Valimised.ee, 2023).

Volby	Parlamentní volby 2023	Parlamentní volby 2019	Parlamentní volby 2015	Parlamentní volby 2011	Parlamentní volby 2007	Komunální volby 2005
Oprávnění voliči	966129	887420	899793	913346	897243	1059292
Zúčastnění voliči	613801	565045	577910	580264	555463	502504
Volební účast	63,50%	63,70%	64,20%	63,50%	61,90%	47,40%
I-voliči	313514	247232	176491	140846	30275	9317
I-hlasy nahrazeny papírovým hl. l.	1332	191	162	82	32	30
I-hlasy se počítají	312182	247041	176329	140764	30243	9287
Neplatné i-hlasy	1	n/a	1	n/a	n/a	n/a
Více I-hlasů (nahrazeno I-hlasy)	10787	6340	4593	4384	789	364
I-voliči mezi oprávněnými voliči	32,50%	27,90%	19,60%	15,40%	3,40%	0,90%
I-voliči mezi zúčastněnými voliči	51,10%	43,80%	30,50%	24,30%	5,50%	1,90%
I-hlasy mezi předem hlasy	68,90%	71,40%	59,60%	56,40%	17,60%	7,20%
I-hlasy odevzdané v zahraničí mezi I-hlasy (na základě IP adresy)	7,80%	6,30%	5,70%	3,90%	2,00%	n/a
Počet států i-voličů	100	143	116	105	51	n/a
I-voliči hlasující přes mobile-ID	13993	72305	22084	2690	n/a	n/a
Mobile-ID I-hlasy mezi všemi I-hlasy	4,50%	29,20%	12,20%	1,90%	n/a	n/a
Podíl I-hlasů, které byly ověřeny voličem	5,50%	5,30%	4,30%	n/a	n/a	n/a
Věk i-voličů 16-17	n/a	n/a	n/a	n/a	n/a	n/a
Věk i-voličů 18-24	24569	18191	14727	14851	3394	932
Věk i-voličů 25-34	55005	53781	44692	39013	9692	3104
Věk i-voličů 35-44	66269	55000	42070	33438	7063	2252
Věk i-voličů 45-54	63043	48750	32738	25752	5206	1595
Věk i-voličů 55-64	48947	37614	23277	17195	3029	844
Věk i-voličů 65-74	32930	21197	11870	7445	1270	382
Věk i-voličů > 75	22751	12699	7117	3152	621	208
Pohlaví i-voličů Muži	141105	112538	83560	65396	15681	5061
Pohlaví i-voličů Ženy	172409	134694	92931	75450	14594	4256

Tabulka 4: Statistiky prvního internetového hlasování a parlamentních voleb v Estonsku (Valimised.ee, 2023)

3.2.2 Norsko

V Norsku probíhal rozvoj elektronických voleb v letech 2008 až 2014, kdy nová konzervativní vláda rozhodla o jeho ukončení (Marcos del Blanco, 2018a). Zkušenost je vhodná ke studiu především díky své transparentnosti od přípravy a zadání projektu, přes organizaci, až po následné kroky, díky zapojení nezávislých odborníků a postupným fázím zavádění (Nore, 2013). Díky transparentní veřejné soutěži

v angličtině (Ministry of Local Government and Regional Development, 2010) si lze stále prostudovat zadávací podmínky včetně nabídek dodavatelů, kde nakonec zvítězilo konsorcium ErgoGroup a ScytL. Dodatečná podmínka na otevřený zdrojový kód umožnila ministerstvu provést technickou analýzu systému, která objevila zranitelnosti při generování nezabezpečených náhodných hodnot a používání nedostatečně dlouhých klíčů (Bjørstad, 2013). V systému došlo k distribuci rolí aktérů (Esteve, 2012; The Carter Center, 2014). Jako ochrana proti nátlaku systém umožňoval opakované hlasování včetně následného papírového hlasování, zvýšený podíl elektronicky hlasujících voličů starších devadesáti let ovšem naznačuje, že mohlo dojít k narušení tajnosti hlasování ve spojitosti s možným ovlivněním ze strany rodiny. Veřejně financovaný vývoj systému podpořil vylepšení některých kryptosystémů jako je ElGamal (Gjøsteen, 2013) nebo integraci ověřitelnosti mixnetů (Wikström, 2007; Cortier, 2012). I další studie našly potenciální hrozby (Koenig, 2013; Kubjas, 2017). I když v parlamentních volbách 2013, kde byl elektronický systém použit formou pilotu ve 12 municipalitách, ve kterých bylo odevzdáno více než 70 tisíc elektronických hlasů představujících 36,4 % hlasujících, nebyly objeveny žádné útoky na systém, došlo v roce 2014 k ukončení pilotního projektu (Ministry of Local Government and Modernisation, 2014; Marcos del Blanco, 2018a).

3.2.3 Austrálie

V Austrálii, kde je hlasování povinné, se přistupuje k vývoji elektronických hlasovacích systémů postupnými kroky pomocí lokálních pilotních projektů — nejdříve v roce 2007 pouze pro australské ozbrojené síly v zahraničí, později ve volbách australského státu Nový Jižní Wales, kde hlasovací systém iVote společnosti ScytL v roce 2015 zpracoval 280 tisíc hlasovacích lístků, kdy mohli hlasovat zrakově či tělesně postižení voliči a ti, kteří bydleli více než 20 km od volební místnosti, či v den voleb byli mimo stát (Burton, 2015; Marcos del Blanco, 2018a). Výzkumníci odhalili bezpečnostní nedostatky daného systému (Halderman, 2015). Od roku 2022 po několika objevených potenciálních rizicích ukončil Nový Jižní Wales možnost hlasovat elektronicky (NSW Electoral Commission, 2023). Pro nevidomé a slabozraké voliče nabízí Nový Jižní Wales možnost hlasovat pomocí telefonického hlasování (NSW Electoral Commission, 2024).

3.2.4 Kanada

Kanada nezavádí systém elektronických voleb centralizovaně (Essex, 2020). Elektronické volby jsou povoleny v rámci komunálních voleb, ovšem konkrétní elektronický volební systém řeší jednotlivé municipality. I když vznikla doporučení, která některé regiony a orgány nechaly zpracovat (Independent Panel on Internet Voting, 2014; Schwartz, 2013), tak nejsou všemi regiony brány v potaz. Problém této distribuční formy zavádění elektronického hlasování a nedostatku koordinace je popsán ve studii Goodman (2014).

Největší zkušenosti v Kanadě s online hlasováním mají obyvatelé státu Ontario (Cardillo, 2018; Cardillo, 2019; Hayes, 2022; Goodman, 2023), kde elektronický volební systém nabízí svým občanům 52 % municipalit a kde jsou elektronické systémy jednotlivých municipalit hodnoceny ve studii Brunet (2023). Data o volební účasti v obcích Ontaria znázorněné tabulka 5.

Název obce	Populace	Dodavatel systému elektronického hlasování	Počet online odevzdaných hlasovacích lístků	Počet voličem ověřovaných hlasovacích lístků hlasovací lístky ověřeny
Arnprior	7504	Voatz	3064	27
Atikokan	2753	Scytl	1140	0
Baldwin	620	Scytl	220	0
Blind River	3472	Scytl	383	0
Centre Wellington	28191	Scytl	9130	0
Greater Madawaska	5232	Voatz	1617	20
Grimsby	23981	Voatz	6096	149
Huron Shores	1664	Scytl	830	0
Ignace	1202	Neuvote/ Smartmatic	725	N/A
LaSalle	30180	Scytl	6868	8
Manitouwadge	1937	Scytl	841	0
Marathon	3273	Scytl	1044	0
Markham	328966	Scytl	64864	2504
McNab / Braeside	6786	Voatz	2629	25
Quinte West	46560	Simply Voting	10587	N/A
Red Lake	1260	Simply Voting	1730	N/A
Sables-Spanish River	3214	Scytl	1093	0
West Lincoln	12559	Voatz	2467	72
West Perth	6963	Voatz	2761	14
Woolwich	25006	Scytl	5283	2
Vaughan	306233	Scytl	36641	617

Tabulka 5: Obce Ontaria s individuální ověřitelností ve volbách v roce 2022 (Goodman, 2023)

Poměrně vysoké procento volební účasti online je pravděpodobně způsobeno velkou vzdáleností volebních místností pro mnoho voličů. Garnett (2021) odvodil, že čím větší vzdálenost od volební místnosti, tím je menší účast na hlasování ve volební místnosti. Internetové hlasování také podporuje domorodé komunity (Budd, 2019).

3.2.5 Spojené státy americké

Spojené státy americké jsou první zemí na světě, která umožnila již roku 1986 hlasovat vzdáleně s možností využití pošty, faxu a následně i e-mailu či webové

stránky (Marcos del Blanco, 2018a). Pravomoc volby daného způsobu mají jednotlivé státy, které musí nabídnout tuto možnost občanům UOCAVA, což jsou občané USA, kteří jsou aktivními členy uniformovaných služeb, námořní pěchoty, pověřených sborů veřejné zdravotnické služby nebo Národní správy oceánů a atmosféry, jejich způsobilí rodinní příslušníci, či občané USA s bydlištěm mimo Spojené státy (FVAP, 2015). Pro využití online hlasování se zpravidla předem musí vzdát nároku na tajnost hlasování (Hastings, 2011). Původní systém SERVE hodnotili na bezpečnostní hrozby akademici (Jefferson, 2004). Státy Arizona, Colorado, Missouri a Západní Virginie používají elektronické volební systémy, 27 států má kombinaci pravidel umožňujících hlasovat e-mailem nebo faxem a zbylých 20 států umožňuje pouze zaslání hlasovacích lístků poštou. Stát Aljaška umožňuje využít této možnosti i voličům na území státu (EAC, 2023). Ministerstvo obrany USA pověřilo implementací systému UOCAVA Federální program pomoci při hlasování (FVAP, 2015). Ze skupiny UOCAVA mohli volit elektronicky například v Západní Virginii v roce 2018 nebo přes systém na bázi blockchain ve městě Denver v Coloradu v roce 2019 (Johnson, 2019).

Začátkem roku 2020 kvůli pandemii COVID-19 tři státy USA – Delaware, Západní Virginie a New Jersey — oznámili, že umožní určitým voličům v prezidentských volbách hlasovat online pomocí OmniBallot společnosti Democracy Live. V rámci Delaware se jednalo o voliče nemocné, v karanténě nebo distancující se od společenského kontaktu kvůli riziku nákazy — po prohlášení de facto všichni voliči. Navzdory dobře známým rizikům internetového hlasování tento systém nikdy nepodstoupil veřejný, nezávislý, bezpečnostní přezkum, jenž nakonec provedla studie od Specter (2021).

3.2.6 Francie

Francie nabízí po pilotním projektu v roce 2003 možnost hlasovat přes internetový volební systém voličům žijícím v zahraničí od roku 2006 (Marcos del Blanco, 2018a; Ministère de l'Europe et des Affaires étrangères, 2023). Systém pro vzdálené hlasování ve Francii musí splňovat doporučení CNIL týkající se bezpečnosti elektronických poštovních hlasovacích systémů, zejména prostřednictvím internetu (La Commission nationale de l'informatique et des libertés, 2019). V roce 2014 využilo možnosti odevzdat hlas online 43,21 % voličů při volbách konzulárních delegátů (Dandoy, 2021).

3.2.7 Švýcarsko

Švýcarsko má bohatou tradici v oblasti internetového hlasování v politických volbách, která sahá až do roku 2003. Jedním z charakteristických rysů Švýcarska je silný systém přímé demokracie, který občanům umožňuje účastnit se různých hlasování, včetně referend, několikrát do roka (Marcos del Blanco, 2018a). Švýcarsko

je známé svou výraznou decentralizací, kdy si jednotlivé kantony samy určují způsoby hlasování. Švýcarsko je také průkopníkem v regulaci internetového hlasování, zejména od doby, kdy bylo v roce 2014 zavedeno nařízení spolkového kancléře o elektronickém hlasování (VEleS). Toto nařízení, zejména jeho revize (The Swiss Federal Chancellery, 2018), podrobně popisuje nejen bezpečnostní požadavky na systém, ale také požadavky na procesy kolem používání e-volby. Zvláště důležité jsou požadavky týkající se transparentnosti, například požadavek, že „Každý je oprávněn zkoumat, upravovat, kompilovat a spouštět zdroj pro vědecké účely a psát a publikovat o něm studie“ (Haines, 2022).

V minulosti bylo využíváno několik různých modelů elektronického hlasování, které byly uplatněny v různých kantonech. Mezi nejvýznamnější patřil systém CHVote s otevřeným zdrojovým kódem (Haenni, 2017), který byl podporován kantonem Ženeva, a proprietární systém sVote, který byl vytvořen společností Scytel a Swiss Post. Verze 1.0 protokolu sVote, která předcházela současnému systému švýcarské pošty (Die Schweizerische Post, 2024), byla v provozu od roku 2016 do roku 2019. Tento systém od svého zrodu poskytoval individuální ověřitelnost, čehož chtěl dosáhnout pomocí techniky zvané hlasování s návratovým kódem. V rámci švýcarských volebních systémů s návratovým kódem dostal každý volič před volbami papír s náhodnými tajnými ověřovacími kódy pro každého kandidáta. Volič poté hlasoval online zaškrtnutím své volby na webové stránce a prohlížeč mu jako odpověď zobrazil kódy, které se měly shodovat s kódy na jeho papírovém listu. To mělo umožnit odhalení škodlivého hlasovacího klienta, pokud by došlo ke změně volby voliče. sVote 2.1 byl představen v roce 2018 a byl navržen tak, aby poskytoval také univerzální ověřitelnost. sVote 2.1 prošel certifikačním procesem až do zveřejnění systému, kdy externí odborníci objevili velké množství chyb, které ovlivnily všechny aspekty bezpečnosti systému, od soukromí až po ověřitelnost. Po těchto zjištěních byl systém vyřazen z používání (Culnane, 2019). Systém elektronického hlasování Švýcarské pošty se neustále zlepšuje a postupně opravuje problémy, které zdědil od sVote (Haines, 2022). Podle Haines (2022) tak systém nebyl ještě kompletní a stále se objevovaly významné bezpečnostní problémy.

Pro švýcarské kantony platí federální nařízení o elektronickém hlasování (The Swiss Federal Chancellery, 2022). V roce 2023 zahájily zkušební elektronické hlasování kantony Basel-Stadt, St.Gallen, Thurgau a Graubünden (E-Voting Informationsplattform der Kantone, 2023). Švýcarská pošta informuje o využívaném systému elektronického hlasování transparentně na webu, kde je dostupné i demo aplikace (Swiss Post, 2024).

3.2.8 Další státy

Mezi další státy, které je nutné v rámci problematiky vzdáleného elektronického hlasování zkoumat, patří Rusko a Spojené arabské emiráty, které nabízejí možnost

hlasovat online v celonárodních volbách. Možnost celonárodního hlasování je schválena i v Ekvádoru, který toho zatím nevyužil. V Rusku, které není bráno jako demokratická země (Freedom House, 2023), studie prokázala prolomitelnost tamního hlasovacího systému založeného na Ethereum blockchain a šifrování ElGamal (Gaudry, 2020). Ruský online systém pro volby budí obavy z manipulace i prolomení tajnosti hlasování (Toepfl, 2018; Romanov, 2020; Epifanova, 2021; Sauer, 2021; Schlauffer, 2021; The Bell, 2024). Spojené arabské emiráty volí pouze do poradního orgánu, který nemá významné pravomoci. Historicky lze zvažovat i zkušenosti z Finska (Volkamer, 2009), Nového Zélandu a dalších zemí. Podrobněji zkušenosti z různých zemí rozebírají další publikace (Brunclík, 2014; EU, 2023).

3.3 Standardizace

Mezinárodní standardizace v rámci elektronických volebních systémů postupuje velmi pomalu. O vytvoření základních norem se snažila skupina IEEE VSSC 1622 pod vedením Johna Wacka (Wack, 2014). V USA platí směrnice VVSG pro systém dobrovolného hlasování (EAC, 2024).

Obecně ohledně bezpečnosti provozovatele a použité infrastruktury lze požadovat splnění standardů Mezinárodní organizace pro normalizaci, kam patří především ISO 27001 ohledně bezpečnosti informací, kybernetické bezpečnosti a ochraně soukromí v rámci systémů řízení bezpečnosti informací (ISO, 2022). V případě využití cloudových služeb se lze také zaměřit na ISO 27017 (ISO, 2015a) a ISO 27018 (ISO, 2019). Mezi další související standardy může patřit ISO 9001 (ISO, 2015b) ohledně systému managementu kvality zahrnující i dodržování zákonných norem.

Protože je práce zpracována v České republice, lze za respektovatelné standardy považovat také související vydané dokumenty Rady Evropy. Mezi ně patří také dokument pro certifikaci elektronických volebních systémů (Council of Europe, 2011). Evropská komise vydala sborník informací (EU, 2023).

3.3.1 Doporučení CM/Rec(2017)5 výboru ministrů členským státům o standardech pro elektronické hlasování

Základním legislativním dokumentem Rady Evropy pro internetové hlasování je Recommendation CM/Rec(2017)5 of the committee of ministers to member states on standards for e-voting (Council of Europe, 2017). Doporučení sice není pro členy závazné, ale předpokládá se jeho dodržování. Dobrovolně doporučení přijaly Norsko a Švédsko, v Estonsku se na doporučení odvolal Nejvyšší soud a v Belgii bylo doporučení použito jako měřítko při hodnocení elektronického hlasování (Rodríguez-Pérez, 2022a).

V mnoha ohledech jsou definované požadavky doporučení vyšší, než jsou na již v zemích EU běžně používané korespondenční hlasování.

Doporučení CM/Rec(2017)5 (Council of Europe, 2017) obsahuje 49 norem, které jsou podrobněji vysvětleny v doplňujících pokynech. Nahrazuje také doporučení (Council of Europe, 2004), které po systémech elektronického hlasování vyžaduje, aby byly bezpečné, spolehlivé, účinné, technicky robustní, otevřené nezávislému ověřování a snadno dostupné voličům. Ke staršímu doporučení Rady Evropy z roku 2004 existuje i český překlad od Ministerstva vnitra (Gronwaldtová Wagnerová, 2010).

3.3.2 Směrnice Výboru ministrů o používání informačních a komunikačních technologií (ICT) ve volebních procesech v členských státech Rady Evropy - CM(2022)10

V roce 2022 bylo vydáno nové doporučení v rámci pokynu Výboru ministrů pro použití informačních a komunikačních technologií (ICT) ve volebních procesech v členských státech Rady Evropy - CM(2022)10 (Council of Europe, 2022), které má řešit všechna ostatní využití ICT ve volbách, s výjimkou elektronického hlasování a elektronické kampaně (Driza Maurer, 2023).

3.4 Způsoby hlasování dle možností výběru

V každých volbách je určen volební systém, podle kterého se rozhoduje, jaká varianta či kandidát uspěje. Volba volebního systému je klíčová pro legitimitu a výsledky volebního procesu. Každý systém výběru varianty hlasování, který může být využit i v rámci elektronického hlasování, lze převést na matematický model (Marcos del Blanco, 2018a). Mezi hlavní varianty hlasování lze zařadit (Marcos del Blanco, 2018a):

- *Ano/Ne* - voliči vybírají mezi dvěma možnostmi, obvykle kladnou či zápornou odpovědí. Výhodou je jednoduchost a jasnost výsledků, nevýhodou omezená schopnost vyjádřit složitější preference (Bowler, 2007).
- *1 z N* - voliči vybírají jednu variantu z určitého množství variant. Výhodou je jednoduchost pro voliče a snadné sčítání hlasů, může ovšem vést k nespravedlivé reprezentaci, pokud je množství variant velké (Cox, 1997).
- *M z N* - voliči vybírají M variant z N možných, kde M je větší nebo rovno 1 a menší nebo rovno N ($M \geq 1$ a $M \leq N$). Výhodou je, že umožňuje širší reprezentaci voličských preferencí, nevýhodou je složitější sčítání a vyšší nároky na pochopení systémů voliči (Felsenthal, 1998).
- *M z N s kladnými a zápornými hlasy* - voliči vybírají M^+ kladných variant, které podporují, a současně M^- záporných variant, které nepodporují, z N možných, kde M je větší nebo rovno 1 a menší nebo rovno N ($M \geq 1$ a $M \leq N$). Výhodou je vyšší míra vyjádření preferencí, omezení negativních kandidátů a podpora konsensuálních kandidátů. Mezi nevýhody patří složitost systému,

administrativní náročnost a zvýšené riziko negativních kampaní (Brams, 2007).

- *M z N s určením pořadí* - voliči vybírají M variant z N možných a seřazují je dle preferovaného pořadí ($M \geq 1$ a $M \leq N$). Výhodou je detailní vyjádření voličských preferencí a menší riziko ztracených hlasů, nevýhodou je komplexní proces sčítání a vyšší nároky na vzdělání voličů (Tideman, 2006).

Každý z uvedených volebních systémů nabízí různé možnosti pro vyjádření voličských preferencí. Ano/Ne hlasování je jednoduché a přímočaré, avšak omezuje schopnost voličů vyjádřit složitější názory. Systémy s více možnostmi (1 až N, M až N, a M až N s určením pořadí) poskytují větší flexibilitu a reprezentativnost, ale zároveň zvyšují složitost procesu jak pro voliče, tak pro organizátory voleb (Marcos del Blanco, 2018a).

3.4.1 Alternativní volební systémy

Alternativní volební systémy nabízejí různé přístupy k tomu, jak voliči mohou vyjádřit své preference a jak jsou tyto preference přetaveny do volebních výsledků. Tyto systémy často usilují o překonání nedostatků tradičních volebních metod, jako je například jednoduchý většinový systém (Brams, 2007). Rozvíjející se způsoby alternativního hlasování také přidávají další varianty hlasování, mezi které patří negativní hlasy, bodové hodnocení nebo určování vah hlasu.

3.4.2 Povinné hlasování

Povinné hlasování popisuje Birch (2009) jako volební systém, který vyžaduje účast voličů ve volbách jako občanskou povinnost. Tento systém se používá v několika zemích po celém světě a jeho cílem je zvýšit volební účast a zajistit, že výsledky voleb budou reprezentativnější pro celou populaci. Mezi země se zkušenostmi s povinným hlasováním se řadí Austrálie, Belgie, Brazílie či Singapur. Mezi výhody povinného hlasování se řadí zvýšená volební účast, lepší reprezentativnost, omezení extremismu, posílení občanské povinnosti. Naopak mezi nevýhody povinného hlasování se řadí narušení osobních svobod voličů, účast voličů s nízkou informovaností o kandidátech, administrativní náročnost a zvýšené riziko protestních hlasů. I nevolit nikoho je určité vyjádření vůle, proto pro všechny varianty by měla zůstat možnost odevzdání prázdného/neplatného hlasu.

3.5 Legislativa

Volební legislativa se liší v každém státě, následující text se zaměřuje na právo v rámci České republiky.

3.5.1 Volební právo v Česku

V České republice je plnohodnotné využití vzdálené elektronické volby výjimkou. V Česku ji používá pro organizování personálních voleb přes Internet pro své členy Česká pirátská strana, která používá systém Helios kombinovaný s vlastními silami vyvinutými systémy a dalším open source softwarem (Martínek, 2022; Martínek, 2024d).

Český právní řád nevylučuje možnost konat personální volby do orgánů institucí, společností, družstev apod. vzdáleně pomocí online nástrojů. Každá soukromá či veřejná instituce si proto může upravit své stanovy tak, aby mohla elektronickou volbu využít. Zákonem (Zákon č. 247/1995 Sb., 1995) jsou regulovány volby do Poslanecké sněmovny, které použití vzdálené elektronické volby vylučují. Obdobné zákony jsou i pro volby do zastupitelstev krajů, obcí, do Evropského parlamentu a k volbě prezidenta.

Ústava ČR stanovuje v čl. 18 odst. 1, že „volby do Poslanecké sněmovny se konají tajným hlasováním na základě všeobecného, rovného a přímého volebního práva, podle zásady poměrného zastoupení“ (Poslanecká sněmovna Parlamentu ČR, 1992). Mezi ústavní zásady volebního práva pro právně závazné politické volby v České republice dle definic Poslanecké sněmovny Parlamentu ČR (2016) patří:

- **Všeobecnost** – všichni zletilí občané ČR mají právo volit bez ohledu na rasu, barvu pleti, národnost, jazyk, pohlaví, náboženství, politické názory, sociální původ, majetek, rod či jiné postavení.
- **Rovnost** – každý volič má jeden hlas a váha všech hlasů je stejná. Předpokladem je, že každého člena Parlamentu volí téměř stejný počet voličů.
- **Přímost** – volba se provádí přímo voličem bez možnosti zastoupení.
- **Tajnost** – voliče nelze spojit s odevzdaným hlasem, což znamená, že hlasování musí být tajné.

Volby v Česku tedy musí být tajné a přímé. Výzvou je zajistit, aby volby byly tajné i v domácím prostředí, kde může docházet k ovlivňování voličů, například rodiči (Kupková, 2013). Již dnes v papírových volbách se stává, že člen rodiny donutí jiného člena rodiny hlasovat pro konkrétní vybranou volbu tím, že jde s ním do volební místnosti, kde dohlédne, že si nevezme náhradní volební lístky a za plentou bude mít pouze jeden volební lístek z domova. Řešení pro zmírnění výše uvedených problémů u elektronických voleb existuje v podobě možnosti opakovaného hlasování, případně i zachování možnosti papírové volby po skončení elektronického hlasování.

Obdobný problém může nastat u podmínky přímosti hlasování, protože v nekontrolovaném prostředí je obtížné garantovat, že skutečně hlasoval oprávněný volič (Kupková, 2013). Na druhou stranu není v mnoha zemích přímost ústavní podmínkou, aby byla možná volba v zastoupení. Volba v zastoupení je proces, který

umožňuje voliči delegovat své hlasovací právo na jinou osobu, která za něj hlasuje v jeho nepřítomnosti. Tento systém je v některých zemích zaveden jako způsob, jak usnadnit účast na volbách těm, kteří se nemohou osobně dostavit k volební urně. Například v Belgii, Francii a Nizozemsku je volba v zastoupení legální a běžně používaná (Karp, 2001).

Naopak všeobecnost při zachování i možnosti papírové volby mohou elektronické volby zlepšit, protože se zlepší dostupnost voleb pro osoby s handicapem či žijícím v zahraničí.

V České republice se volí tradičním způsobem pomocí papírových volebních lístků. Ve volební místnosti jsou zpravidla přítomni členové volební komise. Hlasující vyplňuje hlasovací lístek v soukromí za plentou a obálku s vloženým hlasovacím lístkem odevzdává do zapečetěné hlasovací urny před zraky členů volební komise. Alternativně lze volit do vyžádané přenosné volební urny, kterou k voliči přináší minimálně 2 členové volební komise. Do volební komise má právo nominovat člena každá z volených stran. Po ukončení hlasování provádějí manuální sčítání hlasů členové volební komise. Výsledky v dané komisi zadává tajemník volební komise prostřednictvím počítače zpravidla na flash disk, který následně převáží do sčítacího centra dané matriky, tam jsou již výsledky zadány do online systému Českého statistického úřadu, který poté agreguje a zobrazuje dané výsledky veřejnosti. ČSÚ všechna data zpracovává centrálně pomocí databázového systému ORACLE (EU, 2023).

Rozdílnou kapitolou jsou volby v soukromých společnostech, organizacích, stranách, spolcích a jiných institucích. Politické strany a hnutí si vytváří v rámci vnitrostranické demokracie vlastní interní předpisy. Strany a hnutí musí ovšem dodržet zákon o sdružování v politických stranách a v politických hnutích (Česká republika, 2024a), který vyžaduje, aby strany a hnutí měly demokratické stanovy a demokraticky ustanovené orgány. V případě voleb akademického senátu vysokých škol definuje zákon o vysokých školách (Česká republika, 2024b), že volba má být přímá a tajná. Vysokých škol se také týká zákon o přístupnosti internetových stránek a mobilních aplikací (Česká republika, 2019b). Soukromé společnosti či družstva se řídí zákonem o obchodních společnostech a družstvech (Česká republika, 2012). Podmínky hlasování musí zajistit ověření totožnosti hlasující osoby a určení podílů nebo akcií spojených s hlasovacím právem. Tyto podmínky určuje společenská smlouva nebo stanovy a jsou uvedeny v pozvánce na valnou hromadu nebo v návrhu rozhodnutí. V případě družstva má každý člen při hlasování 1 hlas a tajné hlasování je obecně povoleno. U společností s ručením omezeným je tajné hlasování vyloučeno v některých případech, například když zákon vyžaduje jmenovité uvedení hlasujících společníků v notářském zápisu. Tajné hlasování je vyžadováno při volbě a odvolávání členů dozorčí rady z řad zaměstnanců. Všechny subjekty poté musí dodržovat předpisy ohledně ochrany osobních údajů voličů v rámci nařízení GDPR (EU, 2016),

které do českého práva implementuje zákon o zpracování osobních údajů (Česká republika, 2019a).

3.5.2 Digitální základy pro celonárodní internetové hlasování v Česku

Česká republika prochází v rámci digitalizace postupným vývojem. Zákonem o elektronické identifikaci (Česká republika, 2023) byla zřízena Digitální a informační agentura (DIA), která metodicky zastřešuje digitalizaci veřejné správy. Provoz Datových schránek zajišťuje pro DIA Česká pošta, s. p. Pod DIA také spadá Portál občana, který je hlavním portálem zastřešující digitální služby státu. Mezi tyto služby spadá například Žádost o voličský průkaz, ePetice či eDoklady (DIA, 2024). Pro přihlášení do portálů veřejné správy se využívá Identita občana, která zahrnuje i možnosti státem kontrolovaného přihlášení přes Mobilní klíč, NIA ID nebo eObčanku (Identita občana, 2024). DIA sídlí v prostorách státního podniku Státní pokladna Centrum sdílených služeb (SPCSS), který spadá pod Ministerstvo financí a poskytuje především služby provozu IT od zajištění infrastruktury, OS, databáze, až po provoz vlastních datových center (SPCSS, 2024). Pod Ministerstvo vnitra spadá Národní agentura pro komunikační a informační technologie, s. p. (NAKIT) zajišťující komunikační a informační služby pro veřejnou správu a podporu a rozvoj eGovernmentu (NAKIT, 2024). DIA také zapsala Správu státních služeb vytvářejících důvěru, s. p. o. na seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru (SSSVD, 2024). Všechny jmenované instituce by pravděpodobně byly zapojeny do případné implementace celonárodního elektronického systému pro vzdálené a tajné hlasování v Česku.

Dalším významným zákonem v této oblasti je Zákon o kybernetické bezpečnosti (Česká republika, 2014). V současné době se připravuje (NÚKIB, 2024) jeho změna s ohledem na implementaci směrnice NIS2 (EU, 2022). V souvislosti s daným zákonem je třeba aplikovat i další prováděcí předpisy, mezi které patří Vyhláška o regulovaných službách, Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, Vyhláška o Portálu NÚKIB a požadavcích na vybrané úkony, Vyhláška o nepominutelných funkcích (BDŘ), Vyhláška o bezpečnostních pravidlech a Vyhláška o úrovních cloud computingu (Procházková, 2024).

3.6 Kryptografie

Kryptografie je klíčovým prvkem tajného elektronického vzdáleného hlasování, a proto je důležité ji podrobněji prozkoumat.

Symetrická kryptografie využívá stejný klíč pro šifrování i dešifrování dat, který je nutné bezpečně předat oběma stranám. Mezi nejpoužívanější symetrické algoritmy

patří DES, 3DES, RC5, AES a IDEA (Marcos del Blanco, 2018a). K bezpečnému předání symetrického klíče lze využít asymetrickou kryptografii (Stallings, 2020).

Základem je hashovací funkce, kdy $enc(m) = hash$, kde se pro šifrování (enc) může využít například hashovací funkce SHA-1, SHA-2, MD-4, MD-5 apod., která ze vstupu (m) vytvoří hodnotu $hash$, u které se předpokládá, že má zanedbatelnou pravděpodobnost, že bude rekonstrukce vstupní hodnoty bez znalosti klíče vypočítána v polynomiálním výpočetním čase (Marcos del Blanco, 2018a). Mezi vlastnosti kryptografických hashovacích funkcí patří:

- **Determinismus** - kryptografická hashovací funkce vždy pro stejný vstupní řetězec generuje stejný výstupní hash, což zajišťuje konzistenci při použití hash funkce pro kontrolu integrity dat (Krawczyk, 1997).
- **Jednosměrnost** - je prakticky nemožné zpětně rekonstruovat vstupní data z hash hodnoty bez znalosti původního vstupu. Tato vlastnost je kritická pro zabezpečení hesel a dalších citlivých informací (Rivest, 1992).
- **Uniformita** - výstupy hashovací funkce by měly být rovnoměrně rozloženy po celém možném rozsahu hodnot, což znamená, že každá hodnota hash by měla být generována s přibližně stejnou pravděpodobností, což snižuje pravděpodobnost kolizí (Dworkin, 2015). Kryptografická hashovací funkce by měla být navržena tak, aby bylo velmi nepravděpodobné, že dvě různá vstupní data vytvoří stejný hash (kolize). Tato vlastnost je důležitá pro zabezpečení digitálních podpisů a certifikátů (Wang, 2005).
- **Definovaný rozsah** - výstup hashovací funkce má pevně stanovenou velikost, bez ohledu na velikost vstupních dat. To usnadňuje manipulaci a použití hash hodnot v různých aplikacích (NIST, 2015).
- **Citlivost na vstupy** - malá změna vstupních dat by měla způsobit výrazně odlišný hash výstup (lavinový efekt), což zvyšuje bezpečnost tím, že ztěžuje odhadování vstupních dat z hash hodnoty Schneier (2015).

Nicméně, hashovací funkce čelí bezpečnostním rizikům, jako jsou kolizní útoky, kde dvě různé vstupní hodnoty produkují stejný hash (Wang, 2005). Alternativou může být použití náhodného orákula, kde hashovací procesy provádí orákulum po bezpečném přijetí vstupu (Bellare, 1993), což má také svá rizika (Coron, 2005).

Asymetrická kryptografie, známá také jako kryptografie s veřejným klíčem, používá dvojici kryptografických klíčů: jeden veřejný a jeden soukromý (Marcos del Blanco, 2018a). Tyto klíče jsou propojeny jednosměrnou funkcí, která znemožňuje použití stejného klíče pro šifrování i dešifrování. Asymetrická kryptografie umožňuje nejen důvěrnost komunikace, ale i autentizaci a ověření identity pomocí digitálních certifikátů (Roeder, 2007). Nejznámějším algoritmem je RSA od autorů Rivesta, Shamira a Adlemana, jehož bezpečnost je založena na obtížnosti faktorizace velkých čísel (Rivest, 1978). Výpočetní složitost je hlavní nevýhodou asymetrické

kryptografie, což vedlo k rizikovým praktikám pro snížení náročnosti, které ohrožily standardy jako RSA a TLS (Diffie, 1976).

Kryptosystém RSA je jedním z nejpoužívanějších asymetrických algoritmů a je založen na předpokladu, že faktorizace velkých celých čísel je výpočetně náročná (Rivest, 1978). RSA používá klíče o délce mocniny dvou a je široce přijímán pro svou bezpečnost (Roeder, 2007). Podle Národního institutu standardů a technologie ministerstva obchodu USA je doporučeno používat klíče délky minimálně 2048 bitů, přičemž klíče délky 3072 bitů nebo delší se doporučují pro aplikace vyžadující dlouhodobou bezpečnost (NIST, 2020). V České republice určuje minimální požadavky NÚKIB (2023), který již považuje 2048 za dosluhující délku a nově vyžaduje délku 3072 bitů a více.

Používání kratších klíčů, jako je 1024 bitů, se považuje za nedostatečné, protože je zranitelné vůči pokročilým útokům, včetně těch založených na kvantovém výpočtu. Délka klíče 4096 bitů poskytuje ještě vyšší úroveň bezpečnosti, avšak s výrazně vyššími výpočetními nároky, což může být nepraktické pro některé aplikace. Proto by délka klíče měla být pečlivě zvolena s ohledem na konkrétní požadavky a prostředí, ve kterém je kryptosystém nasazen (Lenstra, 2006; Schneier, 2015).

Šifrování veřejným klíčem

Šifrování pomocí veřejného klíče má tři hlavní algoritmy (Marcos del Blanco, 2018a):

- *Gen* - generování veřejného (pk) a soukromého klíče (sk):

$$Gen(1^k) \rightarrow (pk, sk) \quad (16)$$

- kde 1^k je bezpečnostní parametr

- *Enc* - šifrování textu m pomocí veřejného klíče pk pro získání zašifrovaného textu (Ψ)

$$Enc(pk, m) \rightarrow \Psi \quad (17)$$

- *Dec* - dešifrování Ψ pomocí soukromého klíče (sk) pro získání m

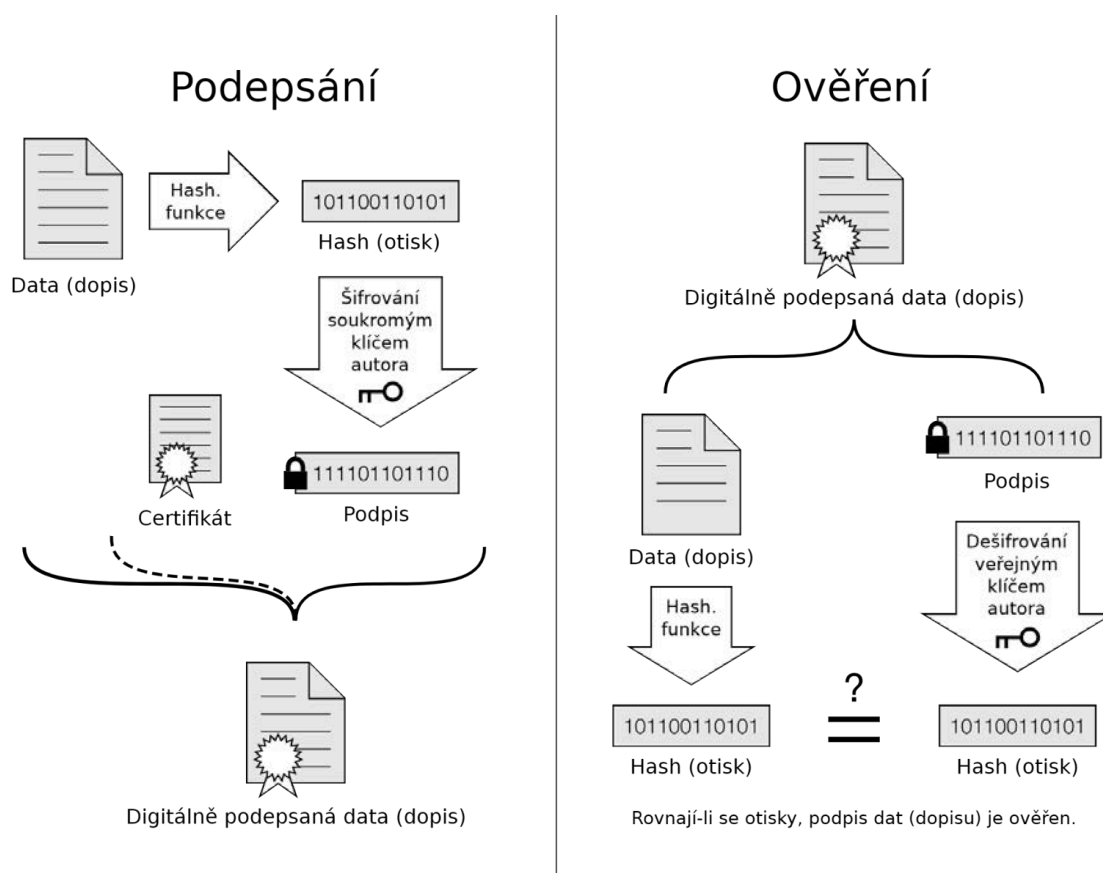
$$Dec(sk, \Psi) \rightarrow m \quad (18)$$

Šifrování veřejným klíčem čelí různým bezpečnostním hrozbám, včetně útoků CCA (Chosen-Ciphertext Attack) a nahrazení veřejného klíče. Útoky CCA zahrnují situace, kdy útočník může získat dešifrované texty pro vybrané zašifrované texty a použít tuto informaci k odhalení původní zprávy (Herzberg, 1997). Útok nahrazení veřejného klíče nastává, když útočník nahradí veřejný klíč oběti svým vlastním

veřejným klíčem. Poté může dešifrovat zprávy určené pro oběť a opět je zašifrovat svým soukromým klíčem (Halevi, 1999; Marcos del Blanco, 2018a).

Digitální podpis

Digitální podpis je základním nástrojem pro ověřování autorství a integrity zpráv v digitálním prostředí. Při použití digitálního podpisu je zpráva podepsána soukromým klíčem odesílatele a příjemce ji může ověřit pomocí veřejného klíče odesílatele (Rivest, 1978). Tento proces zajišťuje, že zpráva nebyla během přenosu změněna a že skutečně pochází od daného odesílatele. Nicméně, pokud útočník získá přístup k soukromému klíči odesílatele, může vytvářet falešné podpisy a tím zneužít důvěryhodnost odesílatele (Marcos del Blanco, 2018a). Schéma fungování digitálního podpisu znázorňuje obrázek 8.



Obrázek 8: Schéma podepsání a ověření digitálního podpisu (ToOb, 2009)

Digitální podpisový systém se skládá ze tří hlavních algoritmů (Rivest, 1978; NIST, 2023; Marcos del Blanco, 2018a):

1. Generování klíčového páru

- Tento algoritmus generuje dvojici klíčů: veřejný klíč (pk) a soukromý klíč (sk). Bezpečnostní parametr 1^k určuje úroveň bezpečnosti a

pravděpodobnostní prvek K zajišťuje, že klíče jsou generovány bezpečným a náhodným způsobem.

$$Gen(1^k, K) \rightarrow (pk, sk) \quad (19)$$

2. Podpisový algoritmus

- Algoritmus podpisu vytváří podpis σ pro danou zprávu m pomocí soukromého klíče sk a veřejného klíče pk . Tento podpis zajišťuje autentizaci a integritu zprávy.

$$\Sigma(pk, sk, m) \rightarrow \sigma \quad (20)$$

3. Ověřovací algoritmus

- Ověřovací algoritmus V používá veřejný klíč pk k ověření platnosti podpisu σ na zprávě m . Tento proces zahrnuje použití hashovací funkce k porovnání původního hash s hash, který je výsledkem dešifrování podpisu veřejným klíčem.

$$V(pk, m, \sigma) \rightarrow \{true \mid false\} \quad (21)$$

V rámci elektronických voleb se používají tři hlavní kryptografické techniky (Kho, 2022) pro zajištění anonymity voliče, konkrétně se jedná o homomorfní šifrování, mixnety a slepé podpisy.

3.6.1 Homomorfní šifrování

Homomorfní šifrování umožňuje provádět matematické operace na zašifrovaných datech bez jejich dešifrování. Tento princip je zásadní pro systémy vzdáleného elektronického hlasování, protože umožňuje práci se zašifrovanými hlasy přímo bez nutnosti jejich jednotlivého dešifrování (ElGamal, 1985; Marcos del Blanco, 2018a).

Schémata (Kho, 2022) jsou buď částečně homomorfní (ElGamal, 1985; Paillier 1999), kde lze provádět pouze operace sčítání, nebo plně homomorfní (Gentry, 2009), kde lze provádět sčítání i násobení.

Pro vzdálené elektronické volební systémy je nejdůležitější vlastnost součtu hlasů — tedy *aditivní homomorfní systém*. V případě aditivního homomorfismu je ve fázi sčítání získán zpět součet hlasů (v) bez jejich jednotlivého dešifrování (Cohen, 1985; Benaloh, 1994; Cramer, 1997; Hirt, 2000):

$$Enc(v_1 + v_2) = Enc(v_1) \cdot Enc(v_2) \quad (22)$$

Naopak *multiplikativní homomorfní systém* ve fázi sčítání dešifruje hlasovací lístek, aby získal součin hlasů, který se následně faktorizuje pro získání hlasů (Peng, 2004).

Sdílení tajemství

K tomu, aby jednotlivec nemohl sám dešifrovat data, se využívá systém sdílení klíčů více aktéry (Shamir, 1979; Blakley, 1979). Prahové schéma sdílení klíčů Shamir (1979) založené na polynomiální interpolaci se používá i v hlasovacích systémech, přičemž je nutné klíč bezpečně uložit každým akterem (Marcos del Blanco, 2018a).

Benaloh (1987) definuje implikaci složených podílů šifrování jako: nechť $\oplus$ a $\otimes$ jsou libovolné binární operace na prvcích tajné domény S a sdílené domény T . Říkáme, že (k, n) prahové schéma má vlastnost $(\oplus, \otimes)$ -homomorfní, pokud pro všechna I platí:

$$s = F_I(t_{i,1}, t_{i,2}, \dots, t_{i,k}) \quad (23)$$

$$s' = F_I(t'_{i,1}, t'_{i,2}, \dots, t'_{i,k}) \quad (24)$$

pak

$$s \oplus s' = F_I(t_{i,1} \otimes t'_{i,1}, \dots, t_{i,k} \otimes t'_{i,k}) \quad (25)$$

Kryptosystém ElGamal

Kryptosystém dle vývojáře HP Tahera ElGamala definuje standard využívaný elektronickými volebními systémy pro vzdálenou volbu (ElGamal, 1985; Katz, 2007; Li, 2014; Marcos del Blanco, 2018a):

Předpokládejme, že máme skupinu G s $|G| = q$. Veřejný klíč je (G, q, g, h) , kde g je generátor G a $h = g^x$, kde x je soukromý klíč.

Šifrování hlasu v je následně $Enc(v) = (g^r, v \cdot h^r)$ pro náhodné $r \in \{0, 1, \dots, q-1\}$

Pro dva zašifrované hlasy v_1 a v_2 :

$$Enc(v_1) = (g^{r_1}, v_1 \cdot h^{r_1}) \quad (26)$$

$$Enc(v_2) = (g^{r_2}, v_2 \cdot h^{r_2}) \quad (27)$$

je homomorfní vlastnost (28):

$$Enc(v_1) \cdot Enc(v_2) = (g^{r_1}, v_1 \cdot h^{r_1}) \cdot (g^{r_2}, v_2 \cdot h^{r_2}) = (g^{r_1+r_2}, (v_1 \cdot v_2) \cdot h^{r_1+r_2}) = Enc(v_1 \cdot v_2)$$

K dosažení aditivní homomorfní vlastnosti v kryptosystému ElGamal se obvykle používá upravená verze, která přijímá součet. Šifrování hlasování je v tomto případě $Enc(v) = (g^r, p^v \cdot h^r)$ pro náhodné $r \in \{0, 1, \dots, q-1\}$, kde p je další nezávislá (od g) generátoru G . Pro dva zašifrované hlasy v_1 a v_2 (ElGamal, 1985; Katz, 2007; Marcos del Blanco, 2018a):

$$Enc(v_1) = (g^{r_1}, p^{v_1} \cdot h^{r_1}) \quad (29)$$

$$Enc(v_2) = (g^{r_2}, p^{v_2} \cdot h^{r_2}) \quad (30)$$

je aditivní homomorfní vlastnost (31):

$$Enc(v_1) \cdot Enc(v_2) = (g^{r_1}, p^{v_1} \cdot h^{r_1}) \cdot (g^{r_2}, p^{v_2} \cdot h^{r_2}) = (g^{r_1+r_2}, p^{v_1+v_2} \cdot h^{r_1+r_2}) = Enc(v_1 + v_2)$$

Pokud součet $v_1 + v_2$ není příliš velký, lze diskretní algoritmus $p^{v_1+v_2}$ vyřešit a získat součet dvou hlasů v_1 a v_2 , což umožňuje sčítání hlasů bez nutnosti jejich dešifrování.

Kryptosystém Paillier

Paillierův šifrovací systém, vyvinutý Pascalem Paillierem (1999), je další pravděpodobnostní šifrovací funkce pro kryptografické systémy s veřejným klíčem, která podporuje homomorfní vlastnosti (Li, 2014).

Paillierova homomorfní vlastnost předpokládá, že veřejný klíč je modulo m a základ je g . Šifrování je definováno jako (Paillier, 1999; Katz, 2007; Li, 2014; Marcos del Blanco, 2018a):

$$Enc(x) = g^x r^m \bmod m^2 \quad (32)$$

pak pro náhodné r platí $r \in \{0, 1, \dots, q-1\}$.

Pro dva zašifrované hlasy v_1 a v_2 :

$$Enc(v_1) = g^{v_1} r_1^m \quad (33)$$

$$Enc(v_2) = g^{v_2} r_2^m \quad (34)$$

platí následující homomorfní vlastnost (35):

$$Enc(v_1) \cdot Enc(v_2) = (g^{v_1} r_1^m) \cdot (g^{v_2} r_2^m) = g^{v_1+v_2} (r_1 r_2)^m = Enc(v_1 + v_2 \bmod m)$$

Mezi další kryptosystémy s homomorfní vlastností patří RSA s podporou multiplikativního homomorfismu (Rivest, 1978), kryptosystém Goldwasser-Micali (Goldwasser, 1984) a další. Se zvyšujícím se výkonem kvantových počítačů se stávají kryptografické systémy založené na výpočetní složitosti méně bezpečné (Xu, 2011). Na tuto hrozbu tak musí nově reagovat i schémata a kryptografická primitiva využívaná v elektronickém hlasování. Jedním z navrhovaných řešení může být *plně homomorfní šifrovací schéma*, které má umožnit vyhodnocení hlasů nad zašifrovanými daty aniž by je bylo možné dešifrovat (Gentry, 2009). Na základě inspirace systémy Helios a Belenios byla navržena konstrukce plně homomorfního šifrování LWE s využitím mřížek (Chillotti, 2016; Marcos del Blanco, 2018b).

3.6.2 Mixnety

Mixnety jsou kryptografické směrovací protokoly představené Davidem Chaumem (1981), které používají posloupnost proxy serverů ke zvýšení anonymity komunikace. V elektronickém hlasování se mixnety využívají k anonymizaci hlasů tím, že znesnadňují spojení mezi hlasem a voličem. Proces funguje následujícím způsobem (Chaum, 1981; Marcos del Blanco, 2018a):

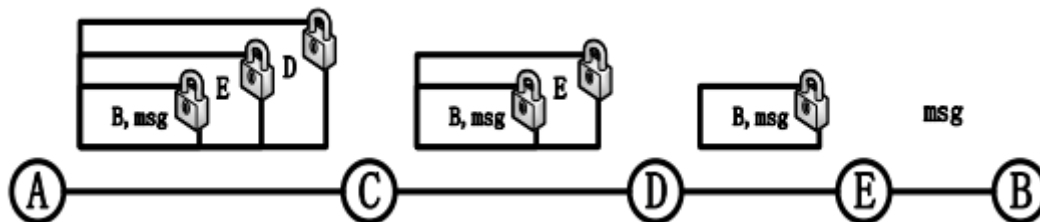
1. **Zašifrování hlasu:** Každý volič zašifruje svůj hlas pomocí veřejného klíče volební komise.
2. **Míchání hlasů:** Zašifrované hlasy jsou poslány do série mix serverů. Každý mix server hlasy náhodně přeskupí, znovu je zašifruje a předá dalšímu příjemci, kterým může být další mix server.
3. **Dešifrování hlasů:** Po průchodu všemi mix servery je možné hlasy dešifrovat a spočítat.

Každý mix server v rámci mixnetu generuje svůj vlastní pár klíčů — soukromý (sk) a veřejný klíč (pk). Když i -tý uživatel posílá svůj hlas v_i , zašifruje ho všemi veřejnými klíči mix serverů M tak, jak formalizuje následující zápis (Sampigethaya, 2006; Li, 2014; Marcos del Blanco, 2018a):

$$v_{enc} = Enc_{pk_1}(r_1, Enc_{pk_2}(r_2, Enc_{pk_3}(\dots Enc_{pk_k}(r_i, v) \dots))) \quad (36)$$

Každý mix přijímá skupinu zpráv, které náhodně přeskupí a poté jako výstup vrací v novém pořadí. Před vstupem do mixnetu je zpráva zašifrována pomocí veřejných klíčů všech mixů, kterými bude procházet v opačném pořadí. Každý mix pak dešifruje jednu vrstvu, jak znázorňuje obrázek 9 (Lin, 2016). Pouze poslední cílový mix může zprávu plně dešifrovat a přečíst. Základními požadovanými vlastnostmi mixnetů jsou (Lin, 2016):

1. **Správnost:** Výsledek mixu musí být správný, což je zaručeno, pokud všechna poctivá mixcentra plní svou funkci.
2. **Soukromí:** Zajištění anonymity odesílatele zprávy, pokud jsou splněny určité podmínky.
3. **Robustnost:** Systém je schopný odhalit a zmařit jakýkoliv pokus o podvod, pokud jsou splněny specifické podmínky.
4. **Dostupnost:** Systém musí být dostupný i v případě otevřené sítě.
5. **Efektivita:** Systém musí být účinný a fungovat efektivně, což je obecný požadavek na jakýkoliv systém provozovaný v síti.



Obrázek 9: Zpráva procházející množstvím mix serverů v mixnetu (Lin, 2016)

Chaumovo řešení pro mixnety, přestože přináší významné přínosy pro anonymitu komunikace, čelí dvěma hlavním problémům. Prvním problémem je možnost, že jakýkoli mix server může nahradit šifrovaný text jiným šifrovaným textem dle svého výběru, čímž narušuje důvěryhodnost celého systému. Druhým problémem je, že velikost šifrovaných textů roste s každým dalším mix serverem, což vede k vyšší výpočetní náročnosti. Park a jeho kolegové navrhli v roce 1994 re-šifrovací mixnety, kde mix servery využívají homomorfní vlastnosti kryptosystému k re-randomizaci šifrovaných textů namísto jejich dešifrování. Tento přístup zajišťuje, že k dosažení anonymity hlasování je nutný pouze jeden poctivý mix server. Navíc tento způsob snižuje výpočetní zátěž voliče, protože každý server provádí část šifrovacího procesu (Park, 1994; Marcos del Blanco, 2018a).

ElGamal a Paillier jsou dva z kryptosystémů často používaných v mixnetech. Tyto systémy využívají homomorfní vlastnosti, což znamená, že umožňují operace

na šifrovaných datech bez jejich dešifrování. Nicméně nejsou zcela bezpečné proti útokům typu IND-CCA2, což znamená, že je třeba zvážit jejich bezpečnostní omezení při implementaci (Dolev, 1991; Marcos del Blanco, 2018a).

Ověření, zda jsou mix servery poctivé, se obvykle provádí pomocí Zero-Knowledge Proof. **Zero-Knowledge Proof (ZKP)** je kritická metoda v elektronickém hlasování, která umožňuje ověřit správnost operací bez odhalení citlivých informací. ZKP se používá k prokázání, že jednotlivé kroky, jako jsou šifrování, permutace a dešifrování hlasů, byly provedeny správně, aniž by se odhalily samotné hlasy. Například při ověřování permutace a re-šifrování mix serverem může být použit ZKP následujícím způsobem: každý mix server obdrží šifrované hlasy $v_1, v_2, \dots, v_n$ a vytvoří permutované a re-šifrované hlasy $v_{\pi(1)}, v_{\pi(2)}, \dots, v_{\pi(n)}$, kde π je náhodná permutace. Server pak prokáže, že permutované hlasy jsou správně odvozeny od původních, aniž by odhalil π . Tento důkaz může zahrnovat předložení závazků k původním a permutovaným hodnotám a použití homomorfních vlastností k prokázání, že $v_{\pi(i)} = \text{Enc}(m_i, r'_i)$ pro všechny i , kde r'_i je nové náhodné číslo použité při re-šifrování a m je původní nezašifrovaný hlas. Formálně může být takový důkaz vyjádřen jako:

$$\text{ZKP}\{(v_1, \dots, v_n) : \forall i \in \{1, \dots, n\}, v_{\pi(i)} = \text{Enc}(m_i, r'_i)\} \quad (37)$$

Tento přístup zajišťuje, že mix servery nemohou manipulovat s hlasy, aniž by byly odhaleny, čímž se výrazně zvyšuje bezpečnost a důvěryhodnost elektronického hlasování (Feige, 1999; Damgård, 2006; Blum, 2019; Goldwasser, 2019).

Nejdříve Sako a Killian (Sako, 1995) a později Furukawa (2001), Neff (2001) a Jakobsson (2002) pracovali na zlepšení efektivity permutací mixnetů. Nicméně se také objevují publikace nalézající zranitelnosti v těchto systémech (Pfitzmann, 1990; Pfitzmann, 1995; Desmedt, 2000; Mitomo, 2000; Wikström, 2004). Heuristicky bezpečný mixnet systém vyvinutý Puiggalím Allepuzem (2010) byl zpochybněn řadou možných útoků (Khazaei, 2012), což dokazuje, že vývoj v oblasti mixnetů je nepřetržitý a stále probíhá. Elektronické hlasovací systémy založené na mixnetech mají stále problém s tím, že počítání hlasů se provádí hlas po hlasu, na rozdíl od systémů založených čistě na homomorfním šifrování, kde lze počítat bez dešifrování každého hlasu. Současně nemůže počítání začít, dokud není ukončeno odevzdávání všech hlasů (Marcos del Blanco, 2018a).

Výhodou mixnetů oproti čistě homomorfnímu šifrování je, že lze přenést podobu celého hlasovacího lístku, což umožňuje využití mixnetů i u složitějších způsobů hlasování jakými jsou využití pořadí a jiné alternativní hlasovací systémy.

3.6.3 Slepé podpisy

Slepé podpisy jsou kryptografickou technikou, která umožňuje autoritě podepsat zprávu bez znalosti jejího obsahu. Tato technologie byla poprvé představena Davidem Chaumem (1983) a následně aplikována na elektronický hlasovací systém v roce 1992 (Fujioka, 1993).

Formálně může být slepý podpis RSA definován následujícím způsobem (Chaum, 1983; Fujioka, 1993; Li, 2014; Marcos del Blanco, 2018a): nechť (n, e) a (n, d) jsou veřejný a soukromý klíč autority, kde d je inverzní k e modulo $\varphi(n)$ a r je náhodný slepý faktor takový, že $\gcd(r, n)=1$. Volič posílá autoritě svůj hlas v po výpočtu:

$$v' = v \cdot r^e \bmod n \quad (38)$$

Hodnota r se používá k utajení hlasu v před autoritou. Po ověření voliče autorita podepíše utajený hlas následujícím způsobem:

$$S' = (v')^d = (v \cdot r^e)^d = v^d \cdot r \bmod n \quad (39)$$

Tento podepsaný hlas S' je poté zaslán zpět voliči. Volič následně obdrží S' a odkryje jej, aby získal hodnotu S s platným podpisem autority, protože zná r :

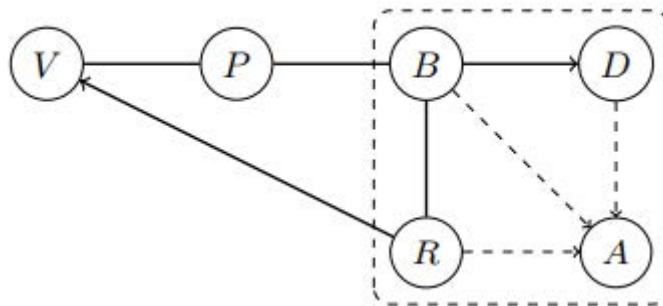
$$S = S' \cdot r^{-1} = v^d \cdot r \cdot r^{-1} = v^d \bmod n \quad (40)$$

Aby se zabránilo zneužití protokolu RSA kvůli jeho homomorfním vlastnostem, je nutné na hlasování v předem aplikovat hashovací funkci. Tato funkce přerušuje spojení mezi voličem a hlasováním, což ovšem ztěžuje zajištění univerzální ověřitelnosti. Kromě toho jsou vyžadovány anonymní a zcela bezpečné kanály pro odesílání hlasů (Bellovin, 2014; Marcos del Blanco, 2018a; Kho, 2022).

3.7 Architektura vzdáleného elektronického volebního systému

3.7.1 Základní schéma vzdáleného elektronického hlasovacího systému

Pro definování volebního schématu v rámci elektronického hlasování existuje několik přístupů (Chaum, 2005; Ryan, 2009; Gjosteen, 2010). Jednoduchou a efektivní definici poskytuje norský volební systém (Gjosteen, 2010; Marcos del Blanco, 2018a):



Obrázek 10: Komunikace mezi aktéry vzdáleného elektronického hlasovacího systému (Gjøsteen, 2010).

Volební systém zahrnuje několik klíčových aktérů, kteří komunikují přes zabezpečené a ověřené kanály. **Volič (V)** používá **volební zařízení (P)**, což může být počítač, mobilní telefon nebo jiné elektronické zařízení určené k interakci s infrastrukturou volebního systému přes Internet. Tato infrastruktura je znázorněna v diagramu jako oblast ohraničená přerušovanou čarou a zahrnuje následující hlavní komponenty:

1. **Volební urna (B)**: slouží k ukládání zašifrovaných hlasovacích lístků.
2. **Generátor účtenek (R)**: generuje sekvenci kódů účtenek pro voliče.
3. **Dešifrovací služba (D)**: zajišťuje dešifrování hlasovacích lístků po ukončení hlasování.
4. **Auditor (A)**: monitoruje a ověřuje celý volební proces, i když není součástí zjednodušeného protokolu.

Postup hlasování:

1. **Výběr hlasu**: volič vybere své možnosti $(v_1, \dots, v_k)$ z množiny možností $O = \{1, 2, \dots\}$.
2. **Vyplnění hlasovacího lístku**: počítač vyplní hlasovací lístky nulami s pevnou délkou k_{max} .
3. **Šifrování**: hlasovací lístek je zašifrován volebním šifrovacím klíčem.
4. **Odeslání do volební urny**: zašifrovaný hlasovací lístek je odeslán do volební urny B .
5. **Generování účtenek**: volební urna spolupracuje s generátorem účtenek R , aby vytvořila sekvenci kódů účtenek ze sady C . Tyto účtenky jsou zaslány přímo voliči. Volič pak ověřuje, zda kódy účtenek odpovídají vybraným možnostem. Pokud je shoda mezi možnostmi a kódy účtenek, volič souhlasí, jinak zjistí, že došlo k chybě.
6. **Uzavření urny a dešifrování**: po ukončení hlasování urna vybere zašifrované hlasovací lístky k dešifrování a odešle je dešifrovací službě D . Celý obsah urny je pak odhalen auditorovi A , který ověřuje správnost a integritu procesu.

Mezi internetové hlasovací systémy pro tajné volby se zveřejněnými zdrojovými kódy, které tak lze hodnotit na základě určitých kritérií, patří Demos, Demos-2, Helios, Belenios, systém švýcarské pošty (SPVS), estonský volební systém (EstVS IVXV), Hyperion, Civitas, CHVote, či Univote (Finogina, 2024).

3.7.2 Schéma vzdáleného elektronického hlasování založené na blockchainu

V poslední době se snaží akademici (McCorry, 2017; Hjalmarsson, 2018; Sheer Hardwick, 2018) navrhnout volební schéma pro vzdálenou elektronickou volbu, které by díky technologii distribuovaných záznamů (DLT) reprezentované blockchainem přineslo výhodu neměnnosti přidáných hlasů do distribuované veřejné elektronické volební urny. Distribuovaně uložené hlasy v blockchainu nelze změnit ani smazat.

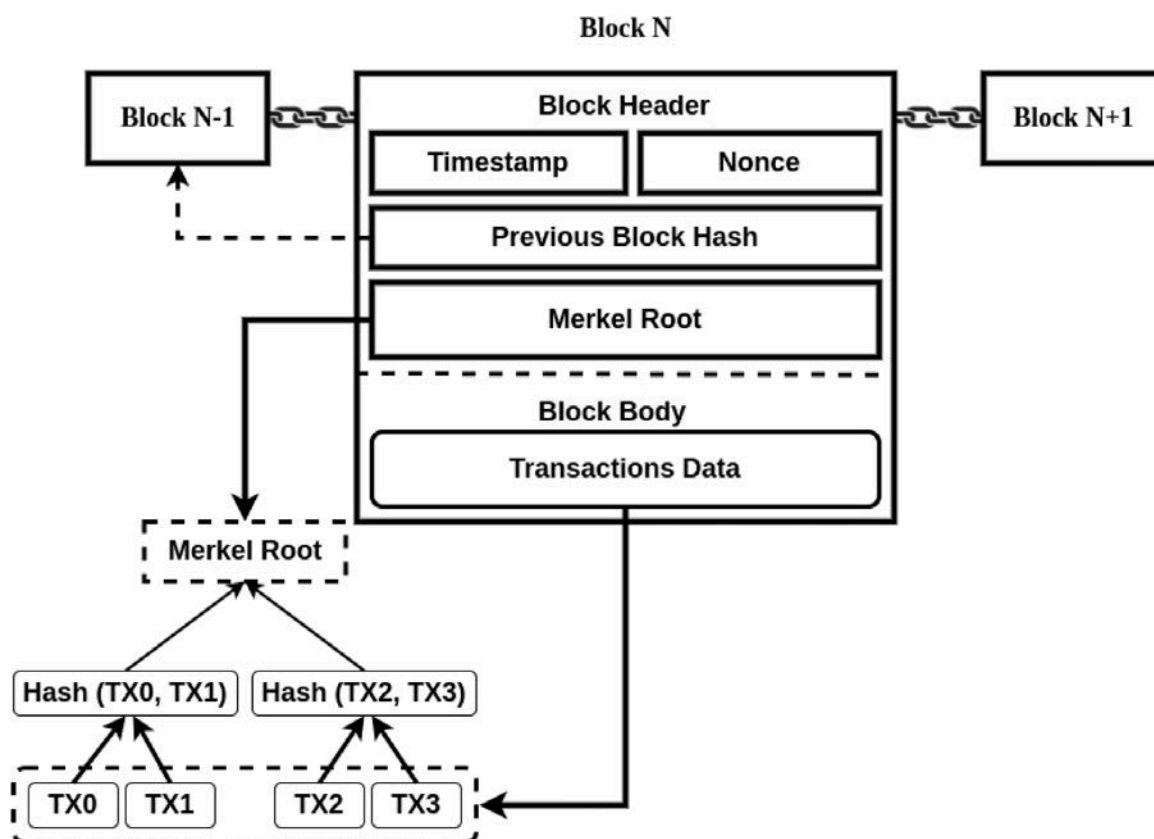
Blockchain, jehož základní koncept byl navržen v roce 1991 (Haber, 1991), je decentralizovaný a distribuovaný systém účetní knihy, který se skládá z řady propojených bloků. Každý blok obsahuje seznam transakcí, přičemž každá transakce zaznamenává určitou událost nebo akci. Hlavička bloku, obsahující hash předchozího bloku, časové razítko, nonce a Merkleho kořen, slouží k identifikaci bloku. Hash předchozího bloku propojuje aktuální blok s tím předchozím, časové razítko potvrzuje data v bloku a přidává čas či datum vytvoření u digitálních dokumentů. Nonce, jedinečné číslo použité jen jednou, je klíčové pro důkaz práce v bloku. Merkleho kořen, což je datová struktura pro různé bloky dat, ukládá všechny transakce v bloku a vytváří digitální otisk celé sady transakcí. Díky této struktuře, znázorněné na obrázku 11, jsou data jednou zaznamenaná v bloku neměnná a bezpečná, protože jakákoliv změna by vyžadovala úpravu všech následujících bloků, což zajišťuje integritu a bezpečnost transakcí v blockchainu (Hajian Berenjestanaki, 2024).

Konsensuální protokoly jsou mechanismy, které umožňují zařazení bloku transakcí do distribuované hlavní knihy v peer-to-peer síti. Tyto protokoly iniciují proces konsenzu mezi uzly, aby se zajistilo, že všechny transakce jsou ověřené a platné. Zároveň zajišťují, že všechny uzly v síti mají identickou kopii účetní knihy (Taş, 2020). Existuje mnoho různých typů konsensuálních algoritmů. Mezi hlavní modely konsensuálních protokolů patří (Hajian Berenjestanaki, 2024):

- **Proof of Work (PoW):** tento často používaný konsensuální algoritmus, například v Bitcoinu (Nakamoto, 2008), zahrnuje řešení výpočetně složitých matematických hádanek členy sítě, známými jako těžaři, což zajišťuje bezpečnost sítě a ověřování transakcí.
- **Proof of Stake (PoS):** tento konsensuální proces vybírá tvůrce bloků (validátory) na základě jejich majetku nebo podílu v síti. Jejich majetek slouží jako záruka, která zajišťuje poctivost a bezpečnost sítě (King, 2012).

- **Proof of Authority (PoA):** tento přístup používá oprávněné subjekty nebo jednotlivce jako validátory bloků. Na rozdíl od jiných metod je PoA založen na předem stanoveném souboru důvěryhodných validátorů, kteří se osvědčili svou spolehlivostí (Kovan, 2017).

Mezi další konsensuální modely patří Byzantine Fault Tolerance (BFT), Practical Byzantine Fault Tolerance (PBFT), Raft consensus algorithm a další (Hajian Berenjestanaki, 2024).



Obrázek 11: Struktura blockchainu (Hajian Berenjestanaki, 2024).

Obecně lze definovat tyto možné zlepšené vlastnosti volebního systému při využití technologie blockchain (Hjalmarsson, 2018; Sheer Hardwick, 2018):

- **Neměnnost:** každý nově navrhovaný blok v blockchain musí navazovat na předešlý záznam. Tím se vytváří nezvratný řetězec, který dal technologii jméno blockchain a chrání integritu již zapsaných dat.
- **Spolehlivost:** blockchain je decentralizovaný a replikovaný na mnoha různých místech, což zvyšuje jeho dostupnost a minimalizuje riziko výpadku jediného místa například zahlcením přes DDoS útok.
- **Distribovaný konsensus:** protokol distribuovaného konsensu stanovuje pravidla pro přidávání nových transakcí do hlavní volební urny. Aby byl nový blok přijat do blockchainu, musí s ním souhlasit většina uzlů v síti.

- **Transparentnost:** konsensuální veřejně přístupná volební urna je rozprostřena po více místech, záznamy mohou být ověřovány nezávislými třetími stranami.

Blockchain (Jafar, 2022) umožňuje využití *intelligentních smluv* (smart contract), což je programovatelný protokol, který umožňuje automatické vykonávání smluvních dohod bez potřeby zásahu třetích stran. Mezi možnosti využití může patřit ověření oprávnění voliče, anonymní registrace hlasu nebo automatické sčítání hlasů (Hjalmarsson, 2018).

Mezi aktuálně používané hlasovací systémy využívající blockchain patří Follow My Vote, Voatz, Votem, POLYAS, Luxoft, DecentraVote, Polys či Agora (Jafar, 2021; Hajian Berenjestanaki, 2024). I když existují návrhy důvěryhodných volebních systémů založených na blockchain (Shahzad, 2019), stále elektronické volby přes blockchain přináší řadu problémů (Park, 2021; Jafar, 2021), mezi které patří potřeba složitější správy a koordinace, menší škálovatelnost, energetická náročnost, složitější upgrade software a oprava chyb. Nové distribuované konsensuální protokoly je obtížné správně implementovat a často trpí kritickými nedostatky kvůli nedostatečnému testování apod. Šifrování ruského volebního systému založeného na blockchainu Ethereum bylo prolomeno (Gaudry, 2020). Na druhou stranu může být využití blockchain řešením vůči riziku prolomení šifrování díky zvyšujícímu se výkonu kvantových počítačů (Gao, 2019; Esgin, 2019) a v éře AI může řešit i jiné možné problémy (Li, 2021).

3.7.3 Techniky autentizace a ověřování identity

V elektronickém hlasování je základem správně ověřit identitu voliče a k volbě připustit pouze přihlášeného voliče, který má právo volit. Obecně lze možnosti autentizace rozdělit podle toho (Matt, 2002; McClanahan, 2024):

- **co volič zná** - například hesla včetně jednorázových (OTP), PIN kódy apod.;
- **co volič umí** - například odpověď na náhodně vygenerovaný kontrolní dotaz;
- **co volič má** - například identifikační karta či jiný dokument, autentizační hardwarové či softwarové tokeny, certifikáty a digitální podpisy, klíče atd.;
- **čím volič je** - například biometrické metody (Jain, 2004) jako otisky prstů, rozpoznání obličeje, skenování duhovky nebo sítnice či hlasová identifikace, nebo behaviorální autentizace založená na monitorování vzorců chování;
- **kde volič je** - například omezení přihlášení dle lokality.

Podrobněji se možnosti autentizace voličů ve stávajících hlasovacích systémech pokusil přiblížit s kolegy Rodríguez-Pérez (2022b). S ohledem na významnost voleb je vhodné při autentizaci používat více autentizačních faktorů v rámci vícefaktorové autentizace — minimálně 2FA — dvoufaktorovou autentizaci.

3.7.4 Fáze volebního procesu vzdáleného elektronického hlasování

Typický internetový volební proces se skládá z těchto fází (U.S. Vote Foundation, 2015):

1. **Příprava:** během přípravy volební úředníci shromažďují všechny potřebné informace pro průběh voleb. To zahrnuje sběr registračních údajů pro všechny voliče, identifikaci volebních možností, tvorbu návrhů hlasovacích lístků (často v několika jazycích) pro všechny volební okrsky, které se účastní voleb, a zasílání pokynů a dalších informací o volbách voličům.
2. **Distribuce:** různé volební systémy používají různé mechanismy pro distribuci hlasovacích oprávnění voličům, jako je pošta, e-mail nebo webová stránka, která poskytuje hlasovací lístky ke stažení. V rámci elektronického hlasování je po registraci nutné zajistit řádnou autentizaci voliče.
3. **Vyplnění hlasu:** voliči vyplňují své hlasovací lístky, často s pomocí softwaru nainstalovaného na jejich vlastních zařízeních.
4. **Odeslání hlasu:** volební úředníci obdrží vyplněné hlasovací lístky. Stejně jako u distribuce se používají různé mechanismy pro vhazování a zabezpečení hlasů.
5. **Sčítání:** fáze sčítání zahrnuje dokončení zbývajících úkolů voleb. Patří sem sčítání hlasů a oznamování výsledků voleb. Některé volební systémy také zahrnují zveřejňování informací potřebných pro audit.
6. **Audit:** jako důkaz integrity voleb by měla být k dispozici možnost nezávislého auditu. Některé volby mohou být sporné, a v takových případech nastává závěrečná fáze, ve které zainteresované strany hledají důkazy o správnosti nebo nesprávnosti výsledku voleb.

3.8 Bezpečnostní rizika

Zabezpečení voleb je klíčovým prvkem, který je nezbytné řešit pro zajištění integrity a důvěryhodnosti celého volebního systému. V případě bezpečnostního incidentu, který ohrožuje integritu voleb, dochází k narušení důvěry veřejnosti v celý systém. Proto je nutné zajistit bezpečnost všech částí systému, kde je to možné. Vzhledem k tomu, že vzdálené elektronické hlasování probíhá přes zařízení voliče, je také nezbytné informovat voliče o možných hrozbách a nutnosti zabezpečit své zařízení i připojení k internetu, aby nedošlo k jejich kompromitaci.

Ve Švýcarsku byly například zavedeny mechanismy pro ověřování výsledků voleb (Galindo, 2015; Germann, 2014). Tyto mechanismy jsou klíčové pro zajištění transparentnosti a důvěryhodnosti voleb.

Útoky na volební systémy jsou klasifikovány v mnoha vědeckých pracích (Mudana, 2005; U.S. Vote Foundation, 2015; Sekibuule, 2007; Zissis, 2011; Wolchok, 2012;

Springall, 2014; Bernhard, 2017; Marcos del Blanco, 2018a; Hajian Berenjestanaki, 2024).

3.8.1 Zranitelnost software

Mezi bezpečnostní slabiny volebního software a technologií použitých na straně serveru mohou patřit zadní vrátka (Marcos del Blanco, 2018a), které umožňují neoprávněný přístup k systému. Pokud by někdo získal neoprávněný přístup, mohl by změnit výsledky voleb, získat citlivé informace o voličích nebo ovládnout celý systém. Zranitelnost software může být vytvořena úmyslně nebo neúmyslně kvůli chybám v programování nebo limitům použitých technologií.

3.8.2 Útoky na klienta voliče

Statistiky ukazují, že až 40 % osobních počítačů je infikováno virem nebo malwarem (U.S. Vote Foundation, 2015). Napadené zařízení může odesílat informace o hlasování třetí straně nebo provádět útoky typu **DoS** (Denial of Service), které znemožní zařízení odevzdat hlas, kdy si neodevzdání hlasu nemusí být volič vědom. V případě norských voleb byla zkoumána možnost útoků na mobilní zařízení voliče, která často postrádají antivirovou ochranu (Koenig, 2013; Marcos del Blanco, 2018a).

3.8.3 Útoky na síťovou infrastrukturu

Útočníci se mohou v rámci vzdálených elektronických systémů snažit zkompromitovat každou část volební infrastruktury která je dostupná online. Volební systémy využívají řadu protokolů klient-server, které jsou vykonávány na různých vrstvách, kde je vše potenciálně ohroženo útokem (Wolchok, 2012; Tsoukalas, 2013; Springall, 2014; Halderman, 2015; Marcos del Blanco, 2018a).

Známým typem je **DDoS útok** (Culnane, 2017), který má za cíl zahltit infrastrukturu systému, aby došlo k selhání systému. Jsou zdokumentovány DDoS útoky na volební systémy, mezi které patří například primárky Demokratické strany v Arizoně roku 2000 (U.S. Vote Foundation, 2015). Infrastruktura volebních systémů by měla být dimenzována na vysoký nápor uživatelů, protože krátké období voleb logicky vede k vysoké zátěži i ze strany voličů. Pokud se jedná o záměrné zatížení systému prostřednictvím DDoS útoku, je možné využít služby třetích stran, které poskytují ochranu proti DDoS útokům snížením rizika výpadku pomocí vlastní silné infrastruktury, skrýváním infrastruktury klienta před útočníky i odrážením útočníků blokováním podezřelých přístupů (Wedos, 2022; Cloudflare, 2009), nebo pomocí vlastní softwarové ochrany, která se snaží eliminovat podezřelý provoz (Fail2ban, 2013; Marcos del Blanco, 2018a).

FREAK útok

V úterý 3. března 2015 výzkumníci oznámili novou zranitelnost SSL/TLS nazvanou útok FREAK, která umožňuje útočníkovi zachytit spojení HTTPS mezi zranitelnými klienty a servery a donutit je k použití oslabeného šifrování, které může útočník prolomit, a tak ukrást nebo manipulovat s citlivými daty. Útok FREAK je možný, když se zranitelný prohlížeč připojí k náchylnému webovému serveru, který přijímá šifrování na úrovni exportu. Servery, které přijímají šifrovací sady RSA_EXPORT, vystavují své uživatele riziku útoku FREAK. V ohrožení je stále více než desetina všech serverů s důvěryhodnými certifikáty prohlížeče (FREAK Attack, 2015; Halderman, 2015; Beurdouche, 2017; Marcos del Blanco, 2018a).

Logjam útok

Logjam je chyba v TLS, která umožňuje man-in-the-middle downgrade připojení na "exportní" Diffie-Hellman. V roce 2015 trpělo touto zranitelností 8,4 % HTTPS webů žebříčku Alexu a 3,4 % všech serverů, které mají certifikáty důvěryhodné pro prohlížeč. V reakci na to se hlavní prohlížeče mění tak, aby odmítaly krátké skupiny umožňující útok Logjam (Adrian, 2015).

3.8.4 Korupce

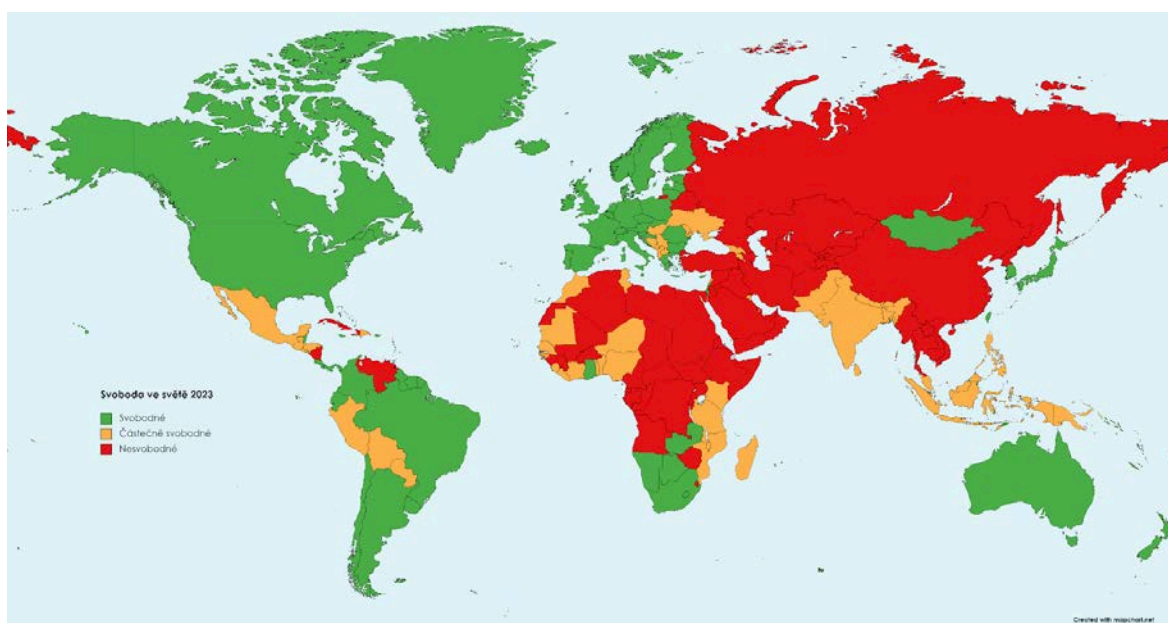
Korupcí je myšleno ovlivňování voličů či jiných aktérů standardně nelegálními způsoby. Může se jednat o tajnou dohodu mezi stranami například pomocí uplácení, nebo-li kupčení s hlasy (Wolchok, 2012). Může se jednat o ovlivňování voliče, který bude volit dle požadavku korupčníka (Martínek, 2024d). Může se jednat o ovlivňování osob zajišťujících bezpečnost sčítání hlasů nebo jinou kritickou část volebního systému. Riziko korupce je přítomno ve všech typech voleb včetně tradičních papírových (Transparency International, 2014). V rámci elektronických systémů pro vzdálené volby je nutné zvažovat odolnost systému proti nátlaku a minimalizovat riziko, že ovlivnění některého z aktérů volebního systému může ohrozit integritu voleb. V případě více volebních komisí typických pro tradiční papírové volby je význam korupce nižší a případný problém spíše izolovaný (Marcos del Blanco, 2018a).

3.8.5 Útoky sociálního inženýrství

V rámci využívání konvenčního hardware a software hrozí útoky na voliče a další aktéry systému prostřednictvím různých metod sociálního inženýrství jako může být **phishing**, **vishing** a podobné. Podle studie je mnohem snazší přesvědčit/oklamat oběť, aby prozradila své heslo, než prolomit systém (Mitnick, 2004; Marcos del Blanco, 2018a). Pro zabezpečení voleb tak je vhodné používat například dvoufaktorové ověření, které snižuje riziko zneužití hesla a prolomení zabezpečení.

3.8.6 Státní manipulace

Závazné politické volby mají významný dopad pro občany dané země. Pokud neexistuje dostatečná transparentnost systému, která umožňuje nezávisle ověřit jeho správné fungování bez narušení integrity ze strany státní moci, nemá takový systém u občanů důvěru (Martínek, 2024e). Manipulace s elektronickým systémem pro volby je proto snazší v nedemokratických zemích, kde by mohlo nastat i to, že celý systém volby pouze simuluje a zobrazuje výsledky, které vyhovují vládnoucí garnituře. Svobodu ve světě znázorňuje obrázek 12.



Obrázek 12: Svoboda ve světě 2023 / vlastní zpracování (Freedom House, 2023)

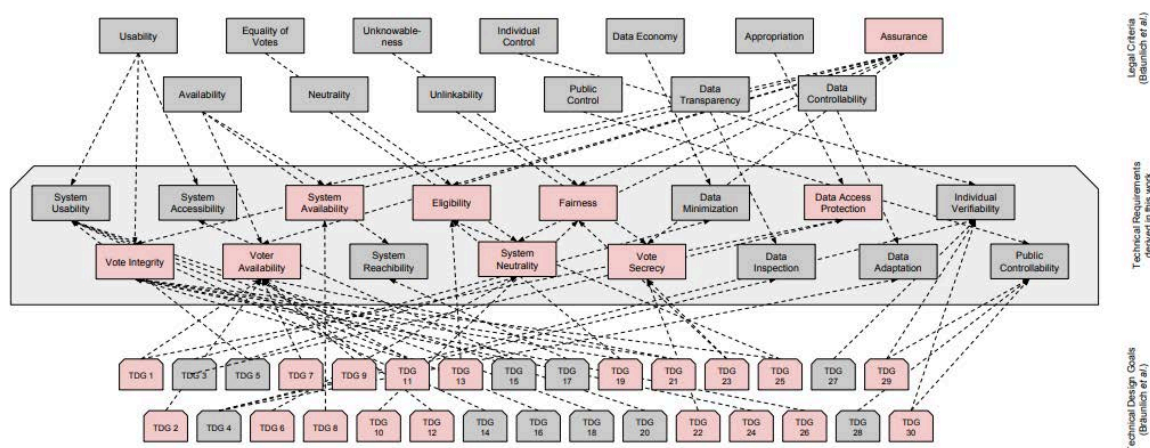
3.9 Koncepty hodnocení systémů pro vzdálenou tajnou elektronickou volbu

Hodnocení elektronických volebních systémů je oproti jiným informačním systémům velmi specifické. Jedná se o multidisciplinární posuzování, kdy kromě technických požadavků je nutné zohlednit i právní, politologické, sociologické a další požadavky.

Základní požadavky na elektronické hlasování definoval na základě ústavních požadavků Gritzalis (2002), právní požadavky na bezpečné e-volby rozvíjí dále v práci Mitrou (2002), později je podrobněji rozebírá s kolegy v souhrnné knize Bezpečnost elektronického hlasování (Gritzalis, 2003). O hodnocení volebních schémat od teoretických po prakticky využitá se pokusili Sampigethaya (2006) a Poovendran. Konkrétně definují obecné bezpečnostní požadavky způsobilost, soukromí, ověřitelnost, bezporuchovost, přesnost, dlouhodobé soukromí, spravedlnost, dále požadavky na nepřátelský protiútok: robustnost, bezúčtenkovost, nepřemožitelnost a požadavky na implementaci systému: škálovatelnost a

praktičnost. Práce Fouard (2007) se snaží kryptograficky hodnotit jednotlivá volební schémata.

Postup pro hodnocení systémů elektronického hlasování navrhli Volkamer (2007) a McGaley, kdy rozdělili požadavky na zajištění, operační a systémové, které dále dělí do kategorií bezpečnost, funkčnost a použitelnost. Později požadavky konkretizuje Volkamer (2009) zvláště pro elektronické hlasovací zařízení s přímým záznamem a pro dálkové elektronické hlasování. Hodnotit bezpečnostní rizika na základě stromu hrozeb navrhl Pardue (2010) s kolegy. Na požadavky v případě využití open cloud computing se zaměřil Zissis (2011). Online hlasovací software dle použité kryptografie srovnává Li (2014).



Obrázek 13: Na základě právnických kritérií (Bräunlich, 2013) odvozené technické požadavky (Neumann, 2016a)

Bräunlich (2013) s kolegy přispěli k hodnocení systémů elektronického hlasování zavedením transformace volebních principů do cílů technického návrhu (TDG). Neumann (2016a) následně identifikoval nedostatky v práci Bräunliche a navrhl technické požadavky na propojení právních kritérií s TDG, což znázorňuje obrázek 13. Neumann (2014; 2016a) odvodil na základě předchozích prací (Sampigethaya, 2006; Moran, 2006; Cetinkaya, 2008; Delaune, 2009; Kremer, 2010; Küsters, 2010) 16 požadavků na internetové hlasovací systémy, které dělí na bezpečnostní (integrita hlasování, dostupnost pro voliče, dostupnost systému, způsobilost, neutralita systému, spravedlnost, utajení hlasování, ochrana přístupu k údajům) a ostatní (použitelnost systému, přístupnost systému, dosažitelnost systému, minimalizace dat, kontrola dat, přizpůsobení údajů, individuální ověřitelnost, veřejná kontrolovatelnost). V práci Neumann (2016b) zmiňuje 12 základních požadavků:

- **Odpovědnost:** systém hlasování zajišťuje, že v případě selhání lze identifikovat a pohnat k odpovědnosti odpovědný subjekt.

- **Odolnost vůči nátlaku:** systém poskytuje mechanismy, které chrání voliče před nátlakem od třetích osob, které by je mohly nutit hlasovat určitým způsobem. Odolnost nátlaku také řeší Achenbach (2015).
- **Způsobilost:** systém zajišťuje, že se do výsledků voleb započítávají pouze hlasy oprávněných voličů.
- **Ověřitelnost způsobilosti:** systém umožňuje pozorovatelům ověřit, že byly započítány pouze hlasy oprávněných voličů.
- **Spravedlnost:** systém neodhaluje úmysly žádného voliče před koncem voleb.
- **Individuální ověřitelnost:** systém umožňuje každému voliči ověřit, že jeho hlas byl správně zaznamenán pro sčítání. Podrobněji řeší Castelló (2016) či Solvak (2020).
- **Dlouhodobé utajení hlasování (tzv. věčné soukromí):** systém chrání úmysly voličů před odhalením, a to i proti silným protivníkům. Řeší například Arapinis (2013).
- **Volnost příjmu:** systém nevydává žádné potvrzení, které by voliči umožnilo prokázat, jak hlasoval. Porušení je chápáno jako vložení nelegitimních hlasů.
- **Robustnost:** systém je schopen vrátit přesný výsledek voleb. Robustnost na základě určení parametru K-resilience navrhla hodnotit Volkamer (2009).
- **Univerzální ověřitelnost:** systém umožňuje každému pozorovateli ověřit, že byly hlasy správně sečteny. Definicemi ověřitelnosti se zabývají práce Benaloh (1987), Juels (2005), Juels (2010), Popoveniuc (2010), Benaloh (2015), Cortier (2015). Více o E2Ev lze nalézt v Příloze A.
- **Integrita hlasování:** systém zajišťuje, že každý hlas je správně zahrnut do výsledků voleb. Porušení je chápáno jako změna hlasu neoprávněnou osobou.
- **Utajení hlasování:** systém nezveřejňuje žádné dodatečné informace o úmyslech voličů mimo konečné výsledky.

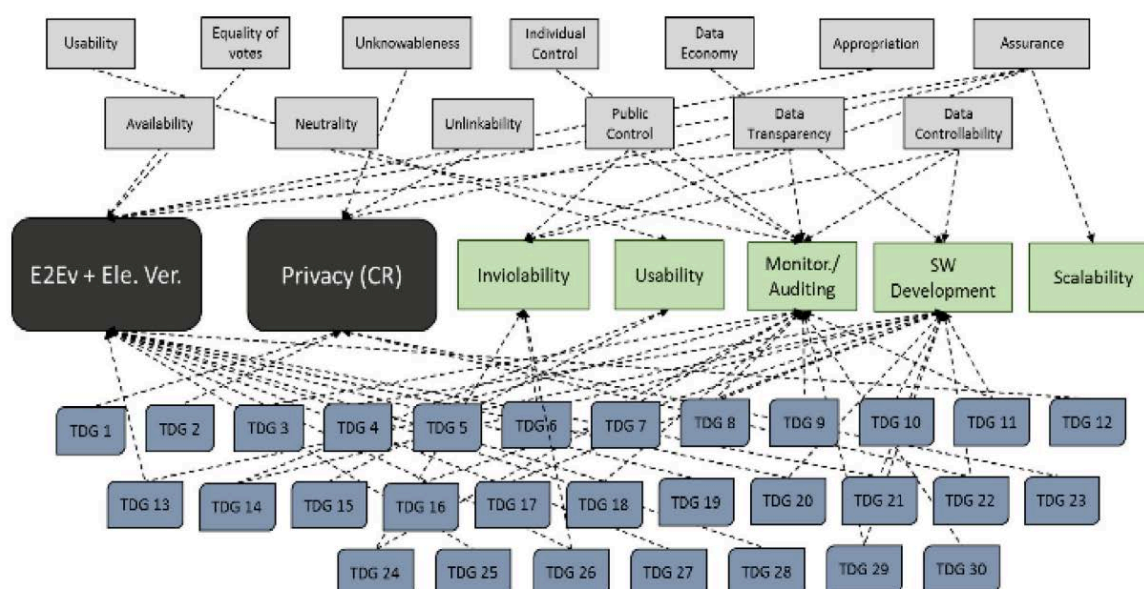
Neumannova vylepšení založená i na implementaci ISO norem (Neumann, 2014) se nadále zvažují, i když metodologie zůstala spíše nástrojem pro simulace než praktickým rámcem pro poskytování hodnotících informací volebním úředníkům.

Porovnáním kryptografických technik se zabývá práce od Kulyk (2016). Neumann (2017) také specifikuje hodnocení bezpečnosti internetových volebních schémat v závislosti na volbách. Na základě Neumannových závěrů připravili Panizo Alonso (2018) s kolegy praktický hodnotící rámec, který má být v souladu s novými (Driza Maurer, 2017) pokyny Rady Evropy pro e-voting (Council of Europe, 2017). Tento komplexní rámec hodnocení (Marcos del Blanco, 2019) zahrnuje následující kroky:

1. **Definice homogenního souboru požadavků na elektronické hlasování:** tento krok zahrnuje integraci různých bezpečnostních standardů jako KORA (Hammer, 1993), CC a ISO 27001-IT Grundschutz (The Common Criteria

Recognition Agreement, 2009), směrnice Rady Evropy (Council of Europe, 2017) a metodiky Neumanna (2016a).

2. **Formální ekvivalence s TDG Bräunlicha (2013):** tento krok zahrnuje porovnání a integraci různých bezpečnostních požadavků.
3. **Konzultace s odborníky:** přes 30 mezinárodních odborníků na elektronické hlasování bylo konzultováno pro přezkoumání rámce hodnocení a přidání váhových faktorů.
4. **Formální definice praktického hodnotícího rámce:** Tento rámec zahrnuje dva sine-qua-non požadavky (end-to-end ověřitelnost a odolnost proti nátlaku) a 73 položek hodnocení.

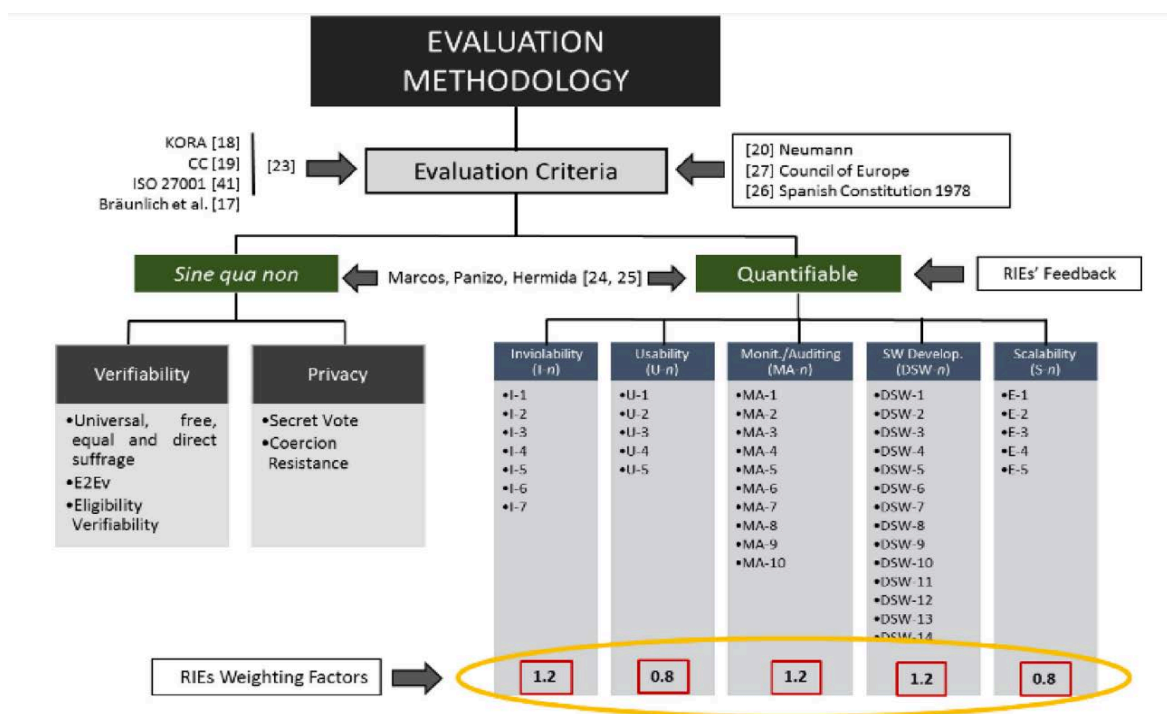


Obrázek 14: Integrace Bräunlich (Bräunlich, 2013) v rámci evaluace Panizo (Panizo Alonso, 2018)

Rámec navržený Panizo Alonsem (2018) obsahuje jak povinné principy, tak kvantifikovatelné tradiční požadavky. Povinné principy zahrnují end-to-end ověřitelnost a odolnost proti nátlaku (Kremer, 2010; Juels, 2010), což odpovídá standardům Rady Evropy pro demokratické volby (Council of Europe, 2017). Tradiční požadavky jsou hodnoceny od 0 do 10 s přesností na jedno desetinné místo. Každá ze 73 měřitelných položek je posouzena jako nevyhovující, částečně vyhovující nebo vyhovující (Marcos del Blanco, 2019).

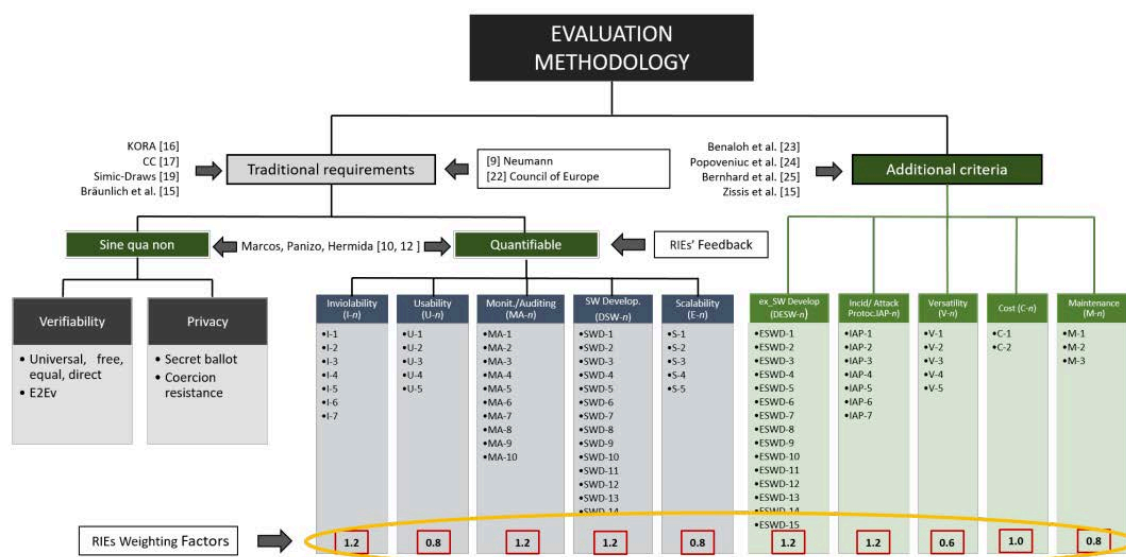
Na základě výzkumů Benaloha, Rivesta, Ryana a Volkamer (Bernhard, 2013; Benaloh, 2015) byla zahrnuta do metodiky Marcos del Blanco (2018a) dodatečná sada pěti požadavků na e-hlasovací systémy. Tyto požadavky byly kodifikovány a rozděleny do konkrétních položek částečným použitím prací Zissis a Lekkas (Zissis, 2014) a novozélandského ministerstva pro vnitřní záležitosti (Te Tari Taiwhenua | Department of Internal Affairs, 2019).

Následující obrázek číslo 15 (Marcos del Blanco, 2019) ukazuje, že existují dva typy kritérií: sine-qua-non, kde end-to-end ověřitelnost a odolnost proti nátlaku (Kremer, 2010; Juels, 2010) představující pět základních principů demokratických voleb podle Rady Evropy (Council of Europe, 2017).



Obrázek 15: Kompletní praktický hodnotící rámec (Marcos del Blanco, 2019)

Hodnocení elektronických hlasovacích systémů v rámci metodiky Marcos del Blanco (2018a) není založeno na číselné hodnotě výkonu, ale spíše na kvalifikovaných označeních. Kritéria jsou hodnocena jako "splněno" (○), "nesplněno" (×) nebo "splněno za určitých podmínek" (Δ). Druhý soubor kritérií zahrnuje kvantifikovatelné tradiční požadavky a doplňková kritéria, která jsou v rámci souhrnných kategorií hodnocena číselně na škále od 0 do 10 s přesností na jedno desetinné místo. Pro výpočet celkové číselné hodnoty se každá ze 73 měřitelných položek klasifikuje jako nevyhovující (×), částečně vyhovující (Δ) nebo vyhovující (○) (Marcos del Blanco, 2019). Kompletní hodnotící rámec znázorňuje obrázek 16.



Obrázek 16: Kompletní praktický hodnotící rámec s přidánými kritérii (Marcos del Blanco, 2019)

Podrobné požadavky definované Marcos del Blanco (2018a) jsou přeloženy v příloze A této práce. Internetové hlasovací systémy zahrnující i technologii blockchain se pokusil obecně hodnotit Alamleh (2021), konkrétní technologie pak hodnotí Hajian Berenjestanaki (2024).

Množství studií se zaměřuje primárně na technickou bezpečnost internetových hlasovacích systémů (Neumann, 2014; Chang-Fong, 2016; Culnane, 2017; Ghonaimy, 2017; Marcos del Blanco 2018), je nutné se ovšem zabývat i provozními, právními, politicko-sociologickými či ústavními aspekty (Schmidt, 2009; Mitrou, 2002; Schwartz, 2013). Šíře vědeckých disciplín dotýkajících se internetového hlasování způsobuje rozdělení výzkumu do technické (Culnane, 2017), právní (Schwartz, 2013) a politologické oblasti (Gabel, 2021). Komplexní hodnocení systémů internetového hlasování by mělo pojmout všechny oblasti. Nelze vynechat ani hodnocení dodržení nařízení o ochraně osobních údajů (GDPR), jak se tomu ve své práci ohledně hlasovacích systémů věnuje Rodríguez-Pérez (2020). Hodnotit internetové hlasovací systémy založené na blockchain se pokusil s kolegy Cucurull (2019), kdy zmiňuje především potřebu bezpečné agregace výsledků v případě vícekanálové možnosti volby.

Kromě kybernetické bezpečnosti samotného softwaru by měly být systémy i-hlasování hodnoceny komplexně z hlediska zajištění integrity celých voleb, jak uvádí Garnett (2020) a James, kteří definují tři základní principy pro hodnocení integrity voleb: příležitosti pro deliberaci, rovnost účasti, robustní kvalita volebního managementu.

Kromě toho existují i další koncepty komplexního hodnocení, které navrhuje Deseriis v rámci digitálních politických stran (Deseriis, 2017; Deseriis, 2019; Deseriis, 2021;

Deseriis, 2023). Pro důkladné zhodnocení je nutné zaměřit se na komplexní hodnocení samotné implementace systému včetně technických standardů, předpisů a naplňování demokratických norem, což výrazně rozšiřuje hodnocení samotného softwaru o hodnocení volební integrity nejen z technologického hlediska. Hodnocení konkrétního případu použití zahrnujícího celý proces volby popisují Von Nostitz (2021) a Sandri, kteří rozdělují analýzu volebních platforem na dvě části: demokratické normy a technické standardy. Demokratické normy obsahují 5 indikátorů, které podle autorů umožňují pochopit limity a možnosti participace na rozhodovacím procesu. Konkrétně se jedná o participaci, reprezentaci, konkurenceschopnost, transparentnost a schopnost reagovat. Technické normy obsahují 4 ukazatele, a to: bezpečnost, proces ověřování a utajení, vlastnictví a kontrola údajů. Pomocí tohoto rámce lze komplexně pochopit digitální demokratický affordance i-hlasovacího systému (Deseriis 2023).

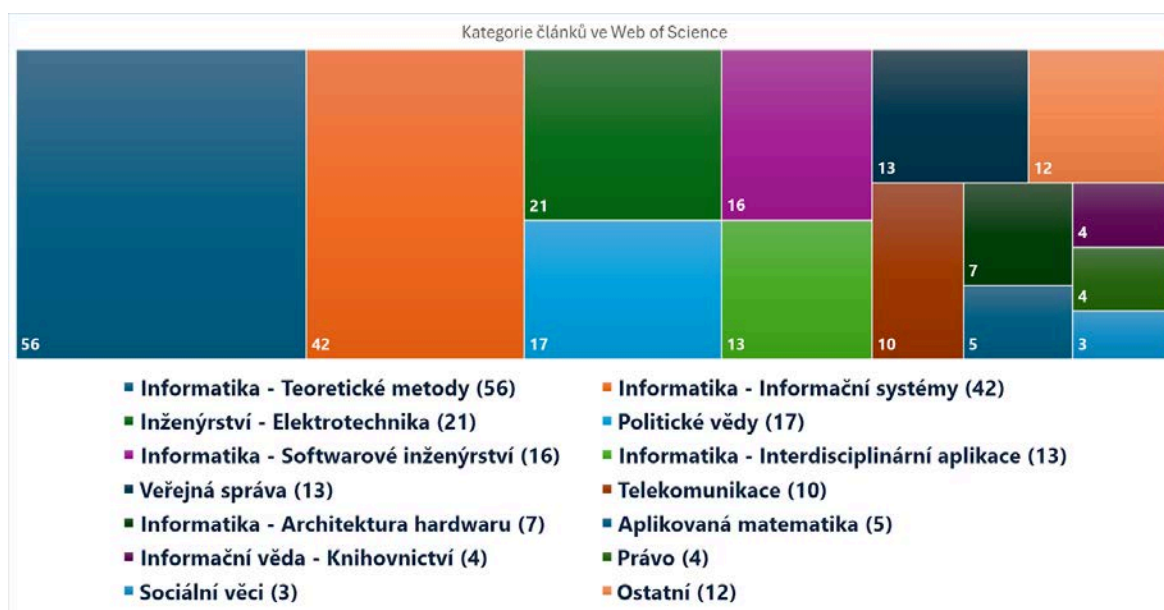
4 Výsledky

Tato kapitola obsahuje výsledky výzkumu autora. Některé výsledky jsou popsány podrobněji mimo tuto kapitolu v přílohách práce. Například navržený metodický postup provedení vzdálené tajné elektronické volby je podrobně rozebrán v článku Martínek (2024e), který je součástí práce v rámci Přílohy I.

4.1 Bibliometrická analýza

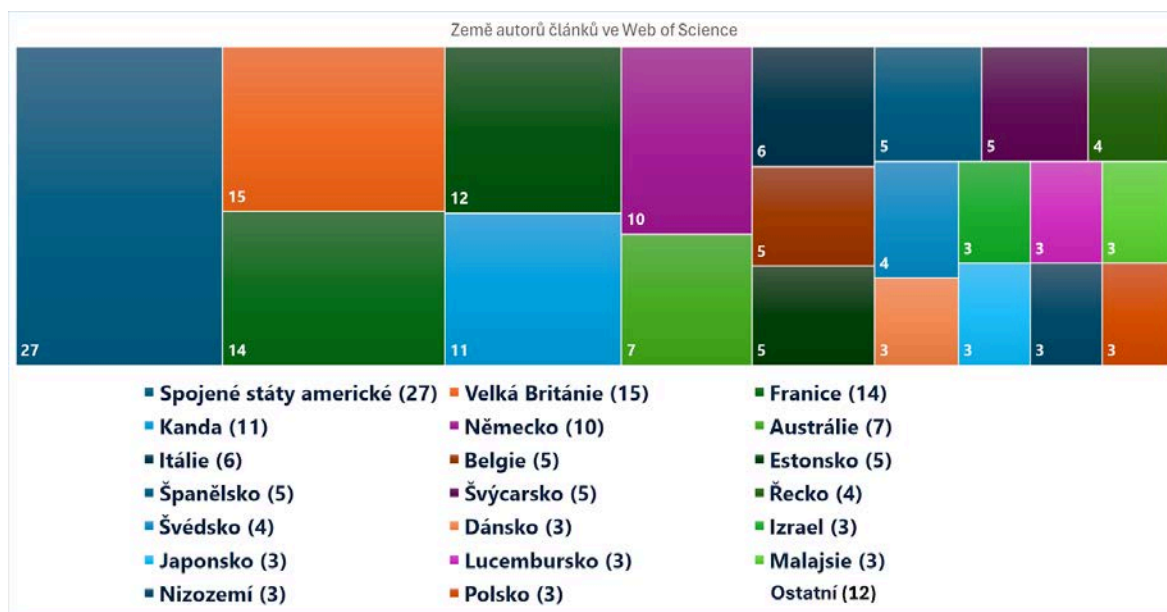
Pro vizualizaci multidisciplinarity problematiky tajných vzdálených elektronických voleb autor analyzoval hlavní zdroje z databáze Web of Science, které mají přímou souvislost s volební kryptografií, internetovými hlasovacími systémy nebo koncepty jejich hodnocení. Konkrétně byla provedena analýza 106 hlavních článků.

Obrázek 17 znázorňuje kategorie článků ve Web of Science, mezi které patří počítačové vědy - teoretické metody i informační systémy, inženýrství, politické vědy, veřejná administrativa, právo, telekomunikace, aplikovaná matematika, sociální věci a jiné, což ukazuje na multidisciplinaritu výzkumu, kterou je vhodné reflektovat i v dalších částech výzkumu.



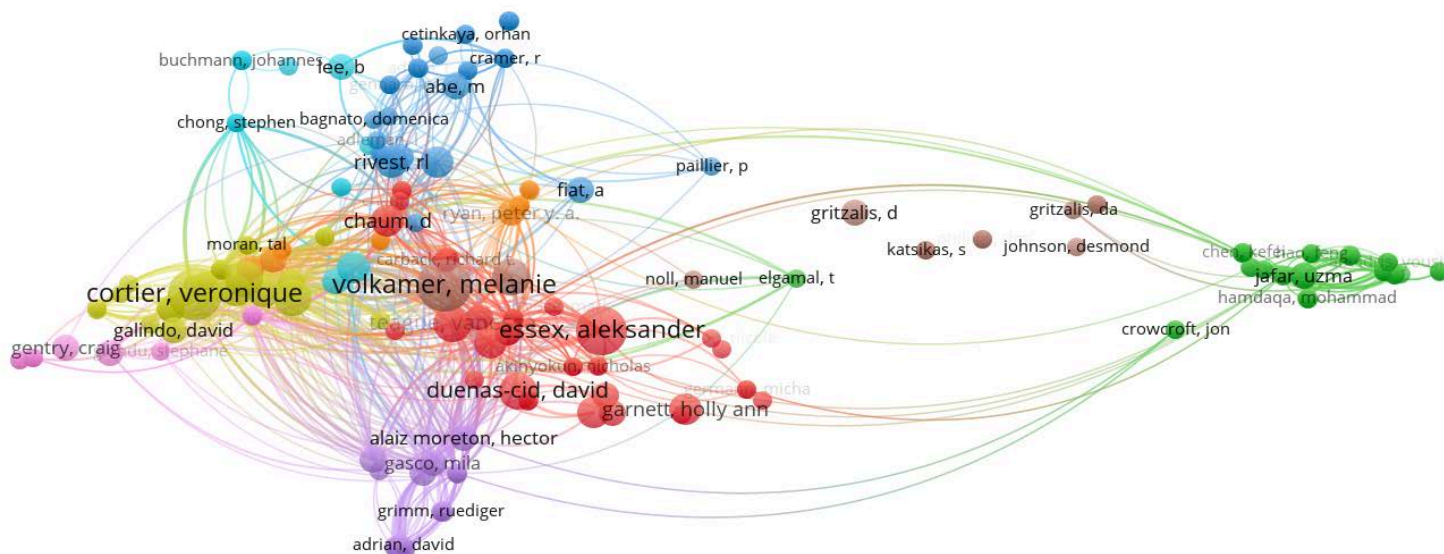
Obrázek 17: Kategorie článků ve Web of Science (vlastní zpracování pomocí Clarivate)

Výzkum dané problematiky také probíhá celosvětově, což znázorňuje obrázek 18 zemí podle původu autorů souvisejících článků. Vědeckému výzkumu kryptografie, elektronických volebních systémů a jejich evaluaci se věnují především výzkumníci svobodného světa zobrazeného na obrázku 12. Konkrétně 139 autorů pochází ze svobodných zemí, 6 z částečně svobodných zemí a 6 z nesvobodných zemí.



Obrázek 18: Země autorů článků ve Web of Science (vlastní zpracování pomocí Clarivate)

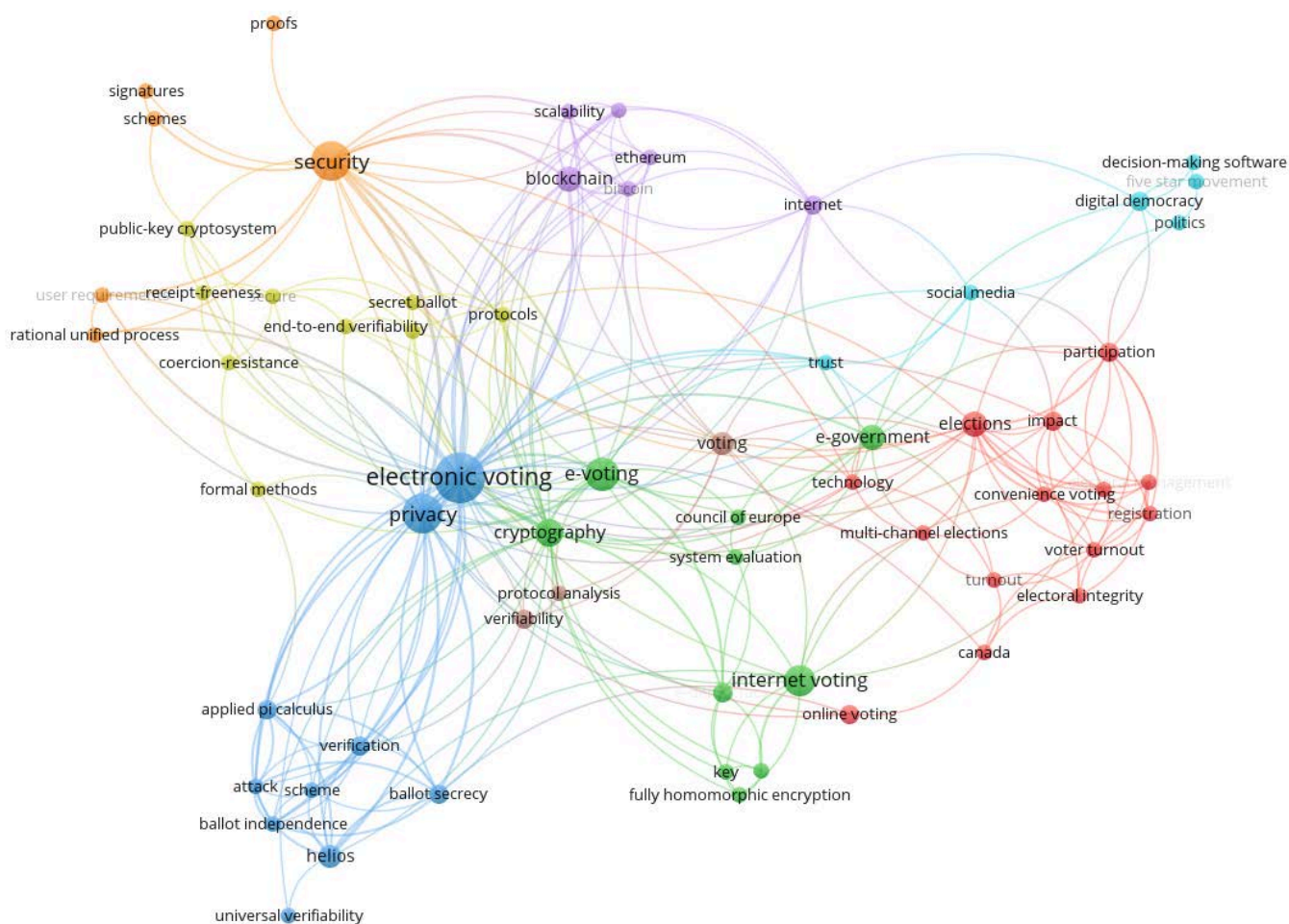
Vizualizace na obrázku 19 znázorňuje citační síť. Z vizualizace vyplývá, že autoři, kteří se zabývají hodnocením a návrhem i-hlasovacích systémů založených na technologii blockchain provádí svůj výzkum do jisté míry odděleně od autorů, kteří navrhují a hodnotí systémy obecně nebo bez využití technologie blockchain.



Obrázek 19: Vizualizace co-citací autorů (vlastní zpracování pomocí VOSviewer)

Nejčastěji použitá klíčová slova a jejich vzájemné propojení znázorňuje analýza klíčových slov vizualizovaná na obrázku 20. Z vizualizace klíčových slov týkajících se elektronického hlasování lze identifikovat několik klíčových témat, která jsou vzájemně propojená a často diskutovaná. Centrálním pojmem je „electronic voting“, kolem kterého se tvoří hlavní klastry. Modrý klaster se zaměřuje na technické aspekty,

jako je „cryptography“ a „privacy“, což naznačuje, že klíčovými otázkami ve výzkumu elektronického hlasování jsou právě kryptografické metody pro zajištění soukromí. Zelený klastr zahrnuje pojmy jako „internet voting“ a „system evaluation“, což odráží zaměření na hodnocení systémů s ohledem na kryptografii i doporučení Rady Evropy. Červený klastr se více soustředí na institucionální a organizační aspekty, například „election integrity“ a „voter authentication“, což naznačuje, že hodnocení volebních systémů se zaměřuje i na spolehlivost a zabezpečení identifikace voličů. Světle modrý klastr se soustředí na politologii, fialový klastr na blockchain, oranžový klastr na bezpečnost a žlutý klastr na ověřitelnost a odolnost nátlaku. Vzájemná propojení mezi těmito klíčovými slovy ukazují na úzkou souvislost mezi technickými, organizačními i politologickými výzvami v oblasti elektronického hlasování, přičemž důraz je kladen zejména na bezpečnost, důvěryhodnost a integritu volebních procesů.



Obrázek 20: Vizualizace analýzy klíčových slov (vlastní zpracování pomocí VOSviewer)

Z hlediska počtu citací evidovaných ve Web of Science mají nad tisíc citací práce, které se zabývají obecnější kryptografickou technikou, konkrétně 8180 (Rivest, 1978), 7101 (Shamir, 1979), 4135 (ElGamal, 1985), 4122 (Paillier, 1999), 2940

(Gentry, 2009), 1908 (Fiat, 2006), 1898 (Chaum, 1981), 1475 citací (Goldwasser, 1988). Z prací, které se zaměřují přímo na e-hlasování, mají práce se zaměřením na volební systémy s využitím technologie blockchain 225 citací (McCorry, 2017), 160 (Kshetri, 2018) nebo 135 citací (Hjalmarsson, 2018). Práce na e-hlasování nezmiňující blockchain mají 194 (Hirt, 2000), 177 (Chaum, 2004), 161 (Clarkson, 2008), 153 citací (Jakobsson, 2002). Z prací zabývajících se čistě hodnocením i-hlasovacích systémů bez ohledu na blockchain mají větší počet citací 135 (Gerbaudo, 2021), 108 (Springall, 2014), 66 (Gritzalis, 2002).

4.2 Analýza názorů stávajících uživatelů internetového hlasování

V rámci kvalitativního výzkumu provedl autor polo-strukturované a nestrukturované rozhovory s odborníky nebo zainteresovanými stranami z různých souvisejících oblastí (Martínek, 2024b; Martínek, 2024d; Příloha K). Kvalitativní část analýzy zahrnuje vyhodnocení dvou dotazníkových šetření.

V rámci rozsáhlého dotazníkového šetření autora (Martínek, 2024c), které probíhalo mezi členy České pirátské strany, která má dlouholeté zkušenosti s používáním internetového hlasování v případě tajných voleb, došlo k vyhodnocení názorů respondentů na základě popisné statistiky i korelační analýzy (Martínek, 2024d):

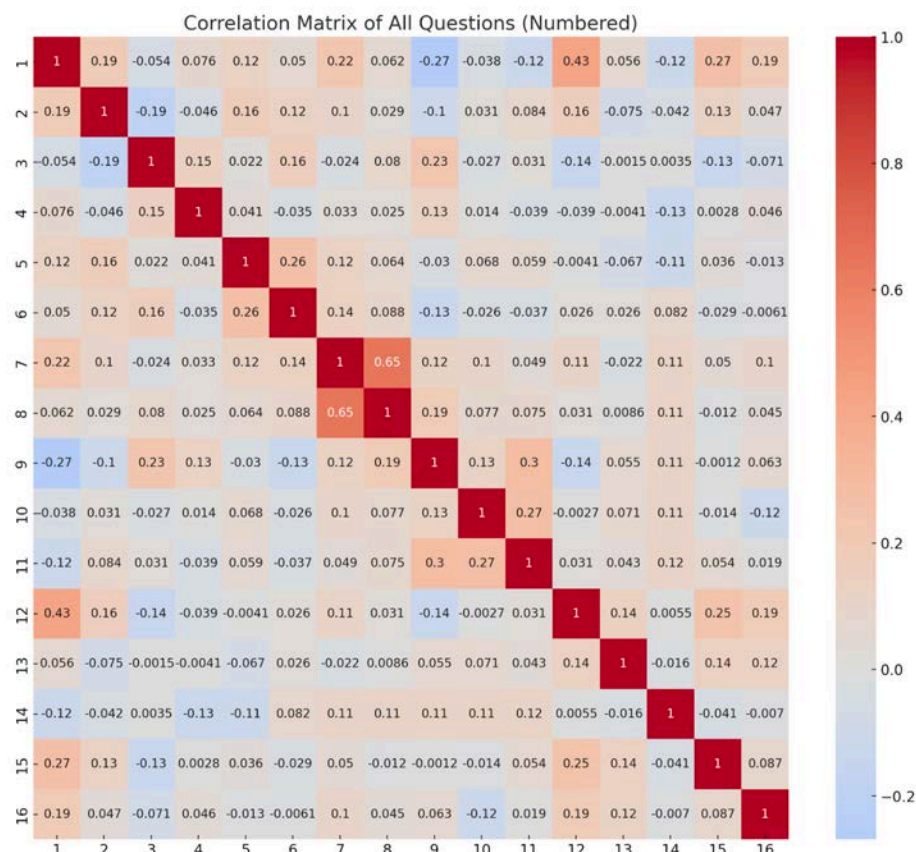
Celkově hodnotí respondenti konkrétní systém Helios pro online hlasování pozitivně, konkrétně 96,2 % respondentů se domnívá, že by Česká pirátská strana měla i nadále umožňovat elektronické hlasování prostřednictvím systému Helios. 93 % respondentů se domnívá, že by se jejich účast snížila, pokud by bylo online hlasování nahrazeno tradičním papírovým hlasováním během zasedání celostátního nebo krajského fóra. 98,6 % respondentů se domnívá, že elektronické hlasování na dálku usnadňuje jejich fungování uvnitř strany.

V dotazníkovém šetření 63,9 % respondentů považuje z hlediska důvěryhodnosti za vhodné, aby byl seznam voličů s informacemi o jejich účasti veřejně dostupný. Znalost možnosti opakovaného hlasování deklaruje 91,1 % respondentů, 81,2 % respondentů opakované hlasování využilo. V přítomnosti třetí osoby, která viděla zvolenou volbu, hlasovalo 24,4 % respondentů, pouze 2,4 % respondentů hlasovalo podle preferencí třetí osoby v její přítomnosti. Třetí osobou se při hlasování nechalo ovlivnit 21,6 % respondentů. 61,5 % respondentů uvedlo, že transparentnost volebního systému, včetně přístupu ke zdrojovému kódu, je pro ně z hlediska důvěry důležitá. 53,1 % respondentů uvedlo, že rozumí způsobu šifrování hlasů a zajištění soukromí v systému Helios, pouze 13,2 % respondentů se obává prolomení tajnosti hlasování. Zajímavé je, že 47,4 % voličů by nevádilo, kdyby někdo odhalil, jak hlasovali. Pouze 31 % respondentů si kontroluje přítomnost svého sledovacího kódu ve veřejně přístupné elektronické volební urně. Spokojenost s provozováním hlasovacího systému přímo stranou vyjádřilo 89,2 % respondentů.

Mezi další zajímavá zjištění patří, že 71,4 % respondentů, kteří se obávají prolomení tajnosti hlasování, nerozumí způsobu, jakým je hlasování v systému Helios šifrováno. Naopak ti, kteří se prolomení tajnosti neobávají, nerozumí systému šifrování hlasů pouze z 44,2 %. To ukazuje na důležitost potřeby dostatečné informovanosti o fungování systému. Dále respondenti (3,8 %), kteří nechtějí systém Helios dále používat, z 87,5 % nepovažují systém za intuitivní a nerozumí způsobu šifrování hlasu v systému Helios. Kromě dostatečné informovanosti by tedy bylo možné zlepšit i uživatelské rozhraní systému.

Systém Helios je založen na tom, že všichni aktéři podnikají maximální možné kroky k ověření svých činností, aby byla zajištěna integrita voleb. Skutečnost, že pouze 31 % voličů provedlo alespoň jedno ověření přítomnosti sledovacího hashe ve volební urně, může zvyšovat riziko manipulace s hlasy.

V otevřených odpovědích se také opakovaně objevoval požadavek na zpřístupnění alternativních způsobů hlasování, které systém Helios na rozdíl od novějšího systému Belenios nenabízí. Z hlediska intuitivnosti respondenti kritizují, že voliči často nevědí o možnosti odevzdat prázdný hlasovací lístek, což je v podstatě hlasování proti všem možnostem. Volby pouze s jednou možností hlasování tak často končí pro danou možnost úspěšně. Respondenti se také obávají prolomení tzv. věčného soukromí (Haines, 2023), neboť systém zobrazuje ve veřejně přístupné volební urně vedle skutečného jména voliče trvalý sledovací hash. S rostoucím výkonem kvantových počítačů by v budoucnu mohlo dojít k prolomení asymetrické šifry (Bavdekar, 2022), což by umožnilo odtajnění hlasovacích lístků v elektronické volební schránce. Kritičtí respondenti internetového hlasování se rovněž obávají možné manipulace s hlasy. Respondenti také podmiňují fungování volebního systému dostatečnou transparentností.



Obrázek 21: Korelační matice otázek číslovaných v pořadí podle přílohy článku (Martínek, 2024d; Příloha G)

V korelační analýze znázorněné korelační maticí na obrázku 21 existuje silná pozitivní korelace 0,65 mezi povědomím o možnosti volit opakovaně a skutečným využitím této možnosti. Respondenti, kteří považují systém za intuitivní, často podporují pokračování elektronického hlasování, což odráží korelace 0,43. Mezi otázkami zaměřenými na volbu za přítomnosti třetí osoby a volbou podle přání třetí osoby je korelace 0,3. Doporučením by mohlo být přidat na začátek výběru prohlášení, že výběr možností musí být proveden nezávisle bez přítomnosti třetí osoby. Vnímaná důležitost transparentnosti hlasovacího systému mírně koreluje (0,26) s ověřením sledovacího kódu po odevzdání hlasování. Podrobnější vyhodnocení této tématem i účastí členů strany unikátní analýzy je k dispozici v článku autora (Martínek, 2024d).

4.3 Analýza názorů potenciálních uživatelů internetového hlasování

Na základě vyhodnocení dotazníkového šetření (Martínek, 2024g) mezi potenciálními uživateli internetového hlasování lze odvodit, že studenti a absolventi vysokých škol očekávají od i-hlasovacího systému splnění všech 5 definovaných dimenzí i transparentnosti, jak je autorem vyhodnoceno mírou očekávání v tabulce 6. Nejvíce je očekávána srozumitelnost, testování, monitoring a ověřitelnost systému.

Dimenze (počet otázek v rámci dimenze)	Průměrná četnost odpovědí							Míra očekávání
	0	1	2	3	4	5	6	
Informační dostupnost (4)	1,25	1,75	3,25	9	15	25,5	44,25	0,81
Srozumitelnost (5)	0	0,2	0,8	3,4	17	33	45,6	0,86
Monitoring a ověřitelnost (5)	0,4	0,4	1,8	8	17,2	30	42,2	0,83
Nápravná opatření (5)	0,6	1,6	4	9,6	15	30,8	38,4	0,80
Testování (4)	0,75	0,75	1,75	8	16,5	27,25	45	0,83
Transparentnost (4)	1,5	0,75	2,25	12,5	19,25	29	34,75	0,79

Tabulka 6: Vyhodnocení dotazníkového šetření očekávaných vlastností i-voting systémů mezi studenty a absolventy vysokých škol (Martínek, 2024e)

V rámci konkrétních otázek lze zmínit, že potenciální uživatelé internetového hlasování očekávají (0,72), že v případě zavedení, využijí možnosti hlasovat přes Internet. U otázky, zda by měl být online hlasovací systém transparentní, je míra souhlasu respondentů 0,81. Transparentnost jako nedílná součást internetového hlasovacího systému se odráží v míře souhlasu 0,78. Transparentnost jako důležitý prvek internetového hlasovacího systému je vyjádřena mírou souhlasu 0,79. Respondenti také uvádějí míru souhlasu 0,74 v otázce, že v případě jakýchkoliv problémů s volebním procesem by měla být určena odpovědná osoba. Míra očekávání 0,85 respondentů představuje požadavek, aby existovala jistota, že jakékoli narušení bezpečnosti bude odhaleno a napraveno. Požadavek na důkladné testování bezpečnostních chyb nezávislými bezpečnostními experty představuje vysoká míra očekávání 0,89. Vysoká míra očekávání 0,89 byla zaznamenána také u otázky, která se týkala možnosti ověřit, zda online hlasovací systém zaznamenal hlas voliče tak, jak bylo zamýšleno. Požadavek na veřejnou dostupnost externích auditů po volbách je zastoupen mírou očekávání 0,79.

Analýza názoru potenciálních uživatelů internetového hlasování je vyhodnocena v článcích (Martínek, 2024e; Příloha K).

4.4 Expertní určení úrovní požadavků Rady Evropy CM/REC(2017)5

Standards elektronického hlasování Rady Evropy (Council of Europe, 2017) spadají do tří hlavních dokumentů, které zahrnují základní text doporučení a dvě podrobnější přílohy. Pro snadnější propojení je v této práci standardizována terminologii dle Bruneta (2023):

- **Zásady** - principy formulující nejvyšší priority. Rada Evropy definuje zásady v oddíle 14 důvodové zprávy, například všeobecné volební právo, rovné volební právo a svobodné volební právo.

- **Normy** - vlastnosti voleb, které musí být dodrženy. Rada Evropy formuluje své požadavky ve svém hlavním normalizačním dokumentu. Například norma číslo 10 (v rámci principu svobodného volebního práva) vyžaduje, aby nebyl voličův záměr neoprávněně ovlivněn.
- **Pokyny** - Poskytují specifičnost ohledně toho, co je minimálně nutné k splnění požadavku. Rada Evropy formuluje pokyny pro některé (ale ne všechny) své normy. Jsou identifikovány písmenem vedle čísla normy.
- **Požadavky** - Pro účely této práce je spojen koncept norem a pokynů do jedné kategorie požadavků. Celkem je tak zkoumáno 143 požadavků zahrnujících 49 norem a 94 pokynů.

Na základě rešerše, analýzy souvisejících textů (International IDEA, 2014; Council of Europe, 2017; NIST, 2020; ISO, 2022) zahrnující především zprávy od Agentury EU pro kybernetickou bezpečnost (ENISA, 2019; ENISA, 2023; ENISA, 2024), i analýz názorů potenciálních uživatelů tajné internetové volby lze usuzovat, že existují různé úrovně významnosti voleb, pro které lze vyžadovat určitá pravidla.

Mezi kritéria ovlivňující významnost voleb autor řadí:

- **závažnost hlasování**, kdy nezávazná konzultační hlasování nesou nízké riziko dopadu na celou společnost;
- **významnost s ohledem na exekutivu či zákonodárství**, kdy volby do orgánů, které mohou následně měnit volební předpisy vyžadují zvýšenou pozornost, aby zmanipulované volby nevedly ke změně volebních zákonů lidmi, kteří nemají legitimitu od voličů, vyšší úroveň se tak týká národních politických voleb;
- **informovanost a technická gramotnost voličů**, kdy vyšší úroveň technické gramotnosti voličů může přispět k lepšímu pochopení bezpečnostních opatření a snížení rizika phishingu či podobných útoků;
- **podíl voličů využívající internetové hlasování jako svůj kanál pro odevzdání hlasu**, kdy nižší podíl voličů může znamenat nižší riziko a menší potřebu složitých bezpečnostních opatření.
- **celkový počet voličů**, kdy počet voličů v řádu milionů vyžaduje vyšší úroveň zabezpečení, podpory i administrativy, naopak nízký počet voličů v řádu jednotek může umožnit individuálně zajistit podporu méně technicky zdatným voličům s provedením volby.

Proto obdobně jako u CNIL (La Commission nationale de l'informatique et des libertés, 2019) autor stanovuje 6 úrovní voleb, pro které bude vyžadováno splnění určitých požadavků:

- **0 - Testovací** - tato úroveň nemusí splňovat žádný požadavek.
- **1 - Nezávazná hlasování** - tato úroveň zahrnuje nezávazná konzultační referenda a nevýznamné volby (anketa Miss sympathie apod.).

- **2 - Volby nižší významnosti informovanými voliči** - tato úroveň zahrnuje volby do orgánů s nižším významem pro celou společnost (volby akademického senátu, volby v soukromých společnostech, vnitrostranické volby apod.), kde se volby účastní technicky gramotní voliči, alternativně je možnost pomoci s odevzdáním hlasu elektronicky nebo jiným volebním kanálem.
- **3 - Závazná lokální referenda, volby nižší významnosti bez ohledu na technickou zdatnost voliče** - tato úroveň zahrnuje závazná místní referenda, volby do orgánů s nižším významem pro celou společnost (volby akademického senátu, volby v soukromých společnostech, volby v SVJ, vnitrostranické volby apod.), které se mohou účastnit i méně technicky zdatní a méně informovaní voliči.
- **4 - Hybridní závazná celonárodní referenda a omezené celonárodní volby** - tato úroveň zahrnuje celonárodní referenda, kde lze hlasovat i papírově, dále celonárodní volby, kde může hlasovat přes Internet maximálně 10 % voličů (např. celonárodní volby pouze pro voliče v zahraničí) a volby, kde se nevolí do orgánů s vlivem na volební zákony (komunální a krajské volby).
- **5 - Volby splňující požadavky Rady Evropy** - tato úroveň musí splňovat všechny požadavky, jedná se například o závazné celonárodní volby pro celou populaci.

Během výzkumu autora práce byly pomocí expertních stanovisek s využitím rozhodovací metody BeCoMe určeny minimální požadavky doporučení Rady Evropy pro každou z úrovní voleb. Úroveň tak musí splňovat požadavky kladené na danou úroveň a současně i požadavky kladené na všechny nižší úrovně.

Na základě v metodice popsaného postupu se podařilo autorovi v rámci expertního výzkumu určit minimální úrovně, od kterých by měl být konkrétní požadavek povinně splněn (Příloha E). Výsledné úrovně jsou zmíněny u každého požadavku v kapitole 4.5.

Pouze 2 požadavky jsou definovány jako povinně požadované již od úrovně 1, konkrétně se jedná o požadavek 21 ohledně ochrany autentizačních dat a požadavek 40(d), který požaduje zachování dostupnosti a integrity hlasů. Od úrovně 2 je navíc vyžadováno 48 požadavků, od úrovně 3 je navíc vyžadováno 79 požadavků, od úrovně 4 je navíc vyžadováno 13 požadavků a nejvyšší úroveň 5 navíc vyžaduje 1 požadavek — konkrétně 15(a), který se týká případného používání hlasovacího zařízení ve volební místnosti (viz Kapitola 4.5, Příloha E).

V rámci slovního komentáře bylo zmíněno, že hlavní zlom je vnímán mezi úrovní 2 a 3, kdy úroveň 3 již zahrnuje i vyjádření vůči orgánům (referenda města, kraje apod.), které si volič standardně nevybírá jako v případě samosprávných orgánů, profesních komor apod. (Respondent - ústavní právník). Obavy ze zavádění celonárodního

internetového hlasování (Respondent - IT expert na kybernetickou bezpečnost) se týkají především situace na trhu s klientskými zařízeními, kde absolutní většina všech zařízení je pod kontrolou několika málo korporací, které navíc mají sídlo v zahraničí. Některé body z doporučení nejsou považovány za potřebné, konkrétně je zmíněn například bod 1(c) ohledně nutné zpětné kompatibility (Respondent - IT expert na kybernetickou bezpečnost), naopak by měl být bod přeformulován na kompatibilitu s otevřenými standardy. Zmiňován je i bod 1(b), kdy nemá být nutné zapojení voličů do designu volebního systému (Respondent - IT expert na kybernetickou bezpečnost), definování požadavků na systém a jejich ověření by měli zajistit odborníci (Respondent - Expert na AI). Obecně je zmíněno (Respondent - IT expert na kybernetickou bezpečnost; Respondent - expert na volební systémy) u možnosti 15(a), že elektronické hlasování by v celonárodních volbách mělo být pouze doplňkovou možností se zachováním možnosti volit pomocí papíru.

4.5 Propojení metodiky s doporučením Rady Evropy CM/REC(2017)5

I když Marcos del Blanco (2018a) deklaruje, že jeho metodika hodnocení reflektuje doporučení Rady Evropy (Council of Europe, 2017), tak z autorem provedené komparativní analýzy není patrné, zda jsou všechny body doporučení splněny, případně do jaké míry jsou naplněny. Stejně tak některé požadavky jsou natolik obecné, že teoreticky mohou zahrnout požadované normy z doporučení, stejně tak ale nemusí být všechny normy brány v potaz.

Standardy elektronického hlasování Rady Evropy (Council of Europe, 2017) jsou v následujícím textu v doslovném českém překladu a se zkráceným názvem dle Bruneta (2023) propojeny na základě komparativní analýzy s metodikou (Marcos del Blanco, 2018a), která je přeložena v příloze A. Požadavky jsou propojeny na základě významové ekvivalence, pokud není za pomlčkou uvedeno označení požadavku z metodiky (Marcos del Blanco, 2018a), nebyl vhodný odpovídající požadavek nalezen. V hranatých závorkách je uvedena úroveň stanovená pomocí expertního šetření, od které má být daný požadavek povinný. K některým bodům jsou zapsány poznámky autora pro usnadnění vyhodnocování splnění konkrétních požadavků.

4.5.1 Všeobecné volební právo

1 Uživatelské rozhraní by mělo být snadno použitelné [2] - U-1

Voličské rozhraní systému elektronického hlasování musí být snadno srozumitelné a použitelné pro všechny voliče.

1(a) Snadná interpretace možností hlasování [2] - U-1

Prezentace možností hlasování na zařízení používaném voličem by měla být optimalizována pro běžného voliče, který nemá specializované počítačové znalosti.

1(b) Voliči zapojení do designu [3] - U-1

Voliči by měli být zapojeni do návrhu systémů elektronického hlasování, zejména s cílem identifikovat omezení a otestovat snadnost použití v každé hlavní fázi procesu vývoje.

1(c) Kompatibilita systému [3] - I-6

Při vývoji nových IT produktů je třeba vzít v úvahu jejich kompatibilitu se stávajícími.

2 Nezávislost pro zdravotně postižené voliče [2] - U-2

Systém elektronického hlasování je navržen tak, aby umožňoval osobám se zdravotním postižením a zvláštními potřebami volit nezávisle.

2(a) Zvláštní hlasovací rozhraní [3] - V-2

Voliči by měli mít k dispozici, kdykoli je to nutné a možné, další zařízení, jako jsou speciální rozhraní nebo jiné ekvivalentní prostředky, jako je osobní asistence.

2(b) Shoda WCAG 2.0 AA [3] - V-5

Internetová hlasovací rozhraní by měla co nejvíce odpovídat pokynům stanoveným v iniciativě Web Accessibility Initiative (WAI).

3 Pokud elektronické hlasování není všeobecně dostupné, jsou k dispozici další hlasovací kanály [3] - ESWD-7

Nejsou-li kanály elektronického hlasování na dálku všeobecně přístupné, jsou pouze doplňkovým a volitelným způsobem hlasování.

(Pozn. autora: v případě, že lze změnit/prodloužit dobu pro odevzdávání hlasů v případě výpadku a současně se jedná o úroveň 0-3, lze považovat jako splněno)

4 Živé volební rozhraní je explicitní [3] - ESWD-15

Před hlasováním pomocí systému elektronického hlasování na dálku musí být voliči výslovně upozorněni na to, že elektronická volba, ve které podávají své rozhodnutí elektronickými prostředky, je skutečnými volbami nebo referendem.

4.5.2 Rovné volební právo

5 Informace o hlasování prezentovány jednotně [2] - SWD-6

Všechny oficiální informace o hlasování jsou prezentovány stejným způsobem, v rámci hlasovacích kanálů i mezi nimi.

5(a) Žádné nadbytečné informace o hlasování [3] - SWD-6

Elektronický hlasovací lístek používaný pro elektronické hlasování by neměl obsahovat žádné informace o možnostech hlasování, kromě těch, které vyžaduje zákon.

5(b) Žádné zkreslené informace o kandidátech [2] - SWD-6

Pokud jsou informace o možnostech hlasování dostupné ze stránky elektronického hlasování, musí být prezentovány spravedlivým způsobem.

6 Bezpečná agregace napříč kanály [2]

Jsou-li při stejných volbách nebo referendu použity elektronické a neelektronické hlasovací kanály, musí existovat bezpečná a spolehlivá metoda pro sečtení všech hlasů a pro výpočet výsledku.

(Pozn. autora: pokud existuje pouze jeden kanál odevzdání, lze považovat za splněno; v případě internetového volebního systému využívající schéma blockchainu lze označit za splněno pouze, pokud skutečně dochází k bezpečné agregaci napříč všemi uzly)

7 Jednoznačně identifikovatelní voliči [2] - I-1

Zajistí se jednoznačná identifikace voličů tak, aby je bylo možné nezaměnitelně odlišit od ostatních osob.

8 Ověřování voličů - I-1 [2]

Systém elektronického hlasování udělí uživateli přístup pouze po jeho ověření jako osoby s hlasovacím právem.

9 Jeden hlas na hlasujícího... [2] - I-1

Systém elektronického hlasování zajistí, aby byl odevzdán pouze příslušný počet hlasů na jednoho voliče, uložen do elektronické volební schránky a zahrnut do výsledku voleb.

9(a) ...i když je povoleno více hlasování [2] - I-1

Pokud je voliči umožněno odevzdat elektronický hlas vícekrát, měla by být přijata vhodná opatření, která zajistí, že bude započítán pouze jeden hlas.

(Pozn. autora: v případě, že lze odevzdat pouze jednou, lze považovat za splněné)

9(b) ...i když je více kanálů [2] - I-1

Pokud je voliči umožněno hlasovat více než jedním hlasovacím kanálem, měla by být přijata vhodná opatření, aby se zajistilo, že se započítává pouze jeden hlas.

(Pozn. autora: v případě, že lze odevzdat pouze jedním hlasovacím kanálem, lze považovat za splněné)

9(c) Jinak je zabráněno vícenásobným hlasováním [2] - I-1

Ve všech ostatních případech by měla být přijata vhodná opatření, která zabrání voliči odevzdat více než jeden platný hlas.

9(d) Informace o možnostech hlasování [2] - SWD-4

Volič by měl být ve všech případech jasně informován o nabízených možnostech hlasování a o pravidlech pro sčítání hlasů.

4.5.3 Svobodné volební právo

10 Hlasovací systém je chráněn [2] - I-1

Úmysl voliče nesmí být ovlivněn systémem hlasování ani žádným nepatřičným vlivem.

10(a) Volič se učil ověřovat spojení [3] - ESWD-15

V případě elektronického hlasování na dálku by měl být volič informován o prostředcích, jak ověřit, že bylo navázáno spojení s oficiálním serverem a že byl předložen pravý hlasovací lístek.

(Pozn. autora: nelze po voliči vynutit spoluúčast na testování; pokud je alespoň online dostupná dostatečná dokumentace, návod a další informace, o kterých byl volič informován, pro zajištění spojení s oficiálním serverem a odevzdáním hlasu lze považovat za splněné)

10(b) Pouze oficiální informace o hlasování [2] - SWD-5

Systém elektronického hlasování by neměl při hlasování umožňovat jakýkoli manipulativní vliv na voliče. Zejména elektronický hlasovací lístek, kterým se provádí elektronické hlasování, by neměl obsahovat žádné neoficiální informace.

10(c) Odevzdané hlasovací lístky jsou odolné proti neoprávněné manipulaci - MA-4

Systém elektronického hlasování by měl zavést všechna možná opatření, aby se zabránilo jakémukoli manipulativnímu ovlivňování hlasování po jeho odevzdání, a bude zahrnovat opatření, která umožní ověřit, že žádný takový vliv nebyl uplatněn.

10(d) Odolnost vůči nátlaku [3] - CR

Je-li to považováno za nutné, měl by systém elektronického hlasování nabízet mechanismy (například vícenásobné hlasování), které voliče ochrání před nátlakem, aby hlasovali určitým způsobem.

(Pozn. autora: možnost vícenásobného hlasování snižuje riziko nátlaku, v případě voleb úrovně 0-3 by v tomto případě mohlo být považováno za splněné do jisté míry; v rámci úrovně 4 a 5 by se pro splnění mělo například umožnit hlasovat v kontrolovaném prostředí po skončení intervalu pro internetové hlasování, což by přepsalo hlas odevzdaný volbou v nekontrolovaném prostředí)

11 Postupy zajišťují autentické hlasování [2] - I-1

Zajistí se, aby systém elektronického hlasování předložil voliči autentický hlasovací lístek a autentické informace.

12 Správné zachycení úmyslu voličů [3] - U-3

Způsob, jakým jsou voliči vedeni procesem elektronického hlasování, je nesmí vést k tomu, aby hlasovali ukvapeně nebo bez potvrzení.

12(a) Hlasovací lístek lze před vhozením upravit [2] - U-3

Voliči by měli mít možnost změnit svou volbu v kterémkoli bodě procesu elektronického hlasování na dálku před odevzdáním svého hlasu nebo postup přerušit.

13 Voliči se mohou zdržet hlasování [2] - U-3

Systém elektronického hlasování poskytne voliči prostředky k účasti ve volbách nebo referendu, aniž by volič upřednostnil některou z možností hlasování.

14 Voliči jsou upozorněni na neplatnost hlasů [2] - U-3

Systém elektronického hlasování upozorní voliče, pokud odevzdá neplatný elektronický hlas.

(Pozn. autora: pokud systém neumožňuje odevzdat nezáměrně neplatný hlas lze považovat za splněné)

15 Individuální ověřitelnost [2] - E2Ev

Volič musí mít možnost ověřit si, že jeho úmysl je při hlasování přesně zastoupen a že zapečetěný hlas vstoupil do elektronické volební schránky beze změny. Jakýkoli nepatřičný vliv, který změnil hlasování, musí být zjistitelný.

15(a) Papírové kopie hlasování ve volbách [5]

Při používání zařízení pro elektronické hlasování ve volebních místnostech by členské státy měly zvážit použití papírových hlasovacích lístků jako druhého média pro uložení hlasu pro účely ověření.

(Pozn. autora: pokud se nepoužívá možnost volby ve volebních místnostech, lze považovat za splněné)

15(b) Statistické audity (např. RLA) [4]

Povinné sčítání hlasů ve druhém médiu ve statisticky významném počtu náhodně vybraných volebních místností by mělo být provedeno zejména u elektronických hlasovacích zařízení a optických skenerů.

(Pozn. autora: pokud se nepoužívá možnost volby typu DRE nebo OCR, lze považovat za splněné)

16 Potvrzení odevzdaného hlasu [2] - U-3

Volič obdrží potvrzení od systému, že hlasování bylo úspěšně odevzdáno a že celý postup hlasování byl dokončen.

17 Dokáže ověřit všechny platné hlasy [3] - E2Ev

Systém elektronického hlasování poskytne spolehlivé důkazy o tom, že každý autentický hlas je přesně zahrnut do příslušných výsledků voleb. Důkazy by měly být ověřitelné prostředky, které jsou nezávislé na systému elektronického hlasování.

18 Dokáže ověřit zahrnutí pouze platných hlasů [3] - E2Ev

Systém poskytne spolehlivý důkaz, že do příslušného konečného výsledku byly zahrnuty pouze hlasy oprávněných voličů. Důkazy by měly být ověřitelné prostředky, které jsou nezávislé na systému elektronického hlasování.

4.5.4 Tajné volební právo

19 Tajnost hlasování [2] - CR

Elektronické hlasování je organizováno tak, aby bylo zajištěno zachování tajnosti hlasování ve všech fázích postupu hlasování.

19(a) Seznam voličů oddělený od hlasovacích částí [2] - SWD-7, IAP-5

Údaje v registru voličů by měly být jasně odděleny od složek hlasování.

20 Minimalizace dat [3] - IAP-4

Systém elektronického hlasování zpracovává a uchovává po dobu nezbytně nutnou pouze osobní údaje potřebné pro průběh elektronické volby.

21 Autentizační data jsou chráněna [1] - ESWD-11

Systém elektronického hlasování a jakákoliv oprávněná strana chrání autentizační údaje tak, aby neoprávněné osoby nemohly tyto údaje zneužít, zachytit, upravit nebo jinak získat znalosti.

21(a) Autentizace používá kryptografii [2] - I-1

Autentizace by měla používat kryptografické mechanismy.

22 Seznam voličů má kontrolu přístupu [2] - ESWD-2

Rejstříky voličů uložené v systému elektronického hlasování nebo sdělované systémem elektronického hlasování jsou přístupné pouze oprávněným stranám.

23 Žádný přenosný doklad o odevzdání hlasů [3] - SWD-6

Systém elektronického hlasování neposkytne voliči důkaz o obsahu odevzdaného hlasu pro použití třetími stranami.

(Pozn. autora: u úrovně 0 až 3 lze za dostatečné považovat v rámci ověřitelnosti to, že případný hash neobsahuje údaje o hlasování, v případě úrovně 4 a 5 by mělo být kvůli možnosti odevzdat hlas před korupčníkem pro splnění umožněno hlasováním v kontrolovaném prostředí přepsat hodnotu novým hlasem, nebo využít jiné možnosti pro zajištění odolnosti nátlaku)

23(a) Ověření založené na papíru [4] - CR

Pokud je voliči poskytnut papírový doklad o elektronickém hlasování v kontrolovaném prostředí, nemělo by být voliči dovoleno jej ukazovat jiné osobě nebo tento doklad odnášet mimo volební místnost.

(Pozn. autora: pokud doklad neobsahuje informace o hlasování — obsahuje pouze například informace pro kontrolu přijetí hlasu bez možnosti ověřit vybranou volbu — lze považovat za splněné; pokud se papírový doklad nevystavuje nebo není umožněno hlasovat v kontrolovaném prostředí, lze považovat za splněné)

23(b) Žádné zbytkové informace po odhlasování [3] - IAP-4, CR

Po odevzdání hlasu by se neměly zobrazovat žádné zbytkové informace související s rozhodnutím voliče.

23(c) Voliči byli poučeni o rizicích utajování hlasování a zmírnění rizik [3] - SWD-4, ESWD-8

V případě elektronického hlasování na dálku by měl být volič před hlasováním informován o možných rizicích pro tajnost hlasování a doporučených prostředcích, jak je omezit.

23(d) Voliči byli poučeni, jak odstraňovat stopy ze zařízení [4] - IAP-6

V případě elektronického hlasování na dálku by měl být volič informován o tom, jak odstranit, pokud je to možné, stopy hlasu ze zařízení použitého k odevzdání hlasu.

(Pozn. autora: nelze po voliči vynutit spoluúčast na školení; pokud je alespoň online dostupná dostatečná dokumentace, návod a další informace, o kterých byl volič informován, pro odstranění stop hlasu ze zařízení lze považovat za splněné)

24 Žádné zveřejnění předčasných výsledků [3]

Systém elektronického hlasování nedovolí nikomu sdělit počet odevzdaných hlasů pro jakoukoliv možnost hlasování až do uzavření elektronické volební schránky. Tyto informace budou zveřejněny až po skončení období hlasování.

25 Utajeny jsou i předchozí hlasy voliče [2] - M-2

Elektronické hlasování zajistí, že bude respektováno tajemství předchozích voleb zaznamenaných a vymazaných voličem před vydáním jeho konečného hlasování.

26 Anonymizace voličů během sčítání [2] - SWD-7

Proces elektronického hlasování, zejména fáze počítání, musí být organizován tak, aby nebylo možné rekonstruovat spojení mezi nezapečetěným hlasem a voličem. Hlasy jsou a zůstávají anonymní.

26(a) Identita a volba voliče odděleny [2] - SWD-7

Informace o voličích by měly být odděleny od rozhodnutí voliče v předem definované fázi procesu sčítání.

26(b) Hlasovací lístky dekódovány ASAP po uzavření [3]

Jakékoli dekódování požadované pro sčítání hlasů by mělo být provedeno co nejdříve po skončení volebního období.

26(c) Důvěrnost během auditu [3] - MA-9, IAP-1

Členské státy by měly přijmout nezbytná opatření, aby zajistily, že bude zaručena důvěrnost veškerých informací získaných jakoukoli osobou při výkonu auditorských funkcí.

4.5.5 Regulační a organizační požadavky

27 Postupné zavádění elektronického hlasování [3]

Členské státy, které zavedou elektronické hlasování, tak učiní postupně a progresivně.

(Pozn. autora: úrovně 0-3 lze považovat za splněné, protože prvním krokem hlasování na úrovni státu by měla být právě úroveň 3; u úrovní 4 a 5 je nutné pro splnění prokázat dřívější úspěšné pilotní projekty internetového hlasování omezené pouze na určité voliče)

27(a) Veřejná studie proveditelnosti předem [3] - MA-3

Před výběrem a zavedením jakékoli technologie elektronického hlasování by měla být vypracována a zveřejněna formální studie proveditelnosti. Měla by obsahovat důvody pro přijetí tohoto systému, analýzu rizik, posouzení právního rámce, plánování pilotních projektů a jejich hodnocení, jakož i analýzu nákladů a přínosů.

27(b) Prvně piloti [3] - E-1

Jakákoli implementace pilotních projektů elektronického hlasování by měla začít s dostatečným předstihem před volbami a zahrnovat základní přípravy, jako je v případě potřeby přijetí podrobných předpisů pro pilotní projekty a testování systému.

27(c) Konečný systém testovaný před volbami [3] - V-4, MA-7, SWD-9, SWD-11, E-1, E-2, E-3, ESWD-12, IAP-7

Finální verze systému elektronického hlasování by měla být otestována před jeho použitím v řádných, závazných volbách.

27(d) Komplexní piloti [4] - E-4, E-5

Pilotní projekty by měly být prováděny na základě jasných a komplexních kritérií pro hodnocení účinnosti a integrity systému elektronického hlasování, včetně předávání výsledků.

28 Předem přijatá legislativa [3]

Před zavedením elektronického hlasování členské státy zavedou požadované změny do příslušných právních předpisů.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud je tajné internetové hlasování implementováno do interních předpisů)

28(a) Zákon: Implementovat/provozovat/počítat [3]

Právní rámec by měl zahrnovat postupy pro provádění elektronického hlasování od zřízení a provozu až po sčítání.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud je tajné internetové hlasování implementováno do interních předpisů)

28(b) Zákon: Platnost hlasování [3]

Právní rámec by měl obsahovat pravidla pro stanovení platnosti elektronického hlasování.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud je tajné internetové hlasování implementováno do interních předpisů)

28(c) Zákon: Nesrovnalosti v ověřování [3]

Právní rámec by měl zahrnovat pravidla zabývající se problémy, selháními a nesrovnalostmi vyplývajícími z používání ověřovacích nástrojů.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud je tajné internetové hlasování implementováno do interních předpisů)

28(d) Zákon: Ničení dat [3]

Právní rámec by měl zahrnovat postupy pro proces likvidace údajů, zejména za účelem sladění zpracování, uchovávání a likvidace údajů (a vybavení) technologie hlasování s právními předpisy o ochraně osobních údajů.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud je tajné internetové hlasování implementováno do interních předpisů)

28(e) Zákon: Domácí/mezinárodní pozorovatelé [3]

Právní rámec by měl zahrnovat ustanovení pro domácí a mezinárodní pozorovatele.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud je tajné internetové hlasování implementováno do interních předpisů)

28(f) Zákon: Časové osy [3]

Legislativa by měla stanovit jasné harmonogramy všech fází e-voleb.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud je tajné internetové hlasování implementováno do interních předpisů)

28(g) Žádné hlasování před obdobím hlasování [3]

Lhůta, ve které lze odevzdat elektronické hlasování, by neměla začít před oznámením voleb nebo referenda.

28(h) Elektronické hlasování před osobním hlasováním povoleno [3]

Dálkové elektronické hlasování může začít a/nebo skončit dříve, než je otevření jakékoli volební místnosti.

(Pozn. autora: v případě pouze internetového hlasování, lze považovat za splněné)

28(i) Žádné elektronické hlasování po období hlasování [3]

Období, ve kterém lze odevzdat elektronický hlas, by po skončení období hlasování nemělo pokračovat.

28(j) Systémová zpoždění neruší platnost hlasování [3]

Vkládání elektronických hlasů do elektronické volební schránky by mělo být umožněno po dostatečně dlouhou dobu po skončení období elektronického hlasování, aby se umožnilo jakékoli zpoždění při předávání zpráv dálkovým kanálem elektronického hlasování.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud se počítá s předem stanoveným koncem na přesný počítačový čas)

28(k) Systém po volbách nepřístupný [3]

Po skončení období elektronického hlasování by žádnému voliči neměl být umožněn přístup do systému elektronického hlasování.

29 Řídící volební orgán má kontrolu nad systémem [3] - ESWD-6

Příslušné právní předpisy upraví odpovědnost za fungování systémů elektronického hlasování a zajistí, aby nad nimi měl kontrolu řídicí volební orgán.

29(a) Transparentní zadávání zakázek [3] - C-1

Procesy zadávání zakázek pro elektronické hlasování by měly být prováděny transparentním způsobem.

(Pozn. autora: v případě využití bezplatného systému implementovaného například svépomocí lze považovat za splněné)

29(b) Omezte střety zájmů [3] - MA-8

Měla by být přijata opatření, která zabrání možným střetům zájmů soukromých zúčastněných stran zapojených do procesu.

29(c) Rozdělení povinností [3] - I-4

Musí být zachováno a zdokumentováno přísné oddělení povinností.

29(d) Není nadměrně závislý na dodavateli [3] - C-2

Členské státy by měly přijmout vhodná opatření, aby se vyhnuly okolnostem, kdy jsou volby nepřiměřeně závislé na prodejcích.

30 Pozorovatelnost počtu [3] - ESWD-4

Každý pozorovatel může sledovat sčítání hlasů. Za proces sčítání odpovídá volební řídící orgán.

30(a) Záznamy o procesu sčítání hlasů [2] - MA-5

O průběhu sčítání elektronických hlasů by měl být veden záznam, včetně informací o začátku a konci sčítání a osobách, které se sčítání účastní.

30(b) Počty hlasů založené na důkazech [3] - E2Ev

Sčítání hlasů by mělo být reprodukovatelné. Měla by existovat možnost získat spolehlivý důkaz, že postup počítání byl proveden uspokojivě, včetně nezávislého přepočtu.

30(c) Vlastnosti přesnosti jsou ověřitelné [3] - E2Ev

Ostatní funkce, které mohou ovlivnit přesnost výsledků systému elektronického hlasování, by měly být ověřitelné.

30(d) Dostupnost/integrita volební urny [3] - M-2

Systém elektronického hlasování by měl zachovat dostupnost a integritu elektronické volební urny a výstup z procesu sčítání tak dlouho, jak je potřeba.

4.5.6 Transparentnost a pozorování

31 Transparentnost [2] - SWD-12, E-4

Členské státy musí být transparentní ve všech aspektech elektronického hlasování.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud je transparentní alespoň provozovatel systému elektronického hlasování)

31(a) Zveřejněný seznam použitého softwaru [2] - SWD-1

Příslušné volební orgány by měly zveřejnit oficiální seznam softwaru použitého při e-volbách. Přinejmenším by měly uvádět použitý software, verzi, datum instalace a stručný popis.

31(b) Veřejný přístup ke zdrojovému kódu, docs [3] - SWD-12

Veřejný přístup ke složkám systému elektronického hlasování a informacím o nich, zejména dokumentaci, zdrojovému kódu a dohodám o mlčenlivosti, by měly být zpřístupněny zainteresovaným stranám a široké veřejnosti v dostatečném předstihu před volebním obdobím.

31(c) Komplexní procedurální příručky [3] - SWD-3

Zavedení technologií elektronického hlasování by mělo zahrnovat vypracování komplexních, podrobných pokynů krok za krokem včetně procedurální příručky.

32 *Voličům poskytnuty informace o volbách [2] - ESWD-8, ESWD-9*

Veřejnost, zejména voliči, musí být v dostatečném předstihu před začátkem hlasování jasným a jednoduchým jazykem informována o: jakýkoliv krocích, které může volič učinit, aby se mohl zúčastnit a hlasovat; správném používání a fungování systému elektronického hlasování; harmonogramu elektronického hlasování, včetně všech fází.

32(a) *Dokumenty a podpora, jak hlasovat [2] - ESWD-8*

Voličům by měl být zpřístupněn podpůrný a poradenský materiál o postupech hlasování.

32(b) *Informace voličům široce dostupné [3] - ESWD-8, SWD-4*

V případě elektronického hlasování na dálku by měl být informační materiál pro voliče dostupný také prostřednictvím jiného, široce dostupného komunikačního kanálu.

32(c) *Veřejná ukázka systému elektronického hlasování [3] - ESWD-15*

Voličům by měla být poskytnuta příležitost procvičit se před a odděleně od okamžiku odevzdání elektronického hlasování. V takovém případě by měli být účastníci výslovně upozorněni na to, že se neúčastní skutečných voleb nebo referenda.

33 *Zveřejnění součástí systému [3] - SWD-14*

Součásti systému elektronického hlasování se zveřejní pro účely ověření a certifikace.

33(a) *Podrobné/spolehlivé údaje z pozorování [3] - MA-2*

Systémy elektronického hlasování by měly vytvářet spolehlivé a dostatečně podrobné údaje z pozorování, aby bylo možné provádět pozorování voleb. Mělo by být možné spolehlivě určit čas, kdy událost vygenerovala pozorovací data. Měla by být zachována pravost, dostupnost a integrita údajů.

33(b) *Pozorovatelé mají přístup k dokumentům [3] - SWD-12*

Domácí a mezinárodní pozorovatelé by měli mít přístup k veškeré relevantní dokumentaci o procesech elektronického hlasování.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud dokumenty zpřístupní provozovatel internetového hlasování)

33(c) *Dokumenty v běžném jazyce [3] - MA-6*

Členské státy by měly pozorovatelům zpřístupnit příslušnou dokumentaci, pokud je to možné, v jazyce běžně používaném v mezinárodních vztazích.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud dokumenty v běžném jazyce zpřístupní provozovatel internetového hlasování)

33(d) Pozorovatelé vyškolení provozovateli [3] - ESWD-4

Členské státy by měly poskytovat školicí programy pro domácí a mezinárodní skupiny pozorovatelů.

33(e) Pozorovatelné testování hardwaru a softwaru [3] - ESWD-4

Domácí a mezinárodní pozorovatelé a média by měli mít možnost sledovat testování softwaru a hardwaru.

33(f) Pozorovatelný certifikační proces [4] - ESWD-4

Volební pozorovatelé by měli mít přístup ke všem krokům procesu hodnocení a certifikace.

34 Pozorovatelné volby [3] - MA-8

Pozorování a připomínkování e-voleb, včetně sestavování výsledků, bude umožněno každému pozorovateli v zákonem povoleném rozsahu.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud je pozorování a připomínkování umožněno alespoň dle interních předpisů)

35 Interoperabilita součástí [3] - ESWD-13, SWD-13

Otevřené normy se použijí k tomu, aby různé technické součásti nebo služby, případně odvozené z různých zdrojů, mohly vzájemně spolupracovat.

(Pozn. autora: v případě, že se jedná o veřejně dostupný otevřený zdrojový kód, lze považovat za částečně splněné)

4.5.7 Odpovědnost

36 Pro elektronické hlasování musí existovat standardy [3]

Členské státy vypracují technické požadavky, požadavky na hodnocení a certifikaci a zajistí, aby plně odrážely příslušné právní a demokratické zásady. Členské státy budou požadavky aktualizovat.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, s ohledem na použití podkladů této práce využívající Doporučení CM/Rec(2017)5 nebo jiných kvalitních podkladů, které nemusí vypracovat přímo členské státy)

36(a) Cíle a metody certifikace [4]

Členské státy by měly stanovit cíle certifikace a metody certifikace.

37 Nezávislá kontrola souladu [4] - MA-1, MA-2, MA-8

Před zavedením systému elektronického hlasování a poté ve vhodných intervalech, a zejména po jakýchkoli významných změnách v systému, nezávislý a kompetentní orgán vyhodnotí soulad systému elektronického hlasování a veškerých informací a komunikačních prostředků komponentu technologie (ICT) s technickými požadavky. To může mít formu formální certifikace nebo jiné vhodné kontroly.

37(a) Náklady na certifikaci stanoveny [4]

Členské státy by měly určit rozdělení nákladů spojených s procesem certifikace. Měli by definovat odpovědnost, včetně finanční, certifikačního orgánu za kvalitu jejich práce.

37(b) Certifikační orgány obdrží relevantní informace a dostatek času [4]

Hodnotící a certifikační orgány by měly mít plný přístup ke všem relevantním informacím a měly by mít dostatek času na provedení certifikačního procesu před volbami.

37(c) Pravidelně přezkoumávaný mandát k certifikaci [4]

Mandát hodnotících a certifikačních orgánů by měl být pravidelně znovu potvrzován v předepsaných intervalech.

37(d) Zprávy o certifikaci jsou zřejmé [4]

Závěry dosažené v certifikační zprávě by měly být zřejmé s informacemi obsaženými v této zprávě.

37(e) Zveřejnění certifikačních dokumentů [4] - ESWD-4

Členské státy by měly stanovit a zveřejnit jasná pravidla, pokud jde o zveřejňování závěrečné certifikační zprávy a všech příslušných dokumentů, s ohledem na důležitost transparentnosti.

38 Certifikát je neměnný [3]

Certifikát nebo jakýkoli jiný příslušný vydaný dokument musí jasně identifikovat předmět hodnocení a musí obsahovat záruky zabraňující jeho tajné nebo neúmyslné změně.

39 Otevřený a komplexní audit [3] - ESWD-4

Systém elektronického hlasování musí být kontrolovatelný. Auditní systém musí být otevřený a komplexní a aktivně informovat o potenciálních problémech a hrozbách.

39(a) Podrobné požadavky na audit [3] - MA-9

Auditní systém by měl zaznamenávat časy, události a akce, včetně: veškeré informace související s hlasováním, včetně počtu oprávněných voličů, počtu odevzdaných hlasů, počtu platných a neplatných hlasů, sčítání a přepočítávání atd.; jakékoli útoky na provoz systému elektronického hlasování a jeho komunikační infrastruktury; systémové poruchy, chyby a další ohrožení systému. Automatizované nástroje a systémové postupy by měly umožňovat rychlou a přesnou analýzu dat a podávání zpráv, a tím umožnit rychlou nápravnou akci. Auditní systém by měl poskytovat ověřitelné zprávy o: křížové kontroly údajů; systémové nebo síťové útoky; detekce a hlášení narušení; manipulace s daty; podvody a pokusy o podvod.

39(b) Komponenty mají synchronizované zdroje času [3]

Systém elektronického hlasování by měl udržovat spolehlivé synchronizované zdroje času. Přesnost zdroje času by měla být dostatečná pro zachování časových značek pro auditní záznamy a pozorovací údaje, jakož i pro zachování časových limitů pro registraci, nominaci, hlasování nebo sčítání.

39(c) Závěry auditu zvažované v budoucích volbách [3] - SWD-14

Závěry vyvozené z procesu auditu by měly být zohledněny v budoucích e-volbách.

4.5.8 Spolehlivost a bezpečnost systému

40 Řídící volební orgán je odpovědný za shodu, dostupnost, spolehlivost, použitelnost a bezpečnost [3] - ESWD-2

Za respektování a dodržování všech požadavků i v případě selhání a útoků odpovídá volební řídicí orgán. Řídící volební orgán odpovídá za dostupnost, spolehlivost, použitelnost a bezpečnost systému elektronického hlasování.

40(a) Žádné prostoje [3]

Dostupnost služeb elektronického hlasování pro všechny voliče během celého procesu elektronického hlasování musí být zachována.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné v případě, že lze změnit/prodloužit dobu pro odevzdávání hlasů v případě výpadku)

40(b) Informování voličů o incidentech [2]

Voliči by měli být neprodleně informováni vhodnými prostředky v případě přerušení, pozastavení nebo restartu elektronického hlasovacího systému.

40(c) Nevyloučení žádní oprávnění voliči [2] - V-2

Hlasovací systém nevylučuje oprávněné voliče z odevzdání svého hlasu.

40(d) Odevzdané hlasy jsou dostupné, bezpečné a přesné [1]

Systém elektronického hlasování by měl zachovat dostupnost a integritu hlasů.

40(e) Žádná ztráta dat v případě technických problémů [3] - IAP-4

Měla by být přijata technická a organizační opatření, která zajistí, že v případě poruchy nebo závady ovlivňující systém elektronického hlasování nebudou trvale ztracena žádná data.

40(f) Bezpečnostní mechanismy berou v úvahu použitelnost [3] - U-4

Členské státy by měly zvážit použitelnost během vývoje bezpečnostních mechanismů.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud bere v úvahu použitelnost provozovatel internetového hlasování)

40(g) V době provozuschopnosti systému pravidelně kontrolován [3] - IAP-1

Měly by být prováděny pravidelné kontroly, aby bylo zajištěno, že součásti systému elektronického hlasování fungují v souladu s technickými specifikacemi systému a že jeho služby jsou dostupné.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za částečně splněné, pokud je zdrojový kód veřejně přístupný a je odborníky kontrolován)

40(h) Infrastruktura elektronického hlasování je bezpečná [2] - I-1, IAP-3

Klíčové zařízení pro elektronické hlasování by mělo být umístěno v zabezpečené oblasti a tato oblast musí být po dobu voleb nebo referenda chráněna proti jakémukoliv neoprávněnému zásahu nebo přístupu.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 v členských státech EU lze považovat za splněné, pokud je systém spravován certifikovanou hostingovou společností, která servery s hlasy má umístěné na území EU)

40(i) Existují plány obnovy po havárii [3] - MA-9

Během volebního období nebo období referenda by měl být zaveden plán obnovy po havárii.

40(j) Možnost kontroly stavu ochrany hlasovacího zařízení [3] - MA-1, MA-3, MA-4, MA-5, MA-7

Stav ochrany hlasovacího zařízení by mělo být možné kdykoli zkontrolovat. Osoby odpovědné za zařízení by měly používat speciální monitorovací postupy, aby se zajistilo, že během období hlasování bude hlasovací zařízení a jeho použití splňovat požadavky.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud je dostatečně chráněno zařízení hlasovacího systému; v rámci státního hlasování by státy měly brát v úvahu riziko napadení hlasovacího zařízení voliče, kterým může být PC, tablet či mobilní zařízení, a programy pro odevzdání hlasu pouze na systémy a zařízení, kde lze s velkou mírou jistoty zajistit bezpečnost)

40(k) K dispozici jsou trvalé plány zálohování [3] - IAP-4, I-3, ESWD-5

Měla by existovat dostatečná záložní opatření, která by měla být trvale k dispozici, aby bylo zajištěno, že hlasování bude probíhat hladce. Jakýkoli záložní systém by měl odpovídat stejným standardům a požadavkům jako původní systém.

40(l) Protokoly reakce na incidenty dostupné personálu [3] - I-2

Dotčení zaměstnanci by měli být připraveni rychle zasáhnout v souladu s postupem vypracovaným příslušnými volebními orgány.

40(m) Po volbách bezpečně uloženo [2] - M-2

Veškeré údaje uchovávané po volbách nebo referendu by měly být bezpečně uloženy.

41 Přístup k infrastruktuře mají pouze oprávněné osoby [2] - I-1, SWD-2, EWSD-3

K centrální infrastruktuře, serverům a volebním datům mají přístup pouze osoby pověřené volebním řídicím orgánem. Jmenování osob oprávněných k elektronickému hlasování bude jasně upraveno.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud zajištění přístupu k infrastruktuře garantuje provozovatel internetového hlasování)

41(a) Přístup do systému omezen na nezbytnou funkci [2] - I-4, SWD-2

Jmenované osoby mají omezený přístup ke službám elektronického hlasování v závislosti na jejich uživatelské identitě nebo uživatelské roli. Autentizace uživatele by měla být účinná před provedením jakékoli akce. Oddělení povinností by mělo být jasné a přísně vynucované prostřednictvím technických opatření.

41(b) Pravidlo dvou osob, povinné podávání zpráv a monitorování během hlasování [3] - SWD-2

V době, kdy je otevřena elektronická volební urna, by jakékoli oprávněné zásahy ovlivňující systém měly být provedeny týmy nejméně dvou lidí, měly by být předmětem zprávy, být sledovány zástupci řídicího volebního orgánu a případnými volebními pozorovateli.

41(c) Pravidlo dvou osob pro jinou kritickou technickou činnost [3] - SWD-2

Jakákoli jiná kritická technická činnost by měla být prováděna týmy nejméně dvou lidí. Složení týmů by se mělo pravidelně obměňovat. Tyto aktivity by měly být pokud možno prováděny mimo volební období. Měly by být předmětem zprávy.

42 Nasazený hlasovací systém je originální a funguje správně [3] - MA-7

Před konáním elektronických voleb se řídicí volební orgán přesvědčí, že systém elektronického hlasování je pravý a správně funguje.

42(a) Kontrola vybavení před každými volbami [3] - ESWD-12

Před každými volbami by mělo být vybavení zkontrolováno a schváleno v souladu s protokolem vypracovaným příslušnými volebními orgány. Zařízení by mělo být zkontrolováno, aby bylo zajištěno, že odpovídá technickým specifikacím. Zjištění by měla být předložena příslušným volebním orgánům.

43 Aktualizace softwaru jsou znovu certifikovány [3] - SWD-14

Stanoví se postup pro pravidelnou instalaci aktualizovaných verzí a oprav veškerého příslušného softwaru.

43(a) Postupy zavádění infrastruktury včetně aktualizace [3] - I-7

Měly by být vyvinuty formální postupy pro nasazení softwaru a konfigurací technologie hlasování. Měly by být stanoveny termíny pro aktualizace. Aktualizace, které jsou distribuovány, by měly být ověřeny (podepsány).

44 Po odevzdání je zašifrovaný hlas neměnný [2] - E2Ev

Jsou-li hlasování uložena nebo sdělována mimo kontrolovaná prostředí, musí být zašifrována.

45 Před zahájením sčítání byly zapečetěny informace o hlasech a voličích [2] - CR

Hlasy a informace o voličích musí být zapečetěny až do zahájení procesu sčítání.

(Pozn. autora: informace o voličích a volební účasti může mít pouze volební komise)

46 Bezpečná manipulace s kryptografickým materiálem volebním orgánem [2] - CR

Řídicí volební orgán nakládá s veškerým kryptografickým materiálem bezpečně.

46(a) Ceremonie generování kryptografického klíče přístupná veřejnosti [4]

Soukromé kryptografické klíče by měly být vygenerovány na veřejné schůzce a měly by být rozděleny na samostatné části a sdíleny alespoň dvěma lidmi, u kterých je nepravděpodobné, že by se domluvili.

47 Incidenty integrity jsou hlášeny [2] - I-5, MA-9

Pokud dojde k incidentům, které by mohly ohrožit integritu systému, osoby odpovědné za provoz zařízení neprodleně informují volební řídicí orgán.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud je alespoň umožněno odhalení chyb, které umožní zneplatnit volby a vyhlásit nový termín voleb)

47(a) Ohrožení integrity specifikované předem [3] - I-5, MA-9

Druhy incidentů jsou předem specifikovány volebními orgány.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud jsou možné incidenty definovány například v akademických publikacích, kdy mohou být zkoumány například systémy s otevřeným zdrojovým kódem)

47(b) Specifikováno zmírnění následků incidentu [3] - I-5, MA-10

V případě incidentu by příslušné volební orgány měly přijmout nezbytná opatření ke zmírnění dopadů incidentu.

(Pozn. autora: v rámci nestátního hlasování do úrovně 3 lze považovat za splněné, pokud má volební komise možnost jednoduše zneplatnit volby a vyhlásit opakované)

48 Autentičnost, dostupnost, integrita seznamů voličů/kandidátů, GDPR [2] - IAP-5

Autenticita, dostupnost a integrita seznamů voličů a seznamů kandidátů bude zachována. Zdroj údajů musí být ověřen. Je třeba dodržovat ustanovení o ochraně údajů.

48(a) Zabezpečení procesu tisku voličských průkazů [3]

Tisk identifikačních údajů voličů, jako jsou volební karty, by měl být přezkoumán, aby byla zajištěna bezpečnost citlivých údajů.

(Pozn. autora: pokud volební systém průkazy netiskne, lze považovat za splněné)

49 Systém identifikuje hlasování s nesrovnalostí [3] - E2Ev

Systém elektronického hlasování identifikuje hlasy, které jsou ovlivněny nesrovnalostí.

49(a) Systém potvrdí odevzdání hlasů v časovém limitu [2] - E2Ev

Skutečnost, že se hlasovalo v předepsaných lhůtách, by měla být zjistitelná.

4.5.9 Doplnující požadavky

I na základě neformálního nestrukturovaného rozhovoru (Respondent - IT expert na kybernetickou bezpečnost) nelze považovat požadavky Rady Evropy za úplný výčet požadavků pro zajištění bezpečného tajného internetového hlasování. Požadavky lze chápat jako minimální požadavky, které nejsou konečným výčtem. Na základě provedené významové ekvivalence v rámci komparativní analýzy byly identifikovány další dodatečné požadavky, které nejsou dostatečně jasně zahrnuty v požadavcích Rady Evropy zahrnuty.

Požadavky (Marcos del Blanco, 2018a), které se týkají přímo volebního softwaru a nebyly identifikovány v požadavcích Doporučení Rady Evropy (Council of Europe, 2017) jsou doplněny jako požadavky začínající číslem 50:

50(a) Hlasovací proces musí nabízet možnost být kdykoli ukončen bez záznamu - SWD-8

Hlasovací systém může volič kdykoliv ukončit, aniž by se ukládaly jakékoliv informace ohrožující soukromí voliče.

50(b) Bez odkazů na třetí strany - SWD-10

Software nesmí umožňovat přístup třetích stran (včetně sociálních médií) ani obsahovat odkazy na programy/stránky mimo infrastrukturu elektronického hlasování.

Pokud by se jednalo o internetový volební systém založený na blockchainu je nutné s větším důrazem zvažovat některé požadavky, zda jsou dostatečně naplněny (Cucurull, 2019), konkrétně je nutné se zaměřit na bezpečnou agregaci v případě více kanálů hlasování nebo informování v případě odevzdání neplatného hlasu. Kromě toho na základě studie od Curuculla (2019) navrhuje autor doplnit další dva požadavky:

50(c) Systém zajišťuje "věčné soukromí"

V rámci věčného soukromí nesmí být umožněno nikdy, včetně vzdálené budoucnosti, prolomit tajnost hlasování.

(Pozn. autora: v případě, že jsou hlasy po ukončení, vyhodnocení voleb a případném rozhodnutí správního orgánu trvale smazány a současně nebyly nikdy zobrazeny jejich hash přímo v souvislosti s konkrétními voliči, lze považovat dodržení věčného soukromí za splněné)

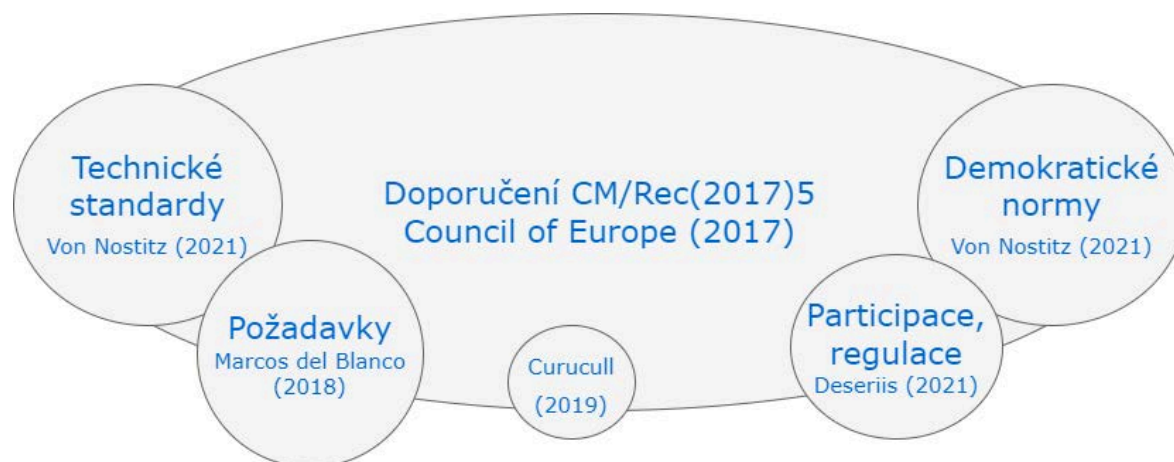
50(d) Systém zajišťuje škálovatelnost

Každý volič může odevzdat hlas kdykoliv během doby hlasování bez ohledu na zatížení systému či systémové nároky na odevzdání hlasu.

(Pozn. autora: pokud systém počítá s tím, že jsou započítány i hlasy odevzdané včas, které dorazí po skončení volebního období kvůli blockchainovému vyřizování transakcí s výrazným zpožděním, lze považovat bod za splněný)

4.6 CoMEvIS - metodika komplexního hodnocení systémů internetového hlasování v rámci tajných voleb

Na základě syntézy poznatků z předchozích částí výzkumu navrhuje autor novou metodiku komplexního hodnocení systémů internetového hlasování CoMEvIS (*Comprehensive Methodology of Evaluating I-voting Systems*). Metodika je využitelná jako koncept hodnocení v podobě metodického frameworku, který vychází z kvantifikovatelného hodnocení pomocí inovativního technického pracovního listu (Martínek, 2024a) s určením minimálních požadavků dané úrovně a popisného hodnocení dalších důležitých vlastností systémů. V rámci metodiky je tak spojen vlastní výzkum s dalšími koncepty hodnocení, které zachycuje obrázek 22.



Obrázek 22: Množina požadavků zahrnutých v hodnotící metodice CoMEvIS (vlastní zpracování)

Hodnocení by měl provádět nezávislý odborník, který by měl mít v rámci pozorování a testování přístup ke zdrojovému kódu, veškeré dokumentaci i zařízením. Pro případ ověření výsledků konkrétního hodnocení je možné provést hodnocení vícekrát s využitím více odborníků. Hodnocení by mělo v rámci závěrečné zprávy zahrnovat výstup ze zpracovaného technického pracovního listu (Martínek, 2024a) i popisné hodnocení dalších vlastností systému — viz podkapitoly níže.

Výhodou navrženého metodického postupu hodnocení je možnost hodnotit stávající nasazené volební systémy i plánovanou metodiku pro provedení tajného vzdáleného

elektronického hlasování, pokud již existuje i software, případně jeho dostatečná dokumentace.

V případě nevyhovujícího hodnocení lze upravit stávající systém nebo plánovanou metodiku pro provedení tajného vzdáleného elektronického hlasování a provést hodnocení znovu. V případě změny systému či způsobu jeho využívání je nutné provést nové hodnocení, protože původní hodnocení pozbývá platnosti.

4.6.1 Hodnocení technických standardů a demokratických norem

Základem konceptu hodnocení je inovativní technický pracovní list zveřejněný autorem na Zenodo (Martínek, 2024a) jako open source. Ten zahrnuje určení úrovně internetového hlasovacího systému (Kapitola 4.4) a jednoduché vyhodnocení požadavků Doporučení Rady Evropy (Council of Europe, 2017) zahrnující i doplňující požadavky (Kapitola 4.5).

Technický pracovní list (Martínek, 2024a) dokáže dle zadaných údajů určit úroveň, pro kterou jsou splněny minimální požadavky. Vyplňují se hodnoty 1 (splněno), 0 (nesplněno), případně jiná hodnota v rozmezí mezi 0 a 1, která je vyhodnocena jako nesplněno, ale může signalizovat částečné splnění pro další zpracování. Přesto je nutné uvést, že každý systém elektronického hlasování pro tajnou vzdálenou volbu by měl splňovat všechny požadavky Doporučení CM/Rec(2017)5 Rady Evropy (Council of Europe, 2017), doplňkové požadavky i další kritéria.

Aby bylo maximálně ulehčeno vyplňování je technický pracovní list doplněn o další list obsahující instrukce, autorské poznámky pro určení splnění některých bodů a další užitečné informace.

V rámci požadavků Doporučení Rady Evropy (Council of Europe, 2017) lze například pro hodnocení použitelnosti využít standardní způsoby evaluace použitelnosti (Acemyan, 2014; Ander, 2022). Speciálně je potřeba vyhodnotit shodu s minimálně WCAG 2.0 AA (W3C, 2008) od WAI (W3C Web Accessibility Initiative (WAI), 2023), i když optimální by bylo splnění aktuální novější verze WCAG 2.2 AA a vyšší (W3C, 2023). K vyhodnocení splnění WCAG 2.0 AA lze použít nástroje jako je například Accessibility Checker (2024) nebo jiný ze seznamu W3C (2024), které je nutné doplnit o manuální testování (W3C, 2008; W3C Web Accessibility Initiative (WAI), 2023).

Mezi další standardizované způsoby hodnocení, které mohou pomoci vyhodnotit některé požadavky, jsou technické normy jako ISO 27001 (ISO, 2022), ISO 27017 (ISO, 2015a), které by měl splňovat poskytovatel infrastruktury, případně i provozovatel. Při vyhodnocování bodů týkajících se auditních nebo certifikačních zpráv, či analýzy a řízení rizik, řízení aktiv, evidence zranitelností a incidentů, řízení identit a přístupů lze podrobněji prostudovat části metodiky (Marcos del Blanco,

2018a) přiložené v české verzi v Příloze A. Bezpečnost použitých kryptografických protokolů lze ověřit pomocí automatického nástroje ProVerif (Blanchet, 2022).

Po vyplnění dokáže technický pracovní list (Martínek, 2024a) kromě úrovně (Kapitola 4.4) doplnit také celkový počet splněných požadavků ze 143 požadavků Rady Evropy (Council of Europe, 2017), stanovit procento splnění požadavků, určit počet alespoň částečně splněných požadavků včetně procenta a určit míru splnění dle subjektivní evaluace hodnotitele.

Do technického pracovního listu (Martínek, 2024a) by měl být definován hodnocený systém, termín hodnocení, určení hodnotitele a kontakt. Ukázka vyplnění je k dispozici v přílohách F a G, které hodnotí systémy podrobně evaluované v člancích (Martínek, 2024d; Martínek, 2024e). V závěrečné zprávě zahrnující i technický pracovní list by mělo být uvedeno více podrobností, nevylučuje se ani zahrnutí více technických pracovních listů od více hodnotitelů.

Poznámky k jednotlivým bodům, kde není splnění jasné, lze popsat v rámci závěrečné hodnotící zprávy.

4.6.2 Hodnocení regulace, předpisů a jiných norem užití

Technický pracovní list (Martínek, 2024a) částečně hodnotí regulaci především v požadavcích 27 až 30. I přesto by mělo být v rámci hodnocení podrobně popsáno jaké regulace se k danému systému vztahují, aby mohlo dojít k jejich případnému doplnění například v rámci interních předpisů. Ukázku takového to popisného hodnocení lze nalézt v člancích v přílohách H, J, K (Martínek, 2024d; Příloha J; Příloha K).

4.6.3 Hodnocení participace na hlasování

V případě, že se volby provádí méně často, třeba jen několikrát za deset let, nebo se jedná o nový systém, je hodnocení participace složité. V prvním případě by i tak mělo být možné vyhodnotit, zda existuje nějaký vliv zavedení internetového hlasování na účast - případně zda lze definovat přímo určitý trend (Příloha K). Míra účasti může naznačit míru přijetí systému voliči. U pravidelně využívaných internetových hlasovacích systémů, kde probíhá několik typově stejných voleb ročně je hodnocení trendu účasti v rámci participace jednodušší. V článku (Martínek, 2024d) navrhuje autor počítat volební účast (T) pro každou hlasovací akci podle následujícího vzorce:

$$T = \left(\frac{V}{M} \right) \times 100 \quad (41)$$

Kde:

- T je volební účast v procentech,
- V je počet hlasujících,
- M je celkový počet oprávněných voličů.

Výpočet průměrné volební účasti (T_{avg}) za celý rok by pak byl vypočítán:

$$T_{avg} = \frac{\sum_{i=1}^n T_i}{n} \quad (42)$$

Kde:

- T_i je volební účast pro i -té hlasování v daném roce,
- n je celkový počet hlasovacích událostí v daném roce.

Průměrná volební účast je klíčovým ukazatelem participace na hlasování (Příloha J). Vyšší účast může naznačovat vyšší angažovanost voličů a vyšší míru přijetí elektronického hlasovacího systému. Naopak nízká účast může naznačovat potřebu úpravy systému nebo větší mobilizace voličů.

Trend volební účasti určuje, zda účast vykazuje ve sledovaném období rostoucí, klesající, nebo stabilní tendenci. K výpočtu trendu volební účasti lze použít lineární regresi (Montgomery, 2010), kde nezávislou proměnnou (x) jsou roky a závislou proměnnou (y) je průměrná volební účast (T_{avg}) pro každý rok. Rovnice lineární regrese má tvar:

$$y = a + bx \quad (43)$$

Kde:

- y je průměrná volební účast,
- x je rok,
- a je intercepce,
- b je sklon, který představuje změnu za jednotku času (roku).

Regresní koeficienty a a b se vypočítají podle následujících vzorců:

$$b = \frac{n \sum_{i=1}^n (x_i y_i) - \sum_{i=1}^n x_i \sum_{i=1}^n y_i}{n \sum_{i=1}^n x_i^2 - \left(\sum_{i=1}^n x_i \right)^2} \quad (44)$$

Kde b udává, zda se volební účast v průměru každý rok zvyšuje nebo snižuje, a a :

$$a = \frac{\sum y_i - b \sum x_i}{n} \quad (45)$$

Kde:

- n je počet let,
- x_i je i -tý rok,
- y_i je průměrná účast v i -tém roce.

Kromě samotné účasti je vhodné hodnotit systém, stejně jako v případě jiných forem hlasování, i dle možnosti zapojení reprezentace kandidátů a dodržení dalších demokratických principů, jako je naznačeno v člancích (Martínek, 2024d; Příloha J). Vyhodnoceno by tak mělo být také dodržení ústavních zásad jako je všeobecnost hlasování. V rámci hodnocení volebního systému by se mělo hledět na reprezentativnost, možnost soutěže kandidátů a další parametry typické i pro tradiční způsoby voleb. To vše by měl hodnotitel popsat v závěrečné zprávě.

4.6.4 Hodnocení transparentnosti

Základem volebního systému je důvěra voličů, kteří ho mají používat. Volič by měl chápat, jak systém funguje. Nemělo by nastat, že se systém uzavře do “black boxu”, kde voliči (Příloha K), někdy dokonce i správci systému, nebudou dostatečně schopni ověřit fungování systému. Aby tak mohlo dojít k důvěryhodnému nezávislému hodnocení daného systému, měl by být v optimálním případě dostatečně transparentní minimálně vůči voličům — jak je rozebíráno ve článku (Martínek, 2024d), alternativně by měl umožnit hodnocení systému na základě transparentního přístupu povoleného odborníkům pro provedení auditu. To může zahrnovat i přístup odborníků ke zdrojovým kódům systému na základě podepsaných NDA. V mnoha případech je vhodné na požadavek transparentnosti myslet již při zadávání podmínek soutěže na daný systém. Hodnocení transparentnosti je hodnoceno v rámci technického pracovního listu (Martínek, 2024a) vyhodnocením požadavků 31 - 35, obecně by mělo být popsáno i v závěrečné zprávě.

4.6.5 Hodnocení nákladovosti, zajištění kontinuálního vývoje a podpory

Stejně jako u každého systému ve veřejné správě bude pravděpodobně nutné hodnotit i nákladovost systému. Z hlediska metodiky Marcos del Blanco (2018a) v Příloze A by měl dodavatel srozumitelně a transparentně definovat náklady na implementaci systému. Současně je nutné myslet na správu, údržbu a případný rozvoj daného systému. Celková cena rozpočítaná na odevzdané hlasy internetovou formou by neměla výrazně překračovat náklady jiných možností hlasování. V případě estonských voleb bylo spočítáno (Krimmer, 2018), že elektronické hlasování je nejlevnějším způsobem odevzdání hlasu. Hodnocení nákladovosti, zajištění kontinuálního vývoje a podpory by mělo být popisně shrnuto v závěrečné zprávě.

4.6.6 Dodatečná hodnotící kritéria

Pro některé zadavatele existují další významná kritéria, která by měla být zahrnuta do evaluace. Může se jednat například o všestrannost, pokud zadavatel počítá i se složitějšími způsoby hlasování, které mohou obsahovat i alternativní způsoby voleb typu pořadí. V každém případě tato dodatečná kritéria hodnocení by měl zadavatel evaluace jasně definovat, v některých případech by měly být součástí zadávací dokumentace.

I v metodice Marcos del Blanco (2018a) lze nalézt kritéria, která lze považovat za benefitní či nadbytečná. Mezi nimi je například požadavek V-3, který vyžaduje možnost odeslání hlasu bez nutnosti instalace dodatečného software. I v estonských volbách (Valimised.ee, 2024a) se pro zvýšení bezpečnosti hlasuje pomocí speciálního softwaru instalovaného na osobní počítač.

Součástí závěrečné zprávy by měl být vyhodnocený technický pracovní list, konkrétní formální náležitosti závěrečné zprávy nejsou touto prací definovány, ale je definován základní obsah v rámci kapitoly 4.6. Pro inspiraci vyplnění závěrečné zprávy lze využít přílohy H, I, K, ve kterých jsou články autora práce (Martínek, 2024d; Martínek, 2024e).

5 Diskuze

V posledních letech se rozvíjí využití tajného internetového hlasování především v rámci různých institucí (Martínek, 2024d; Příloha J, Příloha K), k Estonsku přibývají další státy, které i přes kritiku zavádějí možnost hlasovat přes Internet v celonárodních volbách (Epifanova, 2021; Sauer, 2021; The Bell, 2024) bez toho, aniž by prošel systém nezávislým transparentním hodnocením, které by prokázalo dodržení demokratických norem a technických standardů. V rámci členských zemí Rady Evropy by mělo být zvažováno při evaluaci doporučení (Council of Europe, 2017), které je zahrnuto i v rámci nového metodického hodnocení definovaného touto prací.

Transparentnost v internetových hlasovacích systémech (Martínek, 2024e) je klíčová podle doporučení Rady Evropy (Council of Europe, 2017) i pro posílení důvěry veřejnosti. Výzkum švýcarského volebního systému (Driza Maurer, 2019) rovněž klade důraz na nutnost transparentnosti. Buckland (2012) a jeho kolegové poukazují na to, že nedostatek otevřenosti australského systému elektronického hlasování může negativně ovlivnit voličské postoje k internetovému volebnímu systému. Volkamer (2011) s kolegy také považují transparentnost za zásadní pro důvěryhodnost voleb. Přesto jen málo zemí zavedlo odpovídající zákony nebo standardy pro online volební systémy (Brunet, 2022).

Plnohodnotné hodnocení systémů pro internetové hlasování je možné pouze u open source systémů, jako je například Helios Voting (Panizo Alonso, 2018; Martínek, 2024d), Belenios (Cortier, 2020; Martínek, 2024e), nebo v případech, kdy vývojáři úzce spolupracují, jako je tomu u systémů Scytal iVote (Marcos del Blanco, 2019) či nVotes (Marcos del Blanco, 2020). Částečné hodnocení je možné provádět na základě pozorování, jak tomu je u systému Neovote v práci Blanchard (2022), kde pozorování odhalilo, že Neovote nesplňuje požadavky stanovené CNIL (La Commission nationale de l'informatique et des libertés, 2019). Při tomto způsobu hodnocení ovšem nelze plnohodnotně potvrdit splnění všech demokratických norem a technických standardů. Pokud by tak bylo provedeno hodnocení konceptem dle této práce bez přístupu ke zdrojovému kódu (Příloha K), zařízením i veškeré dokumentaci, tak dané hodnocení nelze považovat za plnohodnotné.

Systémy elektronického hlasování se výrazně liší od ostatních informačních systémů, kde lze případné chyby, manipulace, či jejich následky mnohdy snadno odhalit a opravit. I dle respondentů (Martínek, 2024g) není přednostní zaměření na efektivitu internetových volebních systémů na úkor jejich transparentnosti žádoucí, jak je tomu v případě „black box“ systémů (Cheeseman, 2018). V případě respondentů z řad správců internetových volebních systémů univerzit (Příloha K) byla často zdůvodňována neochota poskytnout dostatečné informace odvoláním se na bezpečnost systému. Správci sami v některých případech neměli informace o tom,

jak daný systém funguje. Nedostatečná transparentnost potřebná pro hodnocení systému má negativní dopad na důvěryhodnost volebního procesu (Příloha K). Sami potenciální voliči (Martínek, 2024g) přitom vyjadřují vysokou míru souhlasu s požadavky na transparentnost, ověřitelnost, přehlednosti či bezpečnost (Martínek, 2024e; Příloha K).

Respondenti (Martínek, 2024g) často zdůrazňovali, že kvůli obavám o zabezpečení systému nechtějí poskytnout dostatek informací, a někdy sami neměli přehled o tom, jak daný systém funguje. Nedostatek transparentnosti, která je nezbytná pro hodnocení systému, tak negativně ovlivňuje důvěryhodnost volebního procesu (Příloha K).

Inspiraci lze čerpat i z transparentního zavádění a kontroly i-hlasovacích systémů v rámci politicky závazných celonárodních voleb. Například v Norsku bylo při implementaci elektronického hlasování na dálku vypsáno transparentní výběrové řízení (Ministry of Local Government and Regional Development, 2010), přičemž požadavek na open source umožnil technickou analýzu systému (Bjørstad, 2013), která odhalila zranitelnosti k následné opravě. Podobně v Estonsku je většina zdrojového kódu volebního systému zveřejněna (Valimised, 2024), což umožnilo provedení bezpečnostních analýz (Springall, 2014; Heiberg, 2015a; Pereira, 2023), díky nimž byl systém upraven pro zvýšení bezpečnosti. V Estonsku je tak systém pravidelně aktualizován, aby byla zajištěna vyšší bezpečnost a integrita voleb, což přispívá k posílení důvěryhodnosti elektronického hlasování na dálku (Příloha K). Proto již v zadávací dokumentaci lze vyžadovat alespoň splnění požadavků Doporučení Rady Evropy (Council of Europe, 2017), kde jejich splnění včetně zhodnocení dalších požadavků umožňuje nový koncept hodnocení definovaný touto prací.

Na personální politiku (Martínek, 2014; Martínek, 2018) stejně jako volby mají vliv sociální sítě (Martínek, 2013; Pal, 2020), proto by se v rámci hodnocení dodržení demokratických norem nemělo zapomínat ani na transparentnost kampaně včetně využití komunikačních kanálů s voliči zahrnující i sociální sítě. Mezi možné nástroje ve volebním právu cílené na sociální sítě patří pravidla pro transparentnost zahrnující zveřejňování, či omezování kampaňových výdajů a donucovací opatření knápravě. Obdobně je vyžadován také nový přístup k digitální informační rovnosti s ohledem na dezinformace za účelem zajištění integrity voleb (Judge, 2020). Pro zlepšení digitální informační rovnosti s ohledem na kontrolu kvality a důvěryhodnosti webů autor práce zpřístupnil zdrojový kód rozšíření *KontrolaWebu.pridat.eu* pro prohlížeče Google Chrome a Mozilla Firefox, které kontroluje přítomnost domény daného webu na seznamu dezinformačních webů *Konspiratori.sk* a seznamu rizikových internetových stránek České obchodní inspekce a v případě nalezení shody upozorňuje uživatele varovnou lištou v horní části prohlížeče (Martínek, 2024f).

5.1 Vyhodnocení výzkumných otázek

V následující části jsou v rámci závěrečné diskuze odpovědi vzešlé z výzkumu na jednotlivé výzkumné otázky:

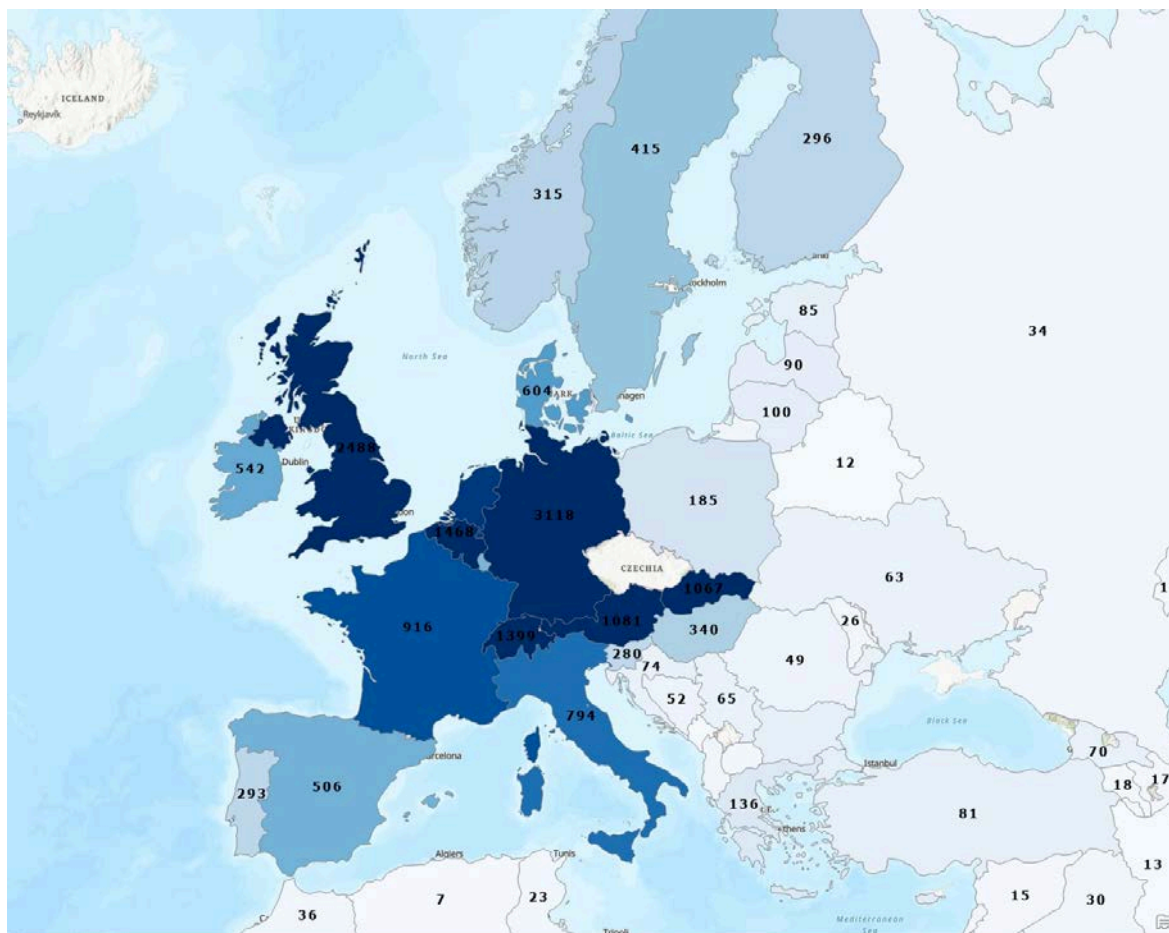
5.1.1 Jak se v České republice využívá tajné internetové hlasování? (V01)

V České republice je známá používáním tajného internetového hlasování v rámci vnitrostranického hlasování Česká pirátská strana, především během pandemie si vyzkoušeli hlasování přes Internet i Starostové a nezávislý nebo Zelení (Martínek, 2024d). Hojně se internetové hlasování používá také na českých vysokých školách, pro volby do akademického senátu využilo internetové hlasování již 18 z 26 veřejných vysokých škol (Příloha K). Hlasování přes Internet se snaží zavést také některé spolky, komory, družstva, SVJ, či jiné společnosti (Martínek, 2024e).

5.1.2 Jak je Česká republika digitálně připravena na zavedení internetového hlasování v rámci politicky závazných voleb? (V02)

Jak je popsáno v kapitole 3.5.2 existují v Česku dobré základy pro možnou digitalizaci. Existuje zastřešující Digitální a informační agentura (DIA, 2024), na území státu SPCSS provozuje několik datových center (SPCSS, 2024), vydávají se občanské průkazy s čipem, které lze využít pro přihlášení nejvyšší úrovně (Identita občana, 2024), stát má k dispozici řadu vlastních vývojářů včetně Národní agentury pro komunikační a informační technologie (NAKIT). Certifikáty lze vydávat prostřednictvím Správy státních služeb vytvářejících důvěru (SSSVD, 2024). Problémem může být to, že neexistuje jednotný registr voličů, místo toho si seznam stálých voličů spravují jednotlivé obce (Ministerstvo vnitra ČR, 2022). V případě centralizovaného řešení by tak musel být nejprve vytvořen jednotný registr voličů, nebo by se internetové hlasování mohlo zavést decentralizovaně, jako tomu je například v Kanadě (Goodman, 2023). Kanadské decentralizované zavádění systémů ovšem sklízí v rámci jeho hodnocení kritiku (Goodman, 2014; Brunet, 2023) a i centralizované řešení v rámci estonských voleb má své kritiky (Springall, 2014; Heiberg, 2015a; Pereira, 2023).

Největší pozitivní dopad internetového hlasování vzhledem k volební účasti by měl být pozorován v případě vzdálených volebních místností (Garnett, 2021). V České republice nejsou většinou volební místnosti vzdáleny více než několik kilometrů. Problém mohou mít ovšem čeští voliči v zahraničí, jak naznačuje obrázek 23 zobrazující Evropu s počty odevzdaných hlasů v jednotlivých zemích.



Obrázek 23: Počet odevzdaných hlasů v prvním kole českých prezidentských voleb v roce 2023 v jednotlivých zemích Evropy v zahraničí dle dat Českého statistického úřadu (Martínek, 2024b)

Ve většině zemí Česko během voleb zřizuje jednu volební místnost, nejvíce volebních místností (4) je v Německu a USA. V některých zemích, jako jsou například Island, či Kosovo, v Evropě a mnoha zemích mimo Evropu, není volební místnost žádná. Celosvětově tuto situaci zachycuje obrázek 24. Tato situace je tak těžká pro české krajané, kteří nesídlí v zemi, kde je volební místnost, nebo je volební místnost v dané zemi příliš vzdálená. Během pandemie COVID-19 by například čeští krajané žijící na Novém Zélandu museli letět do nejbližší volební místnosti v Austrálii, kde by museli podstoupit karanténu stejně jako v případě návratu na Nový Zéland, kde přitom již nepouštěli zpět občany bez přiděleného trvalého pobytu. Stejně tak byla možnost vykonání volebního práva omezena kvůli restrikcím pohybu i snížení frekvence letecké nebo lodní dopravy (Martínek, 2024b).

V současné době se připravuje možnost distanční volby pro české voliče v zahraničí. Protože internetové hlasování vychází dle Kapitoly 3.1 v mnoha ohledech lépe než korespondenční (Puiggali, 2007; Willemson, 2017; Martínek, 2024b), je ke zvážení zavedení možnosti internetového hlasování pouze pro voliče v zahraničí.

(Respondent - ústavní právník), je nutné na volební systémy, kde výsledek voleb může mít dopad na rozhodnutí v rámci veřejné správy (například politické volby, rozhodnutí změny stanov v SVJ apod. — tedy primárně od definované úrovně 3) brát zvláštní zřetel. V tomto případě se nabízí inspirace francouzskou legislativou, která vyžaduje splnění minimálních požadavků alespoň v rámci doporučení národní komise pro informatiku a svobodu (La Commission nationale de l'informatique et des libertés, 2019). Tato práce nabízí podklady pro přijetí, nejdříve nezávazného, doporučení například v rámci některého podvýboru Poslanecké sněmovny.

5.1.4 Mělo by zavedení možnosti internetového hlasování v celonárodních volbách vliv na volební účast a strukturu volebních výsledků? (VO4)

Zahraniční studie prokazuje snižující se volební účast v případě tradičního hlasování ve vzdálenějších volebních místnostech (Garnett, 2021), což by v České republice mohlo mít v případě zavedení internetového hlasování pozitivní vliv především v zahraničí. Podle dřívějšího výzkumu autora zahrnující menší dotazníkového šetření (Martínek, 2017) by se dalo odvodit určité zvýšení volební účasti i určitá změna struktury volebních výsledků.

5.1.5 Jakým způsobem snížit riziko nátlaku na voliče zahrnující i dobrovolnou spolupráci s korupčnímkem v rámci vzdálených elektronických voleb? (VO5)

Často řešeným požadavkem na internetové hlasovací systémy je odolnost nátlaku. Nátlak, kupčení s hlasy a korupce ve volbách je prokázaným rizikem (Walsh, 2008) dokonce i v České republice (Transparency International, 2014). V rámci výzkumu (Příloha K) zastávali někteří univerzitní správci internetových volebních systémů názor, že nepovažují možné ovlivňování hlasování v rámci voleb do akademických senátů za relevantní problém, který by bylo nutné řešit. Jak naznačují některé zprávy — například z voleb v Rusku (Romanov, 2020; Epifanova, 2021; Sauer, 2021; The Bell, 2024) — je nucení k volbě možným problémem, který by se měl zohledňovat i přesto, že dle výzkumu (Martínek, 2024d) hlasovalo za přítomnosti třetí osoby dle jejího přání pouze 2,35 % voličů a obdobně se k tomu staví i potenciální uživatelé internetového hlasování (Martínek, 2024g).

Na druhou stranu plná odolnost vůči nátlaku je problematicky dosažitelná i v ostatních způsobech hlasování. V rámci korespondenčního hlasování je maximálně dosažitelná úroveň odolnosti nátlaku nižší než u elektronických volebních systémů (Puiggalí, 2007). V rámci klasických papírových voleb také není zaručena odolnost nátlaku, zkorumpovaný volič může být sledován u volební urny například pomocí různých sledovacích zařízení včetně chytrých brýlí (Benaloh, 2013). Během českých voleb je možné jít se zkorumpovaným či ovlivněným voličem až do volební místnosti, kde lze dohlédnout na to, že si nevezme sadu náhradních lístků a za plentu jde pouze

s jedním doneseným volebním lístkem. Problematické také je hlasování do přenosné volební urny, kdy mnohdy s odevzdáním hlasu musí pomáhat handicapovanému voliči další osoba.

Odolnost proti nátlaku je klíčovým požadavkem pro zabezpečení voleb. Nicméně plná odolnost proti nátlaku je obtížně dosažitelná i v tradičních volebních způsobech. V rámci internetového hlasování je odolnost nátlaku protikladem ověřitelnosti. Pokud má být zajištěno, že i dobrovolná volba za účasti uzurpátora tzv. “přes rameno”, bude odolná nátlaku, snižuje se míra ověřitelnosti. Pokud je umožněno voliči ověřit přítomnost svého hlasu ve volební urně pomocí sledovacího hash, nelze zabránit předání sledovacího hash pro ověření i uzurpátorovi. Estonsko zajišťuje odolnost nátlaku tím, že lze ověřit přítomnost hlasu ve volební urně pouze krátkou dobu po odevzdání hlasu, hlas lze kdykoliv do konce volebního období pro hlasování přes Internet změnit novým odevzdáním hlasu a navíc se následně může volič i nadále zúčastnit klasické volby pomocí papíru v kontrolovaném prostředí volební místnosti, čímž přepíše elektronicky odevzdaný hlas (Valimised.ee, 2024b). Za základ pro zmírnění nátlaku lze i dle Doporučení Rady Evropy (Council of Europe, 2017) považovat možnost opakovaného hlasování, kdy je započítána pouze poslední zvolená možnost. Některé systémy se snaží zvýšit odolnost nátlaku i dalšími způsoby, mezi které patří například falešné přihlašovací údaje pro hlasování (Clarkson, 2008), které umožní odeslat pouze neplatný hlas, nebo přítomnost všech sledovacích hashů ve volebních urně — včetně těch neplatných, které byly přepsány znovu odeslanými hlasy (Krips, 2019).

5.1.6 Jak zajistit dostupnost elektronických hlasovacích systémů pro vzdálenou volbu v době voleb? (VO6)

Všechny informační systémy vyžadují zajištění dostupnosti. Internetové hlasování je specifické v tom, že probíhá často velmi omezenou dobu, během které mají mít možnost odhlasovat všichni potenciální voliči. Pokud by měli možnost hlasovat všichni občané České republiky, jednalo by se o více než 8 milionů voličů. Mnoho informačních systémů by nápor milionů uživatelů v několika málo dnech těžko ustálo (Martínek, 2024e). V rámci ovlivňování voleb nejsou navíc vyloučeny DDoS útoky, které by mohly hlasovací služby zahltit a voličům hlasování znepřístupnit. Pro minimalizaci dopadů na infrastrukturu lze předpokládat využití nástrojů pro monitoring sítě a reakce (NDR), případně technologie EDR, pro monitoring koncových bodů na přítomnost hrozeb a provádění automatických reakcí. Kybernetická obrana proti robotům je často založena na různých úkolech formy CAPTCHA, či jiných automatických testech, které mají s určitou mírou pravděpodobnosti rozhodnout o tom, zda k systému přistupuje člověk nebo robot. U internetových voleb ovšem může nastat etický problém, protože může být chybným vyhodnocením zamezeno přístupu k systému i skutečnému člověku. Případné řešení tak pravděpodobně zůstane na bezpečnostním operačním centru

(SOC) monitorujícím provoz ve volební infrastruktuře, které by mělo existovat v případě významných voleb, které nelze jednoduše prodloužit či přeložit.

6 Závěr

Tato disertační práce si kladla za cíl komplexně analyzovat problematiku tajných elektronických voleb prováděných s využitím Internetu (DC3) a navrhnout novou metodiku hodnocení těchto systémů s ohledem na zachování demokratických norem, bezpečnosti a technických standardů (HC). Výzkum ukázal, že zavedení elektronického hlasování do politicky závazných voleb představuje náročný úkol, který vyžaduje pečlivé zvážení technologických, právních i společenských aspektů.

V první řadě bylo nutné vymezit základní rámec tajných elektronických voleb (DC1), který zahrnuje zkušenosti různých zemí, jako jsou Estonsko, Norsko, Austrálie, Kanada, USA, Francie nebo Švýcarsko, a popsat přístupy k zabezpečení a transparentnosti hlasovacích procesů. V rámci teoretických východisek v kapitole 3 autor prozkoumal také kategorizaci, standardizaci, legislativu, kryptografii, architekturu nebo bezpečnostní rizika elektronických volebních systémů. V kapitole 3.7 a v přílohách B, H, I jsou analyzovány dostupné open-source systémy, které umožňují tajnou elektronickou vzdálenou volbu. Analýzy a komparace (Martínek, 2024d; Martínek, 2024e; Příloha B) různých volebních systémů (DC1) lze interpretovat tak, že existuje řada open-source řešení, která jsou vhodná pro implementaci tajných voleb, avšak žádný z porovnávaných systémů nesplňuje všechna kritéria plně ve všech ohledech. Nejlepší výsledky vykazují systémy založené na ověřitelné kryptografii, která umožňuje nejen bezpečné hlasování, ale také jeho následné ověření. Bylo zjištěno, že klíčovým faktorem úspěchu implementace těchto systémů je silná důvěra veřejnosti v bezpečnost hlasování a ochranu soukromí voličů. Zkušenosti ukazují, že nedostatky v tomto směru mohou vést k narušení vnímání legitimacy voleb. To platí i v případě České republiky, u které byla zkoumána připravenost na zavedení vzdálené elektronické volby (DC2) v rámci kapitoly 3.5 i závěrečné diskuze s vyhodnocením výzkumných otázek. Přínosy a rizika provedení tajné ověřitelné vzdálené elektronické volby (DC3) jsou řešeny komplexně v rámci celé práce včetně příloh vycházejíce z kapitoly 3.1.

Pomocí dotazníkových šetření byly kvantitativně analyzovány (DC4) názory stávajících uživatelů (Kapitola 4.2) i potenciálních uživatelů internetového hlasování (Kapitola 4.3), jejichž podrobné vyhodnocení proběhlo v člancích autora dostupných v přílohách H, I, K. Obecně lze konstatovat, že voliči očekávají bezpečné, srozumitelné, ověřitelné a transparentní internetové hlasovací systémy, které nabídnou voličům dostatečnou dostupnost informací a řeší monitoring, testování i nápravná opatření v případě bezpečnostního incidentu.

Na základě teoretických východisek, analýzy názorů potenciálních uživatelů, komparace systémů internetového hlasování (Helios Voting, iVote od ScytL, nVotes, Belenios) dostupné v příloze B a ověření funkcí zdrojového kódu open source

systému Belenios došlo v článku v příloze I k návrhu a verifikaci metodického postupu provedení vzdálené elektronické volby (DC5). Navržený metodický postup umožňuje provést tajné internetové hlasování v organizaci s minimálními náklady.

Na základě polostrukturovaných rozhovorů s experty vybranými pomocí stanovení kategorií v rámci bilbiometrické analýzy (Kapitola 4.1) došlo s využitím rozhodovací metody BeCoMe k určení stanovených úrovní (DC6) jednotlivých požadavků doporučení Rady Evropy (Kapitola 4.4, Příloha C, Příloha D, Příloha E). Expertní šetření pomohlo určit významnost jednotlivých požadavků Doporučení Rady Evropy od nejdůležitějších (pro úroveň 1) po nejméně důležité (pro úroveň 5).

Na základě syntézy poznatků (DC7) z provedené rešerše, komparace současných software, analýz názorů stávajících i potenciálních uživatelů, expertního šetření s využitím rozhodovací metody BeCoMe, komparativní analýzy metodik (Kapitola 4.5) a dalších částí výzkumu byla navržena nová komplexní metodika hodnocení elektronických systémů pro tajné vzdálené volby, která reflektuje technické i demokratické požadavky na internetové hlasovací systémy (HC). Autorem navržená metodika CoMEvIS s určením minimálních úrovní jednotlivých požadavků umožňuje posouzení kvality volebních systémů na základě řady kritérií, jako je transparentnost, bezpečnost, ověřitelnost nebo náklady na provoz systému. Prostřednictvím inovativního technického pracovního listu (Příloha F, Příloha G) a popisného hodnocení dalších parametrů umožňuje provést komplexní hodnocení stávajících i připravovaných postupů provedení internetového hlasování, které mohou být implementovány pomocí různých systémů.

Celý výzkum je proveden v souladu s principy Open Science. Zdrojová data a výstupy jsou zveřejněny jako open source v rámci příloh práce nebo veřejně dostupná v univerzálním otevřeném repozitáři Zenodo (Martínek, 2024a; Martínek, 2024c; Martínek, 2024f; Martínek, 2024g; Martínek, 2024h) evropského programu OpenAIRE (OpenAIRE, 2024) v datovém centru CERN. Výzkum také přinesl odpovědi na formulované výzkumné otázky (Kapitola 5.1).

Závěrem (DC7) lze konstatovat, že vzdálené elektronické hlasování nabízí řadu výhod, zejména pro voliče vzdálené od volebních místností, nevidomé a osoby s omezenou mobilitou. Implementace systémů internetového hlasování však musí být prováděna s maximální opatrností a důrazem na dodržení technických standardů i demokratických norem. Základem by mělo být transparentní hodnocení systémů včetně metodického postupu provedení volby. Práce přinesla komplexní přehled problematiky elektronického hlasování přes Internet a dále důležitá doporučení pro další výzkum, zejména v oblasti zvýšení bezpečnosti volebních systémů, zajištění trvalého soukromí, vývoje a hodnocení systémů internetového hlasování.

6.1 Příležitosti budoucího výzkumu

V rámci budoucího výzkumu existuje příležitost zaměřit se na tvorbu a evaluaci elektronických systémů pro vzdálenou volbu, které by byly plně kompatibilní s demokratickými normami a technickými standardy. Případně se může jednat o výzkum v rámci certifikace systémů vzdáleného elektronického hlasování.

Speciálně se výzkumná příležitost nachází v rámci elektronických volebních systémů postavených na blockchainu, kde je nutné brát v úvahu trvalou povahu uložených dat v rámci veřejných blockchainů (Curucull, 2019).

Dále je výzkumná příležitost propojit evaluaci i s dalšími technologickými prostředky využívanými během voleb jako jsou sociální sítě, mediální dezinformace a jiné nástroje spojené s ICT. Kromě toho Evropská agentura pro kybernetickou bezpečnost zmiňuje riziko ovlivnění voleb pomocí manipulace s informacemi přes AI (ENISA, 2023), což je v rámci vědeckého výzkumu velmi aktuální téma.

Výzkum je možné soustředit také na customizaci AI, která by následně zvládla vyhodnotit systémy sama, i když za závěrečnou zprávu by měl i nadále nést odpovědnost člověk.

Výzkum se také může zaměřit na statistickou metodu s využitím software identifikující významné odchylky v rámci okrsků či minulých voleb obdobně, jako identifikuje extrémy a možné manipulace Shpilkinova metoda v Rusku (France24, 2024).

V neposlední řadě s ohledem na rozvoj kvantových počítačů je výzkumná příležitost v řešení dostatečné bezpečnosti u systému, které se spoléhají primárně na asymetrickou kryptografii.

Pro autory metody BeCoMe (Vrana, 2021) vzešlo v rámci výzkumu doporučení budoucího vědeckého bádání připravit technický pracovní list, který by umožňoval i hromadné vyhodnocování velkého množství otázek, protože stávající způsob vyhodnocování po jedné otázce je v případě většího počtu otázek zdlouhavý a neefektivní.

6.2 Přínosy práce

Hlavním přínosem práce pro odbornou i laickou veřejnost je nová metodika CoMEvIS, která zahrnuje i inovativní technický pracovní list (Martínek, 2024a) pro hodnocení systémů internetového hlasování dostupný jako open source. Pomocí určení úrovně požadavků lze hodnotit úroveň splnění technických standardů a demokratických norem.

Zpracováním disertační práce vznikl komplexní přehled problematiky elektronického hlasování přes Internet, který zahrnuje i koncept evaluace daných systémů včetně jednoduchého technického pracovního listu v češtině (Martínek, 2024a). Celá práce tak může sloužit jako podklad pro přípravu oficiálního státního doporučení pro evaluaci systémů elektronických voleb v České republice obdobně, jako dané doporučení vydala například francouzská Národní komise pro informační technologie a svobody (La Commission nationale de l'informatique et des libertés, 2019).

Autor se snaží české veřejnosti informace o evaluaci elektronických systémů pro vzdálené hlasování zpřístupnit na tématickém webu [Odvolit.cz](https://odvolit.cz) (ISSN 2788-2799) v češtině. V samotném doporučení Rady Evropy jsou žádány členské státy o zpřístupnění daných informací v národním jazyce. Autorem předložené neoficiální překlady dokumentů i další dostupné přeložené zdroje s technickými pracovními listy pro provedení metodického hodnocení elektronických systémů pro hlasování přes Internet (Martínek, 2024a) tak mohou naplnit apel Rady Evropy na členy, který Česká republika jinak aktuálně neplní.

Jako součást práce vznikl kromě evaluační metodiky také v Příloze I metodický postup (Martínek, 2024e), jak by mohl být poměrně bezpečný systém pro tajné internetové hlasování implementován do voleb různých institucí veřejného i soukromého sektoru s nízkými vstupními náklady. V rámci diskuze je obsáhle zodpovězena i otázka ohledně možností případné implementace v rámci politicky závazných národních voleb.

6.3 Omezení výzkumu

Zpracovaná práce má určitá omezení, která v neúplném výčtu může představovat následující seznam:

- Množství publikací - i když je provedena důkladná analýza vědeckých databází Web of Science, Scopus a dalších, může dojít k opomenutí některých souvisejících publikací, které mohou být publikovány například v jazycích mimo kompetence autora. Stejně tak může dojít při překladu k nesprávnému pochopení podstaty citované informace.
- Neochota spolupráce aktérů, kterými mohou být vývojáři, dodavatelé, uživatelé, či provozovatelé systémů pro internetové hlasování, kteří v tuto chvíli nemají povinnost zveřejňovat veškerá data, ani povinnost spolupracovat s výzkumníky při evaluaci systémů.
- Nábor respondentů - v dotazníkových šetřeních není řešena reprezentativnost vůči populaci. V případě šetření v politické straně je to z důvodu nízkého počtu členů strany, u šetření potenciálních uživatelů internetového hlasování jsou využity omezené výzkumné prostředky, kdy

většina respondentů jsou studenty a absolventy jedné konkrétní univerzity, kteří s ohledem na vysokou míru využití internetového hlasování na českých vysokých školách (Příloha K) jsou pravděpodobnými uživateli systémů pro internetové hlasování v blízké budoucnosti. .

- Geografické omezení, kdy se práce logicky soustředí primárně na Českou republiku, sekundárně na Evropskou unii a až následně na zbytek světa.
- Technologický pokrok - rozvoj kvantových počítačů a generativní umělé inteligence může v blízké budoucnosti ohrozit kryptografickou bezpečnost a jiné parametry nejen internetových hlasovacích systémů. Proto je nutné při interpretaci výsledků hledět na možný technologický pokrok.
- Deklarace výsledků hodnocení prostřednictvím metodiky CoMEvIS - vyhodnocení pomocí metodiky CoMEvIS nelze chápat za plně dostačující evaluaci systému internetového hlasování. K takovému hodnocení by byla potřebná odborná nezávislá certifikace na základě předem stanovených podmínek.

7 Seznam použitých zdrojů

- ACCESSIBILITY CHECKER, 2024. Find out if your website is Accessible and Compliant. Accessibility Checker [online]. [cit. 2024-09-16]. Dostupné z: <https://www.accessibilitychecker.org/>
- ACEMYAN, Claudia Z, Philip KORTUM, Michael D BYRNE a Dan S WALLACH, 2014. Usability of Voter Verifiable, End-to-end Voting Systems: Baseline Data for Helios,{Prêt}{à} Voter, and Scantegrity {II}: Baseline Data for Helios,{Prêt}{à} Voter, and Scantegrity {II}. In: 2014 Electronic voting technology workshop/workshop on trustworthy elections (EVT/WOTE 14) [online]. [cit. 2024-09-26]. Dostupné z: <https://www.usenix.org/conference/evtvote14/workshop-program/presentation/acemyan>
- ACHENBACH, Dirk, Carmen KEMPKA, Bernhard LÖWE a Jörn MÜLLER-QUADE, 2015. Improved coercion-resistant electronic elections through deniable re-voting. {USENIX} Journal of Election Technology and Systems ({JETS}) [online]. 3, 26-45 [cit. 2024-09-26]. ISSN 2328-2797. Dostupné z: https://www.usenix.org/system/files/conference/jets15/jets_0302-achenbach.pdf
- ADRIAN, David, Karthikeyan BHARGAVAN, Zakir DURUMERIC, et al., 2015. Imperfect Forward Secrecy. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security [online]. New York, NY, USA: ACM, 2015-10-12, s. 5-17 [cit. 2023-12-19]. ISBN 9781450338325. Dostupné z: doi:10.1145/2810103.2813707
- AGBESI, Samuel, Jurlind BUDURUSHI, Asmita DALELA a Oksana KULYK, 2023. Investigating Transparency Dimensions for Internet Voting. Electronic Voting [online]. Cham: Springer Nature Switzerland, 2023-09-22, 1-17 [cit. 2024-01-10]. Lecture Notes in Computer Science. ISBN 978-3-031-43755-7. Dostupné z: doi:10.1007/978-3-031-43756-4_1
- ALAMLEH, Hosam a Ali Abdullah S. ALQAHTANI, 2021. Analysis of the Design Requirements for Remote Internet-Based E-Voting Systems. In: 2021 IEEE World AI IoT Congress (AIoT) [online]. IEEE, 2021-5-10, s. 0386-0390 [cit. 2024-06-29]. ISBN 978-1-6654-3568-0. Dostupné z: doi:10.1109/AIoT52608.2021.9454194
- ANDER, Veronika, 2022. Interakční design v prostředí ambientní inteligence. Praha. Disertační práce. Česká zemědělská univerzita.
- ARAPINIS, Myrto, Véronique CORTIER, Steve KREMER a Mark RYAN, 2013. Practical Everlasting Privacy. In: BASIN, David a John C. MITCHELL, ed. Principles of Security and Trust [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 21-40 [cit. 2023-12-29]. Lecture Notes in Computer Science. ISBN 978-3-642-36829-5. Dostupné z: doi:10.1007/978-3-642-36830-1_2
- AUSTRALIAN ELECTORAL COMMISSION, 2023. Telephone voting [online]. [cit. 2023-11-14]. Dostupné z: <https://www.aec.gov.au/referendums/vote/blv-voters.html>
- BAVDEKAR, Ritik, Eashan Jayant CHOPDE, Ashutosh BHATIA, Kamlesh TIWARI, Sandeep Joshua DANIEL a ATUL, 2022. Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research. In: Arxiv.org [online]. [cit. 2024-06-03]. Dostupné z: doi:10.48550/arXiv.2202.02826
- BELENIOS TEAM, 2023. Who does what during a Belenios election? Belenios [online]. [cit. 2023-04-06]. Dostupné z: <https://www.belenios.org/instructions.html>
- BELLARE, Mihir a Phillip ROGAWAY, 1993. Random oracles are practical. In: Proceedings of the 1st ACM conference on Computer and communications security - CCS '93 [online]. New York, New York, USA: ACM Press, s. 62-73 [cit. 2023-12-20]. ISBN 0897916298. Dostupné z: doi:10.1145/168588.168596
- BELLOVIN, Rebecca, 2014. Cryptography: Authentication, Blind Signatures, and Digital Cash [online]. [cit. 2023-12-12]. Dostupné z: <https://rmbellovin.github.io/writings/chaum.pdf>
- BENALOH, Josh, 2013. Rethinking voter coercion: The realities imposed by technology: The realities imposed by technology. In: 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13) [online]. [cit. 2024-09-26]. Dostupné z: <https://www.usenix.org/conference/evtvote13/workshop-program/presentation/benaloh>
- BENALOH, Josh Daniel Cohen, 1987. Verifiable secret-ballot elections. Yale University. ISBN 9798207129891.
- BENALOH, Josh, Ronald RIVEST, Peter YA RYAN, Philip STARK, Vanessa TEAGUE a Poorvi VORA, 2015. End-to-end verifiability. ArXiv preprint arXiv:1504.03778 [online]. [cit. 2024-09-26]. Dostupné z: doi:10.48550/arXiv.1504.03778
- BENALOH, Josh a Dwight TUINSTRA, 1994. Receipt-free secret-ballot elections. In: Proceedings of the twenty-sixth annual ACM symposium on Theory of computing. s. 544-553.
- BERNHARD, David, Stephan NEUMANN a Melanie VOLKAMER, 2013. Towards a Practical Cryptographic Voting Scheme Based on Malleable Proofs. In: E-Voting and Identify [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 176-192 [cit. 2023-10-13]. Lecture Notes in Computer Science. ISBN 978-3-642-39184-2. Dostupné z: doi:10.1007/978-3-642-39185-9_11

- BERNHARD, Matthew, Josh BENALOH, J. ALEX HALDERMAN, et al., 2017. Public Evidence from Secret Ballots. In: Electronic Voting [online]. Cham: Springer International Publishing, 2017-10-06, s. 84-109 [cit. 2024-06-20]. Lecture Notes in Computer Science. ISBN 978-3-319-68686-8. Dostupné z: doi:10.1007/978-3-319-68687-5_6
- BETHLEHEM, Jelke, 2009. Applied Survey Methods [online]. Wiley [cit. 2024-10-16]. ISBN 9780470373088. Dostupné z: doi:10.1002/9780470494998
- BEURDOUCHE, Benjamin, Karthikeyan BHARGAVAN, Antoine DELIGNAT-LAVAUD, Cédric FOURNET, Markulf KOHLWEISS, Alfredo PIRONTI, Pierre-Yves STRUB a Jean Karim ZINZINDOHOUE, 2017. A messy state of the union. Communications of the ACM [online]. 2017-01-23, 60(2), 99-107 [cit. 2023-12-27]. ISSN 0001-0782. Dostupné z: doi:10.1145/3023357
- BIERNACKI, Patrick a Dan WALDORF, 1981. Snowball Sampling: Problems and Techniques of Chain Referral Sampling. Sociological Methods & Research [online]. 10(2), 141-163 [cit. 2024-09-09]. ISSN 0049-1241. Dostupné z: doi:10.1177/004912418101000205
- BIRCH, Sarah, 2009. Full Participation: A Comparative Study of Compulsory Voting [online]. United Nations University Press [cit. 2024-06-14]. ISBN 978-92-808-1165-0. Dostupné z: https://archive.unu.edu/unupress/sample-chapters/full_participation_web.pdf
- BJØRSTAD, Tor E., 2013. Source code audit of Norwegian electronic voting system. Ministry of Local Government and Regional Development [online]. [cit. 2024-01-06]. Dostupné z: https://www.regjeringen.no/globalassets/upload/krd/prosjekter/e-valg/kildekode/evalg_rapport_kildeko_degjennomgang.pdf
- BLAKLEY, George Robert, 1979. Safeguarding cryptographic keys. In: Managing Requirements Knowledge, International Workshop on. IEEE Computer Society, s. 313-313.
- BLANCHARD, Enka, Antoine GALLAIS, Emmanuel LEBLOND, Djohar SIDHOUM-RAHAL a Juliette WALTER, 2022. An Analysis of the Security and Privacy Issues of the Neovote Online Voting System. In: KRIMMER, Robert, Melanie VOLKAMER, David DUENAS-CID, Peter RØNNE a Micha GERMANN, ed. Electronic Voting [online]. 13553. Cham: Springer International Publishing, 2022-09-03, s. 1-18 [cit. 2023-03-14]. Lecture Notes in Computer Science. ISBN 978-3-031-15910-7. Dostupné z: doi:10.1007/978-3-031-15911-4_1
- BLANCHET, Bruno, Vincent CHEVAL a Véronique CORTIER, 2022. ProVerif with Lemmas, Induction, Fast Subsumption, and Much More. In: 2022 IEEE Symposium on Security and Privacy (SP) [online]. IEEE, s. 69-86 [cit. 2024-10-04]. ISBN 978-1-6654-1316-9. Dostupné z: doi:10.1109/SP46214.2022.9833653
- BLUM, Manuel, Paul FELDMAN a Silvio MICALI, 2019. Non-interactive zero-knowledge and its applications. In: Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali [online]. Association for Computing Machinery, 2019-10-09 [cit. 2024-06-19]. ISBN 9781450372664. Dostupné z: doi:10.1145/3335741.3335757
- BOWLER, Shaun, Todd DONOVAN a Jeffrey A. KARP, 2007. Enraged or Engaged? Preferences for Direct Citizen Participation in Affluent Democracies. In: Political Research Quarterly [online]. s. 351-362 [cit. 2024-06-14]. ISSN 1065-9129. Dostupné z: doi:10.1177/1065912907304108
- BRAMS, Steven J. a Peter C. FISHBURN, 2007. Approval Voting [online]. Springer New York, NY [cit. 2024-06-14]. ISBN 978-0-387-49896-6. Dostupné z: doi:10.1007/978-0-387-49896-6
- BRÄUNLICH, K., R. GRIMM a P. RICHTER, 2013. Sichere Internetwahlen Ein rechtswissenschaftlich-informatisches Modell. In: Nomos.
- BRUNCLÍK, Miloš a Miroslav NOVÁK, 2014. Internetové volby: budoucnost, nebo slepá ulička demokracie? Praha: Sociologické nakladatelství (SLON). Studijní texty. ISBN 978-80-7419-168-8.
- BRUNET, James a Aleksander ESSEX, 2023. Online Voting in Ontario Municipalities: A Standards-Based Review. In: E-Vote-ID 2023: Electronic Voting [online]. Vol 14230. Springer, Cham, s. 52-68 [cit. 2023-10-12]. ISBN 978-3-031-43756-4. Dostupné z: doi:10.1007/978-3-031-43756-4_4
- BRUNET, James, Athanasios Demetri PANANOS a Aleksander ESSEX, 2022. Review Your Choices: When Confirmation Pages Break Ballot Secrecy in Online Elections. In: KRIMMER, Robert, Melanie VOLKAMER, David DUENAS-CID, Peter RØNNE a Micha GERMANN, ed. Electronic Voting [online]. 13553. Cham: Springer International Publishing, s. 36-52 [cit. 2023-03-14]. Lecture Notes in Computer Science. ISBN 978-3-031-15910-7. Dostupné z: doi:10.1007/978-3-031-15911-4_3
- BRYMAN, Alan, 2016. Social research methods. Oxford university press. ISBN 0199689458.
- BUCKLAND, Richard, Vanessa TEAGUE a Roland WEN, 2012. Towards Best Practice for E-election Systems. In: E-Voting and Identity [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 224-241 [cit. 2024-05-08]. Lecture Notes in Computer Science. ISBN 978-3-642-32746-9. Dostupné z: doi:10.1007/978-3-642-32747-6_14
- BUDD, Brian, Chelsea GABEL a Nicole GOODMAN, 2019. Online Voting in a First Nation in Canada: Implications for Participation and Governance. In: KRIMMER, Robert, Melanie VOLKAMER, Veronique CORTIER, Bernhard

- BECKERT, Ralf KÜSTERS, Uwe SERDÜLT a David DUENAS-CID, ed. Electronic Voting [online]. Cham: Springer International Publishing, s. 50-66 [cit. 2023-02-17]. Lecture Notes in Computer Science. ISBN 978-3-030-30624-3. Dostupné z: doi:10.1007/978-3-030-30625-0_4
- BURTON, C, C CULNANE a S SCHNEIDER, 2015. Secure and Verifiable Electronic Voting in Practice: the use of vVote in the Victorian State Election. In: University of Surrey [online]. [cit. 2023-10-12]. Dostupné z: <https://openresearch.surrey.ac.uk/esploro/outputs/99512892902346>
- CARDILLO, Anthony, Nicholas AKINYOKUN a Aleksander ESSEX, 2019. Online Voting in Ontario Municipal Elections: A Conflict of Legal Principles and Technology? In: KRIMMER, Robert, Melanie VOLKAMER, Veronique CORTIER, Bernhard BECKERT, Ralf KÜSTERS, Uwe SERDÜLT a David DUENAS-CID, ed. Electronic Voting [online]. Cham: Springer International Publishing, s. 67-82 [cit. 2023-02-17]. Lecture Notes in Computer Science. ISBN 978-3-030-30624-3. Dostupné z: doi:10.1007/978-3-030-30625-0_5
- CARDILLO, Anthony a Aleksander ESSEX, 2018. The Threat of SSL/TLS Stripping to Online Voting. In: KRIMMER, Robert, Melanie VOLKAMER, Veronique CORTIER, Rajeev GORÉ, Manik HAPSARA, Uwe SERDÜLT a David DUENAS-CID, ed. Electronic Voting [online]. Cham: Springer International Publishing, s. 35-50 [cit. 2023-02-17]. Lecture Notes in Computer Science. ISBN 978-3-030-00418-7. Dostupné z: doi:10.1007/978-3-030-00419-4_3
- CASTELLÓ, Sandra Guasch, 2016. Individual Verifiability in Electronic Voting. In: Universitat Politècnica de Catalunya [online]. [cit. 2023-10-12]. Dostupné z: <https://upcommons.upc.edu/bitstream/handle/2117/96245/TSGC1de1.pdf>
- ČESKÁ REPUBLIKA, 1995. Zákon č. 247/1995 Sb.: Zákon o volbách do Parlamentu České republiky a o změně a doplnění některých dalších zákonů [online]. Česká republika: Sbírka zákonů [cit. 2024-09-26]. Dostupné z: <https://www.e-sbirka.cz/sb/1995/247/2021-07-01>
- ČESKÁ REPUBLIKA, 2012. Zákon č. 90/2012 Sb.: Zákon o obchodních společnostech a družstvech (zákon o obchodních korporacích). Sbírka zákonů [online]. [cit. 2024-04-25]. Dostupné z: <https://www.e-sbirka.cz/sb/2012/90/2023-07-01>
- ČESKÁ REPUBLIKA, 2014. Zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). E-Sbírka [online]. [cit. 2024-09-18]. Dostupné z: <https://www.e-sbirka.cz/sb/2014/181/2022-08-06>
- ČESKÁ REPUBLIKA, 2019a. Zákon č. 110/2019 Sb.: Zákon o zpracování osobních údajů. E-Sbírka [online]. [cit. 2024-07-03]. Dostupné z: <https://www.e-sbirka.cz/sb/2019/110/2019-04-24?zalozka=souvisslosti>
- ČESKÁ REPUBLIKA, 2019b. Zákon č. 99/2019 Sb.: Zákon o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů. Sbírka zákonů [online]. [cit. 2024-09-26]. Dostupné z: <https://www.e-sbirka.cz/sb/2019/99/2023-04-01>
- ČESKÁ REPUBLIKA, 2023. Zákon č. 250/2017 Sb.: Zákon o elektronické identifikaci [online]. [cit. 2024-09-12]. Dostupné z: <https://www.e-sbirka.cz/sb/2017/250/2023-04-01>
- ČESKÁ REPUBLIKA, 2024a. Zákon č. 424/1991 Sb.: Zákon o sdružování v politických stranách a v politických hnutích. Sbírka zákonů [online]. [cit. 2024-03-26]. Dostupné z: <https://www.e-sbirka.cz/sb/1991/424?zalozka=text>
- ČESKÁ REPUBLIKA, 2024b. Zákon č. 111/1998 Sb.: Zákon o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách). Sbírka zákonů [online]. [cit. 2024-04-21]. Dostupné z: <https://www.e-sbirka.cz/sb/1998/111?zalozka=text>
- CETINKAYA, Orhan, 2008. Analysis of Security Requirements for Cryptographic Voting Protocols (Extended Abstract). In: 2008 Third International Conference on Availability, Reliability and Security [online]. IEEE, s. 1451-1456 [cit. 2024-06-23]. ISBN 978-0-7695-3102-1. Dostupné z: doi:10.1109/ARES.2008.167
- CHANG-FONG, Nicholas a Aleksander ESSEX, 2016. The cloudier side of cryptographic end-to-end verifiable voting. In: Proceedings of the 32nd Annual Conference on Computer Security Applications [online]. New York, NY, USA: ACM, 2016-12-05, s. 324-335 [cit. 2024-06-28]. ISBN 9781450347716. Dostupné z: doi:10.1145/2991079.2991106
- CHAUM, David, 1983. Blind Signatures for Untraceable Payments. In: CHAUM, David, Ronald L. RIVEST a Alan T. SHERMAN, ed. Advances in Cryptology [online]. Boston, MA: Springer US, s. 199-203 [cit. 2023-12-12]. ISBN 978-1-4757-0604-8. Dostupné z: doi:10.1007/978-1-4757-0602-4_18
- CHAUM, David, 2004. Secret-ballot receipts: true voter-verifiable elections. IEEE Security & Privacy Magazine [online]. 2(1), 38-47 [cit. 2023-12-22]. ISSN 1540-7993. Dostupné z: doi:10.1109/MSECP.2004.1264852
- CHAUM, David L., 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM [online]. 24(2), 84-90 [cit. 2023-11-29]. ISSN 0001-0782. Dostupné z: doi:10.1145/358549.358563

- CHAUM, David, Peter Y. A. RYAN a Steve SCHNEIDER, 2005. A Practical Voter-Verifiable Election Scheme. In: DI VIMERCATI, Sabrina de Capitani, Paul SYVERSON a Dieter GOLLMANN, ed. Computer Security – ESORICS 2005 [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 118-139 [cit. 2023-12-31]. Lecture Notes in Computer Science. ISBN 978-3-540-28963-0. Dostupné z: doi:10.1007/11555827_8
- CHEESEMAN, Nic, Gabrielle LYNCH a Justin WILLIS, 2018. Digital dilemmas: the unintended consequences of election technology. Democratization [online]. 2018-11-17, 25(8), 1397-1418 [cit. 2024-08-12]. ISSN 1351-0347. Dostupné z: doi:10.1080/13510347.2018.1470165
- CHILLOTTI, Ilaria, Nicolas GAMA, Mariya GEORGIEVA a Malika IZABACHÈNE, 2016. A Homomorphic LWE Based E-voting Scheme. In: TAKAGI, Tsuyoshi, ed. Post-Quantum Cryptography [online]. Cham: Springer International Publishing, s. 245-265 [cit. 2024-06-26]. Lecture Notes in Computer Science. ISBN 978-3-319-29359-2. Dostupné z: doi:10.1007/978-3-319-29360-8_16
- CLARKSON, Michael R, Stephen CHONG a Andrew C. MYERS, 2008. Civitas: Toward a Secure Voting System. In: 2008 IEEE Symposium on Security and Privacy (sp 2008) [online]. IEEE, s. 354-368 [cit. 2024-07-02]. ISBN 978-0-7695-3168-7. ISSN 1081-6011. Dostupné z: doi:10.1109/SP.2008.32
- CLOUDFLARE, 2009. Cloudflare - The Web Performance and Security Company [online]. [cit. 2023-10-24]. Dostupné z: <https://www.cloudflare.com/>
- COHEN, Josh D a Michael J FISCHER, 1985. A robust and verifiable cryptographically secure election scheme. Yale University. Department of Computer Science.
- CORBIN, Juliet a Anselm STRAUSS, 2015. Basics of qualitative research. 14. sage. ISBN 1412997461.
- CORON, Jean-Sébastien, Yevgeniy DODIS, Cécile MALINAUD a Prashant PUNIYA, 2005. Merkle-Damgård Revisited: How to Construct a Hash Function. In: SHOUP, Victor, ed. Advances in Cryptology – CRYPTO 2005 [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 430-448 [cit. 2023-12-20]. Lecture Notes in Computer Science. ISBN 978-3-540-28114-6. Dostupné z: doi:10.1007/11535218_26
- CORTIER, Véronique, 2015. Formal verification of e-voting: solutions and challenges. In: ACM SIGLOG News [online]. Vol. 2, No. 1. 2015-01-28, s. 25-34 [cit. 2023-10-12]. ISSN 2372-3491. Dostupné z: doi:10.1145/2728816.2728823
- CORTIER, Véronique, Pierrick GAUDRY a Stéphane GLONDU, 2020. Analyse de sécurité de la plateforme de vote Belenios Conformité avec les recommandations 2019 de la CNIL [online]. [cit. 2023-12-29]. Dostupné také z: <https://www.belenios.org/analyse-secu.pdf>
- CORTIER, Véronique a Cyrille WIEDLING, 2012. A Formal Analysis of the Norwegian E-voting Protocol. In: DEGANI, Pierpaolo a Joshua D. GUTTMAN, ed. Principles of Security and Trust [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 109-128 [cit. 2024-06-29]. Lecture Notes in Computer Science. ISBN 978-3-642-28640-7. Dostupné z: doi:10.1007/978-3-642-28641-4_7
- COUNCIL OF EUROPE, 2011. Certification of e-voting systems. DIRECTORATE GENERAL OF DEMOCRACY AND POLITICAL AFFAIRS [online]. [cit. 2023-12-29]. Dostupné z: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168059bdf8>
- COUNCIL OF EUROPE, 2004. Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. Bruselas: Council of Europe, Committee of Ministers, [online]. [cit. 2023-11-14]. Dostupné z: [https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/00Rec\(2004\)11_rec_adopted_en.asp](https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/00Rec(2004)11_rec_adopted_en.asp)
- COUNCIL OF EUROPE, 2022. Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States Introduction [online]. [cit. 2024-05-07]. Dostupné z: https://search.coe.int/cm/pages/result_details.aspx?objectId=0900001680a575d9
- COUNCIL OF EUROPE, 2017. Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting: (Adopted by the Committee of Ministers on 14 June 2017 at the 1289th meeting of the Ministers' Deputies) [online]. MINISTERS' DEPUTIES Recommendations: Council of Europe [cit. 2024-09-26]. Dostupné z: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f
- COX, Gary W, 1997. Making votes count: strategic coordination in the world's electoral systems: strategic coordination in the world's electoral systems. Cambridge University Press. ISBN 0521585279.
- CRAMER, Ronald, Rosario GENNARO a Berry SCHOENMAKERS, 1997. A secure and optimally efficient multi-authority election scheme. European Transactions on Telecommunications [online]. 8(5), 481-490 [cit. 2024-06-26]. ISSN 1124-318X. Dostupné z: doi:10.1002/ett.4460080506
- CUCURULL, Jordi, Adrià RODRÍGUEZ-PÉREZ, Tamara FINOGINA a Jordi PUIGGALÍ, 2019. Blockchain-Based Internet Voting: Systems' Compliance with International Standards. In: ABRAMOWICZ, Witold a Adrian PASCHKE, ed.

- Business Information Systems Workshops [online]. Cham: Springer International Publishing, s. 300-312 [cit. 2024-08-18]. Lecture Notes in Business Information Processing. ISBN 978-3-030-04848-8. Dostupné z: doi:10.1007/978-3-030-04849-5_27
- CULNANE, Chris, Mark ELDRIDGE, Aleksander ESSEX a Vanessa TEAGUE, 2017. Trust Implications of DDoS Protection in Online Elections. In: KRIMMER, Robert, Melanie VOLKAMER, Nadja BRAUN BINDER, Norbert KERSTING, Olivier PEREIRA a Carsten SCHÜRMANN, ed. Electronic Voting [online]. Cham: Springer International Publishing, s. 127-145 [cit. 2023-02-17]. Lecture Notes in Computer Science. ISBN 978-3-319-68686-8. Dostupné z: doi:10.1007/978-3-319-68687-5_8
- CULNANE, Chris, Aleksander ESSEX, Sarah Jamie LEWIS, Olivier PEREIRA a Vanessa TEAGUE, 2019. Knights and Knaves Run Elections: Internet Voting and Undetectable Electoral Fraud. IEEE Security & Privacy [online]. 17(4), 62-70 [cit. 2024-07-02]. ISSN 1540-7993. Dostupné z: doi:10.1109/MSEC.2019.2915398
- DAMGÅRD, Ivan, Nelly FAZIO a Antonio NICOLASI, 2006. Non-interactive Zero-Knowledge from Homomorphic Encryption. In: HALEVI, Shai a Tal RABIN, ed. Theory of Cryptography [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 41-59 [cit. 2024-06-19]. Lecture Notes in Computer Science. ISBN 978-3-540-32731-8. Dostupné z: doi:10.1007/11681878_3
- DANDROY, Régis a Tudi KERNALEGENN, 2021. Internet voting from abroad: exploring turnout in the 2014 French consular elections. French Politics [online]. 19(4), 421-439 [cit. 2024-06-28]. ISSN 1476-3419. Dostupné z: doi:10.1057/s41253-021-00148-8
- DELAUNE, Stéphanie, Steve KREMER a Mark RYAN, 2009. Verifying privacy-type properties of electronic voting protocols. In: Journal of Computer Security [online]. 2009-07-02, s. 435-487 [cit. 2024-06-23]. ISSN 18758924. Dostupné z: doi:10.3233/JCS-2009-0340
- DESERIIS, Marco, 2017. Direct Parliamentarianism: An Analysis of the Political Values Embedded in Rousseau, the 'Operating System' of the Five Star Movement. In: JeDEM - eJournal of eDemocracy and Open Government [online]. 2017-12-18, s. 47-67 [cit. 2024-06-12]. ISSN 2075-9517. Dostupné z: doi:10.29379/jedem.v9i2.471
- DESERIIS, Marco, 2021. Rethinking the digital democratic affordance and its impact on political representation: Toward a new framework. New Media & Society [online]. 23(8), 2452-2473 [cit. 2024-06-26]. ISSN 1461-4448. Dostupné z: doi:10.1177/1461444820929678
- DESERIIS, Marco, 2023. Reducing the Burden of Decision in Digital Democracy Applications: A Comparative Analysis of Six Decision-making Software. Science, Technology, & Human Values [online]. 48(2), 401-427 [cit. 2024-06-26]. ISSN 0162-2439. Dostupné z: doi:10.1177/01622439211054081
- DESERIIS, Marco a Davide VITTORI, 2019. The Impact of Online Participation Platforms on the Internal Democracy of Two Southern European Parties: Podemos and the Five Star Movement [online]. 13(1), 5695-5714 [cit. 2024-03-19]. Dostupné z: doi:1932-8036/20190005
- DESMEDT, Yvo a Kaoru KUROSAWA, 2000. How to Break a Practical MIX and Design a New One. In: PRENEEL, Bart, ed. Advances in Cryptology — EUROCRYPT 2000 [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 557-572 [cit. 2023-12-12]. Lecture Notes in Computer Science. ISBN 978-3-540-67517-4. Dostupné z: doi:10.1007/3-540-45539-6_39
- DIA, 2024. Digitální a informační agentura [online]. [cit. 2024-09-12]. Dostupné z: <https://www.dia.gov.cz/>
- DIE SCHWEIZERISCHE POST, 2024. E-Voting-Community-Programm der Schweizerischen Post. Evoting-Community [online]. [cit. 2024-01-07]. Dostupné z: <https://evoting-community.post.ch/de/>
- DIFFIE, W. a M. HELLMAN, 1976. New directions in cryptography. In: IEEE Transactions on Information Theory [online]. s. 644-654 [cit. 2023-12-19]. ISSN 0018-9448. Dostupné z: doi:10.1109/TIT.1976.1055638
- DILLMAN, Don A, 2011. Mail and Internet surveys: The tailored design method--2007 Update with new Internet, visual, and mixed-mode guide: The tailored design method--2007 Update with new Internet, visual, and mixed-mode guide. John Wiley. ISBN 1118044630.
- DOLEV, Danny, Cynthia DWORK a Moni NAOR, 1991. Non-malleable cryptography. In: Proceedings of the twenty-third annual ACM symposium on Theory of computing - STOC '91 [online]. New York, New York, USA: ACM Press, s. 542-552 [cit. 2023-12-12]. ISBN 0897913973. Dostupné z: doi:10.1145/103418.103474
- DRIZA MAURER, Ardita, 2019. The Swiss Post/Scytl Transparency Exercise and Its Possible Impact on Internet Voting Regulation. Electronic Voting [online]. Cham: Springer International Publishing, 2019-09-24, 83-99 [cit. 2024-05-08]. Lecture Notes in Computer Science. ISBN 978-3-030-30624-3. Dostupné z: doi:10.1007/978-3-030-30625-0_6
- DRIZA MAURER, Ardita, 2017. Updated European Standards for E-voting. In: KRIMMER, Robert, Melanie VOLKAMER, Nadja BRAUN BINDER, Norbert KERSTING, Olivier PEREIRA a Carsten SCHÜRMANN, ed. Electronic Voting [online]. Cham: Springer International Publishing, s. 146-162 [cit. 2024-06-28]. Lecture Notes in Computer Science. ISBN 978-3-319-68686-8. Dostupné z: doi:10.1007/978-3-319-68687-5_9

- DRIZA MAURER, Ardita, Melanie VOLKAMER a Robert KRIMMER, 2023. Council of Europe Guidelines on the Use of ICT in Electoral Processes. In: KATSIKAS, Sokratis, Frédéric CUPPENS, Christos KALLONIATIS, et al., ed. Computer Security. ESORICS 2022 International Workshops. ESORICS 2022. Lecture Notes in Computer Science [online]. 13785. Cham: Springer International Publishing, s. 585-599 [cit. 2023-03-16]. Lecture Notes in Computer Science. ISBN 978-3-031-25459-8. Dostupné z: doi:10.1007/978-3-031-25460-4_34
- DWORKIN, Morris J., 2015. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. Federal Inf. Process. Stds. (NIST FIPS) - 202 [online]. NIST Pubs [cit. 2024-06-18]. Dostupné z: doi:10.6028/NIST.FIPS.202
- EAC, 2024. Voluntary Voting System Guidelines. U.S. Election Assistance Commission [online]. [cit. 2024-01-22]. Dostupné z: <https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines>
- EAC, 2023. Studies and Reports. U.S. Election Assistance Commission [online]. [cit. 2024-01-06]. Dostupné z: <https://www.eac.gov/research-and-data/studies-and-reports>
- ELGAMAL, Taher, 1985. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In: BLAKLEY, George Robert a David CHAUM, ed. Advances in Cryptology [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985-11-24, s. 10-18 [cit. 2023-11-23]. Lecture Notes in Computer Science. ISBN 978-3-540-15658-1. Dostupné z: doi:10.1007/3-540-39568-7_2
- ENISA, 2023. Volby do EU jsou ohroženy nárůstem manipulace s informacemi pomocí umělé inteligence. Agentura Evropské unie pro kybernetickou bezpečnost [online]. [cit. 2024-07-01]. Dostupné z: <https://www.enisa.europa.eu/news/eu-elections-at-risk-with-rise-of-ai-enabled-information-manipulation>
- ENISA, 2024. Compendium on Elections Cybersecurity and Resilience. Agentura Evropské unie pro kybernetickou bezpečnost [online]. [cit. 2024-07-01]. Dostupné z: <https://ec.europa.eu/newsroom/dae/redirection/document/103148>
- ENISA, 2019. Election Cybersecurity: Challenges and Opportunities. European Union Agency for Network and Information Security (ENISA) [online]. [cit. 2024-07-01]. Dostupné z: <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/election-cybersecurity-challenges-and-opportunities>
- EPIFANOVA, Alina, 2021. Online Elections in Russia. DGAP [online]. [cit. 2024-09-15]. Dostupné z: <https://dgap.org/en/research/publications/online-elections-russia>
- ERICSSON, K. Anders, Neil CHARNESS, Paul J. FELTOVICH a Robert R. HOFFMAN, ed., 2012. The Cambridge Handbook of Expertise and Expert Performance [online]. Cambridge University Press [cit. 2024-09-09]. ISBN 9780521840972. Dostupné z: doi:10.1017/CBO9780511816796
- ESGIN, Muhammed F, Raymond K. ZHAO, Ron STEINFELD, Joseph K. LIU a Dongxi LIU, 2019. MatRiCT: Efficient, Scalable and Post-Quantum Blockchain Confidential Transactions Protocol. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security [online]. New York, NY, USA: ACM, 2019-11-06, s. 567-584 [cit. 2024-06-26]. ISBN 9781450367479. Dostupné z: doi:10.1145/3319535.3354200
- ESSEX, Aleksander a Nicole GOODMAN, 2020. Protecting Electoral Integrity in the Digital Age: Developing E-Voting Regulations in Canada. Election Law Journal: Rules, Politics, and Policy [online]. 2020-06-01, 19(2), 162-179 [cit. 2024-06-28]. ISSN 1533-1296. Dostupné z: doi:10.1089/elj.2019.0568
- EU, 2016. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Text s významem pro EHP). EUR-Lex [online]. [cit. 2024-04-22]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex%3A32016R0679>
- EU, 2022. Směrnice Evropského parlamentu a Rady (EU) 2022/2555: o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2). Úřední věstník Evropské unie [online]. [cit. 2024-09-18]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022L2555&from=CS>
- EU, 2023. Compendium of e-voting and other ICT practices. In: Justice and Consumers [online]. [cit. 2024-10-05]. ISBN 978-92-68-09554-6. Dostupné z: doi:10.2838/464803
- E-VOTING INFORMATIONSPLATTFORM DER KANTONE, 2023. E-Voting in der Schweiz: Wissenswertes rund um die elektronische Stimmabgabe. E-Voting [online]. [cit. 2024-02-21]. Dostupné z: <https://www.evoting-info.ch/>
- FAIL2BAN, 2013. Daemon to ban hosts that cause multiple authentication errors [online]. [cit. 2023-10-24]. Dostupné z: <http://www.fail2ban.org/>
- FEC, 2002. Voting System Standards. Federal Election Commission USA [online]. [cit. 2024-01-05]. Dostupné z: https://www.eac.gov/sites/default/files/eac_assets/1/28/Voting_System_Standards_Volume_I.pdf

- FEIGE, Uriel, Dror LAPIDOT a Adi SHAMIR, 1999. Multiple NonInteractive Zero Knowledge Proofs Under General Assumptions. In: SIAM Journal on Computing [online]. s. 1-28 [cit. 2024-06-19]. ISSN 0097-5397. Dostupné z: doi:10.1137/S0097539792230010
- FELSENTHAL, Dan S. a Moshé MACHOVER, 1998. The Measurement of Voting Power. Edward Elgar Publishing. Dostupné také z: <https://EconPapers.repec.org/RePEc:elg:eebook:1489>
- FIAT, Amos a Adi SHAMIR, 2006. How To Prove Yourself: Practical Solutions to Identification and Signature Problems. In: ODLYZKO, Andrew M., ed. Advances in Cryptology — CRYPTO' 86 [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006-12-1, s. 186-194 [cit. 2024-07-02]. Lecture Notes in Computer Science. ISBN 978-3-540-18047-0. Dostupné z: doi:10.1007/3-540-47721-7_12
- FINOGINA, Tamara, Jordi CUCURULL JUAN a Nuria COSTA, 2024. Selective comparison of verifiable online voting systems. SECURITY AND PRIVACY [online]. [cit. 2024-07-27]. ISSN 2475-6725. Dostupné z: doi:10.1002/spy2.394
- FOUARD, Laure, Mathilde DUCLOS a Pascal PASCAL, 2007. Survey on electronic voting schemes. In: ANR project AVOTÉ [online]. [cit. 2024-08-02]. Dostupné z: <https://luca-giuzzi.unibs.it/corsi/Support/papers-cryptography/e-vote.pdf>
- FOWLER JR, Floyd J, 2013. Survey research methods. Sage publications. ISBN 1483312402.
- FRANCE24, 2024. 'Shpilkin method': Statistical tool gauges voter fraud in Putin landslide: Statistický nástroj měří volební podvody v Putinově drtivě. France 24 [online]. [cit. 2024-09-16]. Dostupné z: <https://www.france24.com/en/europe/20240320-shpilkin-method-statistical-analysis-gauges-voter-fraud-in-putin-landslide>
- FREAK ATTACK, 2015. Tracking the FREAK Attack [online]. [cit. 2023-10-12]. Dostupné z: <https://freakattack.com/>
- FREEDOM HOUSE, 2023. Freedom in the World 2023. FreedomHouse.org [online]. [cit. 2024-01-02]. Dostupné z: https://freedomhouse.org/sites/default/files/2023-03/FIW_World_2023_DigitalPDF.pdf
- FUJIOKA, Atsushi, Tatsuaki OKAMOTO a Kazuo OHTA, 1993. A practical secret voting scheme for large scale elections. In: SEBERRY, Jennifer a Yuliang ZHENG, ed. Advances in Cryptology — AUSCRYPT '92 [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 244-251 [cit. 2023-12-12]. Lecture Notes in Computer Science. ISBN 978-3-540-57220-6. Dostupné z: doi:10.1007/3-540-57220-1_66
- FURUKAWA, Jun a Kazue SAKO, 2001. An Efficient Scheme for Proving a Shuffle. In: KILIAN, Joe, ed. Advances in Cryptology — CRYPTO 2001 [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 368-387 [cit. 2023-12-12]. Lecture Notes in Computer Science. ISBN 978-3-540-42456-7. Dostupné z: doi:10.1007/3-540-44647-8_22
- FVAP, 2015. Review of FVAP's Work Related to Remote Electronic Voting for the UOCAVA Population [online]. [cit. 2024-01-06]. Dostupné z: https://www.fvap.gov/uploads/FVAP/Reports/FVAP_EVDP_20151229_final.pdf
- GABEL, Chelsea a Nicole GOODMAN, 2021. Indigenous Experiences with Online Voting. FN Digital Democracy [online]. [cit. 2024-06-28]. Dostupné z: http://www.digitalimpactfn.com/wp-content/uploads/2021/05/FN_DIGITAL_REPORT_DIGITAL_FNL6.pdf
- GALINDO, David, Sandra GUASCH a Jordi PUIGGALÍ, 2015. 2015 Neuchâtel's Cast-as-Intended Verification Mechanism. In: HAENNI, Rolf, Reto E. KOENIG a Douglas WIKSTRÖM, ed. E-Voting and Identity [online]. Cham: Springer International Publishing, s. 3-18 [cit. 2023-12-31]. Lecture Notes in Computer Science. ISBN 978-3-319-22269-1. Dostupné z: doi:10.1007/978-3-319-22270-7_1
- GAO, Shiyao, Dong ZHENG, Rui GUO, Chunming JING a Chencheng HU, 2019. An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function. IEEE Access [online]. 7, 115304-115316 [cit. 2024-06-26]. ISSN 2169-3536. Dostupné z: doi:10.1109/ACCESS.2019.2935895
- GARNETT, Holly Ann a Sean GROGAN, 2021. I Came, I Saw, I Voted: Distance to Polling Locations and Voter Turnout in Ontario, Canada. Canadian Journal of Political Science [online]. 54(2), 316-334 [cit. 2024-06-29]. ISSN 0008-4239. Dostupné z: doi:10.1017/S0008423921000196
- GARNETT, Holly Ann a Toby S. JAMES, 2020. Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity. In: Election Law Journal: Rules, Politics, and Policy [online]. 2020-06-01, s. 111-126 [cit. 2024-06-07]. ISSN 1533-1296. Dostupné z: doi:10.1089/elj.2020.0633
- GAUDRY, Pierrick a Alexander GOLOVNEV, 2020. Breaking the Encryption Scheme of the Moscow Internet Voting System. In: BONNEAU, Joseph a Nadia HENINGER, ed. Financial Cryptography and Data Security [online]. Cham: Springer International Publishing, s. 32-49 [cit. 2024-01-07]. Lecture Notes in Computer Science. ISBN 978-3-030-51279-8. Dostupné z: doi:10.1007/978-3-030-51280-4_3
- GENTRY, Craig, 2009. Fully homomorphic encryption using ideal lattices. In: Proceedings of the forty-first annual ACM symposium on Theory of computing [online]. New York, NY, USA: ACM, 2009-05-31, s. 169-178 [cit. 2024-06-25]. ISBN 9781605585062. Dostupné z: doi:10.1145/1536414.1536440

- GERBAUDO, Paolo, 2021. Are digital parties more democratic than traditional parties? Evaluating Podemos and Movimento 5 Stelle's online decision-making platforms. *Party Politics* [online]. 27(4), 730-742 [cit. 2024-07-02]. ISSN 1354-0688. Dostupné z: doi:10.1177/1354068819884878
- GERMANN, Micha a Uwe SERDÜLT, 2014. Internet Voting for Expatriates: The Swiss Case. *JeDEM - eJournal of eDemocracy and Open Government* [online]. 2014-12-09, 6(2), 197-215 [cit. 2023-12-31]. ISSN 2075-9517. Dostupné z: doi:10.29379/jedem.v6i2.302
- GHONAIMY, M. Adeeb, Mahmoud T. EL-HADIDI a Heba K. ASLAN, 2017. Erratum to: Security in the Information Society. In: GHONAIMY, M. Adeeb, Mahmoud T. EL-HADIDI a Heba K. ASLAN, ed. *Security in the Information Society* [online]. Boston, MA: Springer US, E1-E1 [cit. 2024-06-30]. IFIP Advances in Information and Communication Technology. ISBN 978-1-4757-1026-7. Dostupné z: doi:10.1007/978-0-387-35586-3_46
- GJØSTEEN, Kristian, 2010. Analysis of an internet voting protocol. *CRYPTOLOGY EPRINT ARCHIVE*. Cryptology ePrint Archive [online]. (Paper 2010/380) [cit. 2023-12-31]. Dostupné z: <https://eprint.iacr.org/2010/380>
- GJØSTEEN, Kristian, 2013. The Norwegian Internet Voting Protocol. In: *Cryptology ePrint Archive*, Paper 2013/473 [online]. [cit. 2023-10-12]. Dostupné z: <https://eprint.iacr.org/2013/473>
- GOLDWASSER, Shafi, Silvio MICALI a Ronald L. RIVEST, 1988. A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. *SIAM Journal on Computing* [online]. 17(2), 281-308 [cit. 2024-07-02]. ISSN 0097-5397. Dostupné z: doi:10.1137/0217017
- GOLDWASSER, Shafi, Silvio MICALI a Chales RACKOFF, 2019. The knowledge complexity of interactive proof-systems. In: *Providing sound foundations for cryptography: On the work of shafi goldwasser and silvio micali*. s. 203-225.
- GOLDWASSER, Shafi a Silvio MICALI, 1984. Probabilistic encryption. *Journal of Computer and System Sciences* [online]. 28(2), 270-299 [cit. 2024-06-19]. ISSN 00220000. Dostupné z: doi:10.1016/0022-0000(84)90070-9
- GOODMAN, Leo A., 1961. Snowball Sampling. In: *The Annals of Mathematical Statistics* [online]. Vol. 32, No. 1. Institute of Mathematical Statistics, s. 148-170 [cit. 2023-10-13]. Dostupné z: <https://www.jstor.org/stable/2237615>
- GOODMAN, Nicole a Jon PAMMETT, 2014. The patchwork of internet voting in Canada. In: *2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE)* [online]. IEEE, s. 1-6 [cit. 2024-01-06]. ISBN 978-3-2000-3697-0. Dostupné z: doi:10.1109/EVOTE.2014.7001134
- GOODMAN, Nicole, Iuliia SPYCHER-KRIVONOSOVA, Aleksander ESSEX a James BRUNET, 2023. Verifiability Experiences in Ontario's 2022 Online Elections. *Electronic Voting* [online]. Cham: Springer Nature Switzerland, 2023-09-22, 87-105 [cit. 2024-01-06]. *Lecture Notes in Computer Science*. ISBN 978-3-031-43755-7. Dostupné z: doi:10.1007/978-3-031-43756-4_6
- GRITZALIS, Dimitris A., ed., 2003. *Secure Electronic Voting* [online]. Boston, MA: Springer US [cit. 2024-08-02]. *Advances in Information Security*. ISBN 978-1-4613-4981-5. Dostupné z: doi:10.1007/978-1-4615-0239-5
- GRITZALIS, Dimitris A., 2002. Principles and requirements for a secure e-voting system. *Computers & Security* [online]. 21(6), 539-556 [cit. 2024-06-28]. ISSN 01674048. Dostupné z: doi:10.1016/S0167-4048(02)01014-3
- GRONWALD TOVÁ WAGNEROVÁ, Petra, 2010. Doporučení Rec(2004)11 Výboru ministrů členským státům o právních, operačních a technických standardech elektronického hlasování [online]. [cit. 2024-09-11]. Dostupné z: <http://www.mvcr.cz/soubor/spravni-pravo-78-09web-gronwaldtova-pdf.aspx>
- HABER, Stuart a W. Scott STORNETTA, 1991. How to time-stamp a digital document. *Journal of Cryptology* [online]. 3(2), 99-111 [cit. 2024-07-02]. ISSN 0933-2790. Dostupné z: doi:10.1007/BF00196791
- HAENNI, Rolf, Reto E. KOENIG, Philipp LOCHER a Eric DUBUIS, 2017. CHVote Protocol Specification. *Cryptology ePrint Archive* [online]. (Paper 2017/325) [cit. 2024-01-07]. Dostupné z: <https://eprint.iacr.org/2017/325>
- HAINES, Thomas, Rafieh MOSAHEB, Johannes MÜLLER a Ivan PRYVALOV, 2023. SoK: Secure E-Voting with Everlasting Privacy. In: *Proceedings on Privacy Enhancing Technologies* [online]. s. 279-293 [cit. 2024-06-03]. ISSN 2299-0984. Dostupné z: doi:10.56553/popets-2023-0017
- HAINES, Thomas, Olivier PEREIRA a Vanessa TEAGUE, 2022. Running the Race: A Swiss Voting Story. In: KRIMMER, Robert, Melanie VOLKAMER, David DUENAS-CID, Peter RØNNE a Micha GERMANN, ed. *Electronic Voting* [online]. Cham: Springer International Publishing, s. 53-69 [cit. 2024-01-07]. *Lecture Notes in Computer Science*. ISBN 978-3-031-15910-7. Dostupné z: doi:10.1007/978-3-031-15911-4_4
- HAJIAN BERENJESTANAKI, Mohammad, Hamid R. BARZEGAR, Nabil EL IOINI a Claus PAHL, 2024. Blockchain-Based E-Voting Systems: A Technology Review. *Electronics* [online]. 13(1) [cit. 2024-07-02]. ISSN 2079-9292. Dostupné z: doi:10.3390/electronics13010017

- HALDERMAN, J. Alex a Vanessa TEAGUE, 2015. The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. In: ArXiv.org [online]. [cit. 2023-12-29]. Dostupné z: doi:10.48550/arXiv.1504.05646
- HALEVI, Shai a Hugo KRAWCZYK, 1999. Public-key cryptography and password protocols. *ACM Transactions on Information and System Security* [online]. 2(3), 230-268 [cit. 2023-12-20]. ISSN 1094-9224. Dostupné z: doi:10.1145/322510.322514
- HAMMER, Volker, Ulrich PORDESCH a Alexander ROSSNAGEL, 1993. Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet. In: Springer-Verlag, Berlin [online]. [cit. 2023-10-13]. Dostupné z: https://kobra.uni-kassel.de/handle/123456789/2017062252647
- HASSAN, Nik R a Claudia LOEBBECKE, 2017. Engaging scientometrics in information systems. *Journal of Information Technology* [online]. 32(1), 85-109 [cit. 2024-07-02]. ISSN 0268-3962. Dostupné z: doi:10.1057/jit.2015.29
- HASTINGS, Nelson, Rene PERALTA, Stefan POPOVENIUC a Andrew REGENSCHEID, 2011. Security Considerations for Remote Electronic UOCAVA Voting [online]. [cit. 2024-01-06]. Dostupné z: doi:10.6028/NIST.IR.7770
- HAYES, Helen A, Nicole GOODMAN, R. Michael MCGREGOR, Zachary SPICER a Scott PRUYERS, 2022. The Effect of Exogenous Shocks on the Administration of Online Voting: Evidence from Ontario, Canada. In: KRIMMER, Robert, Melanie VOLKAMER, David DUENAS-CID, Peter RØNNE a Micha GERMANN, ed. *Electronic Voting. E-Vote-ID 2022. Lecture Notes in Computer Science* [online]. 13553. Cham: Springer International Publishing, s. 70-89 [cit. 2023-03-14]. *Lecture Notes in Computer Science*. ISBN 978-3-031-15910-7. Dostupné z: doi:10.1007/978-3-031-15911-4_5
- HEIBERG, Sven, Arnis PARSOVS a Jan WILLEMSON, 2015a. Log Analysis of Estonian Internet Voting 2013–2014. In: HAENNI, Rolf, Reto E. KOENIG a Douglas WIKSTRÖM, ed. *E-Voting and Identity* [online]. Cham: Springer International Publishing, s. 19-34 [cit. 2023-12-29]. *Lecture Notes in Computer Science*. ISBN 978-3-319-22269-1. Dostupné z: doi:10.1007/978-3-319-22270-7_2
- HEIBERG, Sven, Arnis PARSOVS a Jan WILLEMSON, 2015b. Log Analysis of Estonian Internet Voting 2013–2015 [online]. 2015-08-13 [cit. 2024-01-05]. *Lecture Notes in Computer Science*. Dostupné z: https://eprint.iacr.org/2015/1211
- HEINMAA, Thomas, 2020. Special Voting Arrangements (SVAs) in Europe: In-Country Postal, Early, Mobile and Proxy Arrangements in Individual Countries: Vnitrostátní poštovní, předčasné, mobilní a proxy ujednání v jednotlivých zemích. *International IDEA* [online]. [cit. 2023-11-17]. Dostupné z: https://www.idea.int/news/special-voting-arrangements-svas-europe-country-postal-early-mobile-and-proxy-arrangements
- HERZBERG, Amir, Markus JAKOBSSON, Stanisław JARECKI, Hugo KRAWCZYK a Moti YUNG, 1997. Proactive public key and signature systems. In: *Proceedings of the 4th ACM conference on Computer and communications security - CCS '97* [online]. New York, New York, USA: ACM Press, s. 100-110 [cit. 2023-12-20]. ISBN 0897919122. Dostupné z: doi:10.1145/266420.266442
- HIRT, Martin a Kazuo SAKO, 2000. Efficient Receipt-Free Voting Based on Homomorphic Encryption. In: PRENEEL, Bart, ed. *Advances in Cryptology — EUROCRYPT 2000* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 539-556 [cit. 2024-06-26]. *Lecture Notes in Computer Science*. ISBN 978-3-540-67517-4. Dostupné z: doi:10.1007/3-540-45539-6_38
- HJALMARSSON, Friorik P, Gunnlaugur K. HREIOARSSON, Mohammad HAMDAQA a Gisli HJALMTYSSON, 2018. Blockchain-Based E-Voting System. In: 2018 IEEE 11th International Conference on Cloud Computing (CLOUD) [online]. IEEE, s. 983-986 [cit. 2024-06-26]. ISBN 978-1-5386-7235-8. Dostupné z: doi:10.1109/CLOUD.2018.00151
- IDENTITA OBČANA, 2024. Portál Identity občana [online]. [cit. 2024-09-12]. Dostupné z: https://www.identitaobcana.cz/
- INDEPENDENT PANEL ON INTERNET VOTING, 2014. Recommendations Report to the Legislative Assembly of British Columbia [online]. [cit. 2024-01-06]. Dostupné z: https://elections.bc.ca/docs/recommendations-report.pdf
- INTERNATIONAL IDEA, 2014. International Obligations for Elections [online]. [cit. 2024-07-01]. Dostupné z: https://www.idea.int/sites/default/files/publications/international-obligations-for-elections.pdf
- INTERNATIONAL IDEA, 2023. ICTs in Elections Database. *International IDEA* [online]. [cit. 2023-11-17]. Dostupné z: https://www.idea.int/data-tools/data/question
- INTERNATIONAL IDEA, 2024. Global in-country postal voting data. *International IDEA* [online]. [cit. 2024-09-19]. Dostupné z: https://www.idea.int/data-tools/tools/special-voting-arrangements/postal-in-country
- ISO, 2019. ISO/IEC 27018: 2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. *ISO* [online]. [cit. 2024-09-18]. Dostupné z: https://www.iso.org/standard/76559.html

- ISO, 2022. ISO/IEC 27001:2022. International Organization for Standardization [online]. [cit. 2024-07-01]. Dostupné z: <https://www.iso.org/standard/27001>
- ISO, 2015a. ISO/IEC 27017: 2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. ISO [online]. [cit. 2024-09-18]. Dostupné z: <https://www.iso.org/standard/43757.html>
- ISO, 2015b. ISO 9001: 2015 Quality management systems — Requirements. ISO [online]. [cit. 2024-09-18]. Dostupné z: <https://www.iso.org/standard/62085.html>
- ISO, 2023. ISO/IEC 25010:2023 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Product quality model: 2023 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Product quality model. ISO [online]. [cit. 2024-10-12]. Dostupné z: <https://www.iso.org/standard/78176.html>
- JAFAR, Uzma, Mohd Juzaidin AB AZIZ, Zarina SHUKUR a Hafiz Adnan HUSSAIN, 2022. A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. *Sensors* [online]. 22(19) [cit. 2024-06-28]. ISSN 1424-8220. Dostupné z: doi:10.3390/s22197585
- JAFAR, Uzma, Mohd Juzaidin Ab AZIZ a Zarina SHUKUR, 2021. Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors* [online]. 21(17) [cit. 2024-06-28]. ISSN 1424-8220. Dostupné z: doi:10.3390/s21175874
- JAIN, A.K., A. ROSS a S. PRABHAKAR, 2004. An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology* [online]. 14(1), 4-20 [cit. 2024-07-02]. ISSN 1051-8215. Dostupné z: doi:10.1109/TCSVT.2003.818349
- JAKOBSSON, Markus, Ari JUELS a Ron RIVEST, 2002. Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking. *Cryptology ePrint Archive* [online]. [cit. 2023-12-12]. Dostupné z: <https://eprint.iacr.org/2002/025>
- JEFFERSON, David, Aviel D. RUBIN, Barbara SIMONS a David WAGNER, 2004. Analyzing internet voting security. In: *Communications of the ACM* [online]. s. 59-64 [cit. 2024-06-24]. ISSN 0001-0782. Dostupné z: doi:10.1145/1022594.1022624
- JOHNSON, Desmond, 2019. Blockchain-Based Voting in the US and EU Constitutional Orders: A Digital Technology to Secure Democratic Values? *European Journal of Risk Regulation* [online]. 10(2), 330-358 [cit. 2024-07-02]. ISSN 1867-299X. Dostupné z: doi:10.1017/err.2019.40
- JUDGE, Elizabeth F a Amir M. KORHANI, 2020. Disinformation, Digital Information Equality, and Electoral Integrity. *Election Law Journal: Rules, Politics, and Policy* [online]. 2020-06-01, 19(2), 240-261 [cit. 2024-06-28]. ISSN 1533-1296. Dostupné z: doi:10.1089/elj.2019.0566
- JUELS, Ari, Dario CATALANO a Markus JAKOBSSON, 2005. Coercion-resistant electronic elections. *ACM Conferences* [online]. 61-70 [cit. 2023-10-12]. Dostupné z: doi:10.1145/1102199.1102213
- JUELS, Ari, Dario CATALANO a Markus JAKOBSSON, 2010. Coercion-Resistant Electronic Elections (Extended Abstract). In: CHAUM, David, Markus JAKOBSSON, Ronald L. RIVEST, Peter Y. A. RYAN, Josh BENALOH, Miroslaw KUTYLOWSKI a Ben ADIDA, ed. *Towards Trustworthy Elections* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 37-63 [cit. 2024-06-26]. *Lecture Notes in Computer Science*. ISBN 978-3-642-12979-7. Dostupné z: doi:10.1007/978-3-642-12980-3_2
- KARP, Jeffrey A. a Susan A. BANDUCCI, 2001. Absentee Voting, Mobilization, and Participation. In: *American Politics Research* [online]. s. 183-195 [cit. 2024-06-18]. ISSN 1532-673X. Dostupné z: doi:10.1177/1532673X01029002003
- KATZ, Jonathan a Yehuda LINDELL, 2007. *Introduction to modern cryptography: principles and protocols: principles and protocols*. Chapman and hall/CRC. ISBN 042914380X.
- KHAZAEI, Shahram, Bjorn TERELIUS a Douglas WIKSTROM, 2012. Cryptanalysis of a Universally Verifiable Efficient Re-Encryption Mixnet [online]. *KTH Royal Institute of Technology* [cit. 2023-12-12]. Dostupné z: <https://eprint.iacr.org/2012/100.pdf>
- KHO, Yun-Xing, Swee-Huay HENG a Ji-Jian CHIN, 2022. A Review of Cryptographic Electronic Voting. *Symmetry* [online]. 14(5) [cit. 2024-06-25]. ISSN 2073-8994. Dostupné z: doi:10.3390/sym14050858
- KING, Sunny a Scott NADAL, 2012. *Whitepaper: PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. *Peercoin.net* [online]. [cit. 2024-07-02]. Dostupné z: <https://www.peercoin.net/read/papers/peercoin-paper.pdf>
- KOENIG, Reto E., Philipp LOCHER a Rolf HAENNI, 2013. Attacking the Verification Code Mechanism in the Norwegian Internet Voting System. In: HEATHER, James, Steve SCHNEIDER a Vanessa TEAGUE, ed. *E-Voting and Identify* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 76-92 [cit. 2023-12-29]. *Lecture Notes in Computer Science*. ISBN 978-3-642-39184-2. Dostupné z: doi:10.1007/978-3-642-39185-9_5

- KOITMÄE, Arne, Jan WILLEMSON a Priit VINKEL, 2021. Vote Secrecy and Voter Feedback in Remote Voting – Can We Have Both? In: KRIMMER, Robert, Melanie VOLKAMER, David DUENAS-CID, Oksana KULYK, Peter RØNNE, Mihkel SOLVAK a Micha GERMANN, ed. *Electronic Voting* [online]. Cham: Springer International Publishing, s. 140-154 [cit. 2023-02-17]. *Lecture Notes in Computer Science*. ISBN 978-3-030-86941-0. Dostupné z: doi:10.1007/978-3-030-86942-7_10
- KOVAN, 2017. Stable Ethereum Public Testnet. GitHub [online]. [cit. 2024-07-02]. Dostupné z: <https://github.com/kovan-testnet/proposal/blob/master/README.md>
- KRAWCZYK, Hugo, Mihir BELLARE a Ran CANETTI, 1997. HMAC: Keyed-hashing for message authentication: Keyed-hashing for message authentication. ISSN 2070-1721.
- KREMER, Steve, Mark RYAN a Ben SMYTH, 2010. Election Verifiability in Electronic Voting Protocols. In: GRITZALIS, Dimitris, Bart PRENEEL a Marianthi THEOHARIDOU, ed. *Computer Security – ESORICS 2010* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 389-404 [cit. 2024-06-23]. *Lecture Notes in Computer Science*. ISBN 978-3-642-15496-6. Dostupné z: doi:10.1007/978-3-642-15497-3_24
- KRIMMER, Robert, David DUENAS-CID, Iuliia KRIVONOSOVA, Priit VINKEL a Arne KOITMAE, 2018. How Much Does an e-Vote Cost? Cost Comparison per Vote in Multichannel Elections in Estonia. In: KRIMMER, Robert, Melanie VOLKAMER, Véronique CORTIER, Rajeev GORÉ, Manik HAPSARA, Uwe SERDÜLT a David DUENAS-CID, ed. *Electronic Voting* [online]. Cham: Springer International Publishing, s. 117-131 [cit. 2023-02-17]. *Lecture Notes in Computer Science*. ISBN 978-3-030-00418-7. Dostupné z: doi:10.1007/978-3-030-00419-4_8
- KRIPS, Kristjan a Jan WILLEMSON, 2019. On Practical Aspects of Coercion-Resistant Remote Voting Systems. In: KRIMMER, Robert, Melanie VOLKAMER, Veronique CORTIER, Bernhard BECKERT, Ralf KÜSTERS, Uwe SERDÜLT a David DUENAS-CID, ed. *Electronic Voting* [online]. Cham: Springer International Publishing, s. 216-232 [cit. 2023-02-17]. *Lecture Notes in Computer Science*. ISBN 978-3-030-30624-3. Dostupné z: doi:10.1007/978-3-030-30625-0_14
- KSHETRI, Nir a Jeffrey VOAS, 2018. Blockchain-Enabled E-Voting. *IEEE Software* [online]. 35(4), 95-99 [cit. 2024-07-02]. ISSN 0740-7459. Dostupné z: doi:10.1109/MS.2018.2801546
- KUBJAS, Ivo, Tiit PIKMA a Jan WILLEMSON, 2017. Estonian Voting Verification Mechanism Revisited Again. In: KRIMMER, Robert, Melanie VOLKAMER, Nadja BRAUN BINDER, Norbert KERSTING, Olivier PEREIRA a Carsten SCHÜRMANN, ed. *Electronic Voting* [online]. Cham: Springer International Publishing, s. 306-317 [cit. 2023-02-17]. *Lecture Notes in Computer Science*. ISBN 978-3-319-68686-8. Dostupné z: doi:10.1007/978-3-319-68687-5_19
- KULYK, Oksana, Vanessa TEAGUE a Melanie VOLKAMER, 2015. Extending helios towards private eligibility verifiability. In: *E-Voting and Identity: 5th International Conference, VoteID 2015, September 2-4. Proceedings 5*. Bern, Switzerland: Springer International Publishing, s. 57-73.
- KULYK, Oksana a Melanie VOLKAMER, 2016. Efficiency Comparison of Various Approaches in E-Voting Protocols. In: CLARK, Jeremy, Sarah MEIKLEJOHN, Peter Y.A. RYAN, Dan WALLACH, Michael BRENNER a Kurt ROHLOFF, ed. *Financial Cryptography and Data Security* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 209-223 [cit. 2024-08-02]. *Lecture Notes in Computer Science*. ISBN 978-3-662-53356-7. Dostupné z: doi:10.1007/978-3-662-53357-4_14
- KUPKOVÁ, Lenka, Lenka PAVLÍKOVÁ, Kateřina ROVNÁ, Ondřej KAŠPÁREK a Radomír ŠUHEJ, 2013. E-volby v ČR [online]. Masarykova univerzita v Brně [cit. 2023-12-11]. Dostupné z: https://is.muni.cz/el/1421/podzim2013/VIKMA10/um/44524582/Evolby_2_verze.pdf
- KÜSTERS, Ralf, Tomasz TRUDERUNG a Andreas VOGT, 2010. Accountability. In: *Proceedings of the 17th ACM conference on Computer and communications security* [online]. New York, NY, USA: ACM, 2010-10-04, s. 526-535 [cit. 2024-06-23]. ISBN 9781450302456. Dostupné z: doi:10.1145/1866307.1866366
- KVALE, Steinar, 2009. *Interviews: Learning the craft of qualitative research interviewing: Learning the craft of qualitative research interviewing*. Sage.
- LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, 2019. Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet: NOR : CNIL1917529X. *Légifrance* [online]. [cit. 2023-04-06]. Dostupné z: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038661239>
- LEE RODGERS, Joseph a W Alan NICEWANDER, 1988. Thirteen ways to look at the correlation coefficient. *The American Statistician*. Taylor & Francis, 42(1), 59-66. ISSN 0003-1305.
- LENSTRA, Arjen K, 2006. Key lengths. *The Handbook of Information Security* [online]. Wiley [cit. 2024-09-26]. ISBN 0471648302. Dostupné z: <https://infoscience.epfl.ch/record/164539/files/NPDF-32.pdf>
- LICHT, Nathan, David DUENAS-CID, Iuliia KRIVONOSOVA a Robert KRIMMER, 2021. To i-vote or Not to i-vote: Drivers and Barriers to the Implementation of Internet Voting. In: KRIMMER, Robert, Melanie VOLKAMER, David DUENAS-CID, Oksana KULYK, Peter RØNNE, Mihkel SOLVAK a Micha GERMANN, ed. *Electronic Voting*

- [online]. Cham: Springer International Publishing, s. 91-105 [cit. 2023-02-17]. Lecture Notes in Computer Science. ISBN 978-3-030-86941-0. Dostupné z: doi:10.1007/978-3-030-86942-7_7
- LI, Huian, Abhishek Reddy KANKANALA a Xukai ZOU, 2014. A taxonomy and comparison of remote voting schemes. In: 2014 23rd International Conference on Computer Communication and Networks (ICCCN) [online]. IEEE, s. 1-8 [cit. 2023-12-27]. ISBN 978-1-4799-3572-7. Dostupné z: doi:10.1109/ICCCN.2014.6911807
- LI, Huilin, Yunnan LI, Yong YU, Baocang WANG a Kefei CHEN, 2021. A Blockchain-Based Traceable Self-Tallying E-Voting Protocol in AI Era. IEEE Transactions on Network Science and Engineering [online]. 2021-4-1, 8(2), 1019-1032 [cit. 2024-06-29]. ISSN 2327-4697. Dostupné z: doi:10.1109/TNSE.2020.3011928
- LIN, Jiaxi, Xiaofeng DU a Yang LI, 2016. Towards an Analysis of Verifiable Mix Network Properties. In: International Journal of Future Generation Communication and Networking [online]. 2016-07-31, s. 269-278 [cit. 2023-12-11]. ISSN 22337857. Dostupné z: doi:10.14257/ijfgcn.2016.9.7.25
- MARCOS DEL BLANCO, David Yeregui, 2018a. Cybersecurity applied to e-democracy: Cryptographic analysis and development of a Practical Evaluation Methodology for i-voting systems and its application to the most relevant solutions. Universidad de León.
- MARCOS DEL BLANCO, David Yeregui, Luis PANIZO ALONSO a Jose Angel HERMIDA ALONSO, 2018b. Review of Cryptographic Schemes applied to Remote Electronic Voting systems: remaining challenges and the upcoming post-quantum paradigm. Open Mathematics [online]. 2018-02-23, 16(1), 95-112 [cit. 2024-06-30]. ISSN 2391-5455. Dostupné z: doi:10.1515/math-2018-0013
- MARCOS DEL BLANCO, D. Y. a M. GASCÓ, 2019. A Protocolized, Comparative Study of Helios Voting and Scytl/iVote. In: 2019 Sixth International Conference on eDemocracy & eGovernment (ICEDEG) [online]. Quito, Ecuador: IEEE, s. 31-38 [cit. 2024-09-26]. ISBN 978-1-7281-1704-1. ISSN 2573-1998. Dostupné z: doi:10.1109/ICEDEG.2019.8734351
- MARCOS DEL BLANCO, David Yeregui, David DUENAS-CID a Héctor ALÁIZ MORETÓN, 2020. E-Voting System Evaluation Based on the Council of Europe Recommendations: nVotes. In: KRIMMER, Robert, Melanie VOLKAMER, Bernhard BECKERT, Ralf KÜSTERS, Oksana KULYK, David DUENAS-CID a Mihkel SOLVAK, ed. Electronic Voting [online]. Cham: Springer International Publishing, s. 147-166 [cit. 2023-02-17]. Lecture Notes in Computer Science. ISBN 978-3-030-60346-5. Dostupné z: doi:10.1007/978-3-030-60347-2_10
- MARTÍNEK, Tomáš a Petr HANZLÍK, 2013. Analysis of the influence of internet social networks on employee selection process in the Czech Republic. ACC Journal [online]. Liberec, (B), 77-88 [cit. 2024-02-15]. ISSN 1803-9782. Dostupné z: https://acc-ern.tul.cz/archiv/PDF/ACC_2013_2_07.pdf
- MARTÍNEK, Tomáš a Petr HANZLÍK, 2014. Analysis of the Structure of Job Offers on the Czech Labour Market. Review of Economic Perspectives [online]. 14(3), 287-306 [cit. 2024-02-15]. ISSN 1804-1663. Dostupné z: doi:10.2478/revecp-2014-0015
- MARTÍNEK, Tomáš, 2017. Možnosti zavedení elektronických voleb v České republice a jejich případné dopady. In: Think Together 2017 [online]. [cit. 2023-11-20]. ISSN 2788-2799. Dostupné z: <https://odvolit.cz/moznosti-zavedeni-elektronickych-voleb-v-ceske-republice-a-jejich-pripadne-dopady/>
- MARTÍNEK, Tomáš, 2018. Metodika pro otevřené výběrové řízení na politicky obsazované funkce. In: Think Together 2018 [online]. [cit. 2024-02-15]. ISSN 2788-2799. Dostupné z: <https://odvolit.cz/metodika-pro-otevrene-vyberove-rizeni-na-politicky-obsazovane-funkce/>
- MARTÍNEK, Tomáš a Lukáš FORÝTEK, 2022. The highly secure anonymous e-voting system of the Czech Pirate Party. In: KRIMMER, Robert, Melanie VOLKAMER, David DUENAS-CID, et al., ed. E-Vote-ID 2022: Seventh Joint International Conference on Electronic Voting [online]. 7. Estonia: University of Tartu Press, s. 165-168 [cit. 2024-09-26]. ISBN 978-9916-27-035-6. Dostupné z: doi:10.15157/diss/036
- MARTÍNEK, Tomáš, 2024a. Technical worksheet - Evaluation of the i-voting system - Recommendation CMRec(2017)5 of the Council of Europe. Zenodo [online]. [cit. 2024-09-22]. Dostupné z: doi:10.5281/zenodo.13825941
- MARTÍNEK, Tomáš a Jakub KONOPÁSEK, 2024b. Possibilities of introducing distance voting in the Czech parliamentary and presidential elections for voters abroad. In: Think Together 2024.
- MARTÍNEK, Tomáš a Michal MALÝ, 2024c. Questionnaire survey among members of the Czech Pirate Party regarding the use of the online voting system Helios. In: Zenodo [online]. [cit. 2024-03-18]. Dostupné z: doi:10.5281/zenodo.10829926
- MARTÍNEK, Tomáš a Michal MALÝ, 2024d. Evaluation of the I-Voting System for Remote Primary Elections of the Czech Pirate Party. Acta Informatica Pragensia [online]. 13(3), 395-417 [cit. 2024-07-28]. ISSN 1805-4951. Dostupné z: doi:10.18267/j.aip.249
- MARTÍNEK, Tomáš, Martin PELIKÁN, Jan TYRYCHTR a Jakub KONOPÁSEK, 2024e. Implementation of a Secret and Verifiable Personal Remote Electronic Election of an Agrarian Organization per the Recommendation of the

- Council of Europe. AGRIS on-line Papers in Economics and Informatics [online]. 16(3), 59-73 [cit. 2024-09-30]. ISSN 1804-1930. Dostupné z: doi:10.7160/aol.2024.160305
- MARTÍNEK, Tomáš a Martin REJMAN, 2024f. KontrolaWebu.pridat.eu - browser plugin for checking the trustworthiness of the visited website. Zenodo [online]. [cit. 2024-03-13]. Dostupné z: doi:10.5281/zenodo.10813490
- MARTÍNEK, Tomáš a Jan TYRYCHTR, 2024g. A questionnaire survey of expected characteristics of i-voting systems among students and graduates of agricultural colleges: [Data set]. In: Zenodo [online]. [cit. 2024-05-21]. Dostupné z: doi:10.5281/zenodo.11234690
- MARTÍNEK, Tomáš, 2024h. Resources related to the evaluation of electronic voting systems indexed in Web of Science [Data set]. Zenodo [online]. [cit. 2024-10-15]. Dostupné z: doi:10.5281/zenodo.13934387
- MATT, Bishop, 2002. Computer security: art and science: art and science. Addison-Wesley Professional. ISBN 0203301528.
- MCCLANAHAN, Patrick, 2024. What is Authentication?: Authentication. Engineering LibreTexts [online]. [cit. 2024-09-12]. Dostupné z: https://eng.libretexts.org/Courses/Delta_College/Information_Security/02%3A_Authenticate_and_Identify/2.2%3A_Authentication
- MCCORRY, Patrick, Siamak F. SHAHANDASHTI a Feng HAO, 2017. A Smart Contract for Boardroom Voting with Maximum Voter Privacy. In: KIAYIAS, Aggelos, ed. Financial Cryptography and Data Security [online]. Cham: Springer International Publishing, s. 357-375 [cit. 2024-06-26]. Lecture Notes in Computer Science. ISBN 978-3-319-70971-0. Dostupné z: doi:10.1007/978-3-319-70972-7_20
- MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES, 2023. Vote par internet. France Diplomatie - Ministère de l'Europe et des Affaires étrangères [online]. [cit. 2023-11-19]. Dostupné z: <https://www.diplomatie.gouv.fr/fr/services-aux-francais/voter-a-l-etranger/modalites-de-vote/vote-par-internet/>
- MINISTERSTVO VNITRA ČR, 2012. Informace o elektronickém způsobu hlasování [online]. [cit. 2024-01-09]. Dostupné z: <https://www.mvcr.cz/volby/soubor/priloha-1-informace-o-elektronickem-zpusobu-hlasovani.aspx>
- MINISTERSTVO VNITRA ČR, 2022. Vedení seznamu voličů. Volby [online]. [cit. 2024-09-13]. Dostupné z: <https://www.mvcr.cz/volby/clanek/vedeni-seznamu-volicu.aspx>
- MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČR, 2024. Zvláštní seznam voličů. Velvyslanectví České republiky v Hanoji [online]. [cit. 2024-09-13]. Dostupné z: https://mzv.gov.cz/hanoi/cz/vizove_a_konzularni_informace/volby/zvlastni_seznam_volicu.html
- MINISTRY OF LOCAL GOVERNMENT AND MODERNISATION, 2014. Internet voting pilot to be discontinued. Government.no [online]. [cit. 2024-01-06]. Dostupné z: <https://www.regjeringen.no/en/historical-archive/solbergs-government/Ministries/kmd/press-releases/2014/Internet-voting-pilot-to-be-discontinued/id764300/>
- MINISTRY OF LOCAL GOVERNMENT AND REGIONAL DEVELOPMENT, 2010. Specification, tenders, evaluation and contract. Government.no [online]. [cit. 2024-01-06]. Dostupné z: <https://www.regjeringen.no/en/historical-archive/Stoltenbergs-2nd-Government/Ministry-of-Local-Government-and-Regional-tema-og-redaksjonelt-innhold/kampanjesider/e-vote-trial/System-documentation/specification-tenders-evaluation-and-con/id612121/>
- MITNICK, Kevin a A KASPERAVIČIUS, 2004. CSEPS course workbook. NY: Mitnick Security Publishing.
- MITOMO, Masashi a Kaoru KUROSAWA, 2000. Attack for Flash MIX. In: OKAMOTO, Tatsuki, ed. Advances in Cryptology — ASIACRYPT 2000 [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 192-204 [cit. 2023-12-12]. Lecture Notes in Computer Science. ISBN 978-3-540-41404-9. Dostupné z: doi:10.1007/3-540-44448-3_15
- MITROU, Lilian, Dimitris GRITZALIS a Sokratis KATSIKAS, 2002. Revisiting Legal and Regulatory Requirements for Secure E-Voting. In: GHONAIMY, M. Adeeb, Mahmoud T. EL-HADIDI a Heba K. ASLAN, ed. Security in the Information Society [online]. Boston, MA: Springer US, s. 469-480 [cit. 2024-06-28]. IFIP Advances in Information and Communication Technology. ISBN 978-1-4757-1026-7. Dostupné z: doi:10.1007/978-0-387-35586-3_37
- MOLNÁR, Zdeněk, Stanislava MILDEOVÁ, Hana ŘEZANKOVÁ, Radim BRIXÍ a Jaroslav KALINA, 2012. Pokročilé metody vědecké práce. [Zeleneč]: Profess Consulting. Věda pro praxi (Profess Consulting). ISBN 978-80-7259-064-3.
- MONTGOMERY, Douglas C a George C RUNGER, 2010. Applied statistics and probability for engineers. John Wiley. ISBN 0470053046.
- MORAN, Tal a Moni NAOR, 2006. Receipt-Free Universally-Verifiable Voting with Everlasting Privacy. In: DWORK, Cynthia, ed. Advances in Cryptology - CRYPTO 2006 [online]. Berlin, Heidelberg: Springer Berlin

- Heidelberg, s. 373-392 [cit. 2023-12-29]. Lecture Notes in Computer Science. ISBN 978-3-540-37432-9. Dostupné z: doi:10.1007/11818175_22
- MUDANA, Sandeep, 2005. Security Flaws in Internet Voting System. Computer Science Department, University of Auckland [online]. [cit. 2023-12-31]. Dostupné z: <https://www.cs.auckland.ac.nz/courses/compsci725s2c/archive/termpapers/sr.pdf>
- NAKAMOTO, Satoshi, 2008. Bitcoin: A Peer-to-Peer Electronic Cash System [online]. [cit. 2024-07-02]. Dostupné z: <https://bitcoin.org/bitcoin.pdf>
- NAKIT, 2024. Národní agentura pro komunikační a informační technologie, s. p. [online]. [cit. 2024-09-12]. Dostupné z: <https://nakit.cz/>
- NEFF, C. Andrew, 2001. A verifiable secret shuffle and its application to e-voting. In: Proceedings of the 8th ACM conference on Computer and Communications Security [online]. New York, NY, USA: ACM, 2001-11-05, s. 116-125 [cit. 2023-12-12]. ISBN 1581133855. Dostupné z: doi:10.1145/501983.502000
- NEUMANN, Stephan a Melanie VOLKAMER, 2014. A Holistic Framework for the Evaluation of Internet Voting Systems. In: Design, Development, and Use of Secure Electronic Voting Systems [online]. IGI Global, s. 76-91 [cit. 2024-06-23]. Advances in Electronic Government, Digital Divide, and Regional Development. ISBN 9781466658202. Dostupné z: doi:10.4018/978-1-4666-5820-2.ch004
- NEUMANN, Stephan Rouven, 2016a. Evaluation and Improvement of Internet Voting Schemes Based on Legally-Founded Security Requirements [online]. Darmstadt [cit. 2023-10-13]. Dostupné z: <https://d-nb.info/1112269037/34>. Dissertation. Technischen Universität Darmstadt.
- NEUMANN, Stephan, Melanie VOLKAMER, Jurlind BUDURUSHI a Marco PRANDINI, 2016b. SecIVo: a quantitative security evaluation framework for internet voting schemes. In: Annals of Telecommunications [online]. s. 337-352 [cit. 2024-06-23]. ISSN 0003-4347. Dostupné z: doi:10.1007/s12243-016-0520-0
- NEUMANN, Stephan, Manuel NOLL a Melanie VOLKAMER, 2017. Election-Dependent Security Evaluation of Internet Voting Schemes. In: DE CAPITANI DI VIMERCATI, Sabrina a Fabio MARTINELLI, ed. ICT Systems Security and Privacy Protection [online]. Cham: Springer International Publishing, s. 371-382 [cit. 2024-08-02]. IFIP Advances in Information and Communication Technology. ISBN 978-3-319-58468-3. Dostupné z: doi:10.1007/978-3-319-58469-0_25
- NIST, 2020. Recommendation for Key Management – Part 1: General (Rev. 5): NIST SP 800-57 Part 1 Rev. 5 [online]. National Institute of Standards and Technology [cit. 2024-06-18]. Dostupné z: doi:10.6028/NIST.SP.800-57pt1r5
- NIST, 2023. FIPS 186-5: Digital Signature Standard (DSS). National Institute of Standards and Technology [online]. [cit. 2024-06-18]. Dostupné z: doi:10.6028/NIST.FIPS.186-5
- NIST, 2015. FIPS 180-4: Secure Hash Standard (SHS) [online]. [cit. 2024-06-18]. Dostupné z: doi:10.6028/NIST.FIPS.180-4
- NIST, 2020. Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology [online]. [cit. 2024-07-01]. Dostupné z: doi:10.6028/NIST.SP.800-53r5
- NORE, Henrik, 2013. Can we trust internet voting?: Internet voting in Norway. In: OAS.org [online]. [cit. 2024-01-06]. Dostupné z: https://www.oas.org/es/sap/deco/seminarios/peru/pre/Henrik_Nore.pdf
- NSW ELECTORAL COMMISSION, 2024. Telephone assisted voting. NSW Electoral Commission [online]. [cit. 2024-01-07]. Dostupné z: <https://elections.nsw.gov.au/voters/voting-options/telephone-assisted-voting>
- NSW ELECTORAL COMMISSION, 2023. Technology assisted voting. Elections.nsw.gov.au [online]. [cit. 2024-01-07]. Dostupné z: <https://elections.nsw.gov.au/getmedia/32e75622-e0d2-49df-9ffa-751fef5fedda/tav-review-final-report.pdf>
- NÚKIB, 2024. Nová směrnice EU o bezpečnosti sítí a informací NIS2. NÚKIB [online]. [cit. 2024-09-18]. Dostupné z: <https://osveta.nukib.gov.cz/course/view.php?id=184>
- NÚKIB, 2023. Minimální požadavky na kryptografické algoritmy. Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 2024-06-18]. Dostupné z: https://nukib.gov.cz/download/uredni_deska/Minimalni%20požadavky%20na%20kryptograficke%20algoritmy.pdf
- OCHRANA, František, 2019. Metodologie, metody a metodika vědeckého výzkumu. Praha: Univerzita Karlova, nakladatelství Karolinum. ISBN 978-80-246-4200-0.
- OLECKÁ, Ivana a Kateřina IVANOVÁ, 2010. Metodologie vědecko-výzkumné činnosti. Olomouc: Moravská vysoká škola Olomouc. ISBN 978-80-87240-33-5.
- OPENAIRE, 2024. Open Science in Europe. OpenAIRE.eu [online]. [cit. 2024-10-17]. Dostupné z: <http://www.openaire.eu/open-science-europe-overview>

- PAILLIER, Pascal, 1999. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In: STERN, Jacques, ed. *Advances in Cryptology — EUROCRYPT '99* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 223-238 [cit. 2023-11-29]. Lecture Notes in Computer Science. ISBN 978-3-540-65889-4. Dostupné z: doi:10.1007/3-540-48910-X_16
- PAL, Michael, 2020. Social Media and Democracy: Challenges for Election Law and Administration in Canada. *Election Law Journal: Rules, Politics, and Policy* [online]. 2020-06-01, 19(2), 200-213 [cit. 2024-06-28]. ISSN 1533-1296. Dostupné z: doi:10.1089/elj.2019.0557
- PANIZO ALONSO, L., M. GASCÓ, D. Y. MARCOS DEL BLANCO, J. Á. Hermida ALONSO, J. BARRAT a H. Aláiz MORETON, 2018. E-Voting System Evaluation Based on The Council of Europe Recommendations: Helios Voting. *IEEE Transactions on Emerging Topics in Computing* [online]. 9(1), 161-173 [cit. 2024-09-26]. ISSN 2168-6750. Dostupné z: doi:10.1109/TETC.2018.2881891
- PARDUE, Harold, Alec YASINSAC a Jeffrey LANDRY, 2010. Towards Internet voting security: A threat tree for risk assessment. In: 2010 Fifth International Conference on Risks and Security of Internet and Systems (CRISIS) [online]. IEEE, s. 1-7 [cit. 2024-08-02]. ISBN 978-1-4244-8641-0. Dostupné z: doi:10.1109/CRISIS.2010.5764925
- PARK, Choonsik, Kazutomo ITOH a Kaoru KUROSAWA, 1994. Efficient Anonymous Channel and All/Nothing Election Scheme. In: HELLESETH, Tor, ed. *Advances in Cryptology — EUROCRYPT '93* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994-7-13, s. 248-259 [cit. 2023-12-12]. Lecture Notes in Computer Science. ISBN 978-3-540-57600-6. Dostupné z: doi:10.1007/3-540-48285-7_21
- PARK, Sunoo, Michael SPECTER, Neha NARULA a Ronald L RIVEST, 2021. Going from bad to worse: from internet voting to blockchain voting: from internet voting to blockchain voting. *Journal of Cybersecurity*. Oxford University Press, 7(1), tyaa025. ISSN 2057-2085.
- PEARSON, Karl, 1895. VII. Note on regression and inheritance in the case of two parents. In: *Proceedings of the Royal Society of London* [online]. 1895-12-31, s. 240-242 [cit. 2024-05-31]. ISSN 0370-1662. Dostupné z: doi:10.1098/rspl.1895.0041
- PENG, Kun, Riza ADITYA, Colin BOYD, Ed DAWSON a Byoungcheon LEE, 2004. Multiplicative homomorphic e-voting. In: *International Conference on Cryptology in India*. Springer, s. 61-72.
- PEREIRA, Olivier, 2023. Individual Verifiability and Revoting in the Estonian Internet Voting System. In: MATSUO, Shin'ichiro, Lewis GUDGEON, Arian KLAGES-MUNDT, et al., ed. *Financial Cryptography and Data Security. FC 2022 International Workshops* [online]. Cham: Springer International Publishing, s. 315-324 [cit. 2024-01-16]. Lecture Notes in Computer Science. ISBN 978-3-031-32414-7. Dostupné z: doi:10.1007/978-3-031-32415-4_21
- PFITZMANN, Birgit, 1995. Breaking an efficient anonymous channel. In: DE SANTIS, Alfredo, ed. *Advances in Cryptology — EUROCRYPT'94* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 332-340 [cit. 2023-12-12]. Lecture Notes in Computer Science. ISBN 978-3-540-60176-0. Dostupné z: doi:10.1007/BFb0053448
- PFITZMANN, Birgit a Andreas PFITZMANN, 1990. How to Break the Direct RSA-Implementation of Mixes. In: QUISQUATER, Jean-Jacques a Joos VANDEWALLE, ed. *Advances in Cryptology — EUROCRYPT '89* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 1990-5-18, s. 373-381 [cit. 2023-12-12]. Lecture Notes in Computer Science. ISBN 978-3-540-53433-4. Dostupné z: doi:10.1007/3-540-46885-4_37
- POPOVENIUC, Stefan, John KELSEY, Andrew REGENSCHEID a Poorvi VORA, 2010. Performance Requirements for {End-to-End} Verifiable Elections. In: 2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 10) [online]. [cit. 2024-09-26]. Dostupné z: https://www.usenix.org/legacy/event/ewtote10/tech/full_papers/Popoveniuc.pdf
- POSLANECKÁ SNĚMOVNA PARLAMENTU ČR, 1992. Ústava České republiky. PSP.cz [online]. [cit. 2023-12-11]. Dostupné z: <https://www.psp.cz/docs/laws/constitution.html>
- PROCHÁZKOVÁ, Daniela a Adam KUČÍNSKÝ, 2024. Nový zákon o kybernetické bezpečnosti: Dopad regulace na obce. Ministerstvo vnitra ČR [online]. [cit. 2024-09-18]. Dostupné z: <https://www.mvcr.cz/soubor/porada-mv-s-tajemniky-orp-a-mc-hmp-ze-dne-19-brezna-2024-06-priloha-c-05-pdf.aspx>
- PUIGGALÍ ALLEPUZ, Jordi a Sandra GUASCH CASTELLÓ, 2010. Universally Verifiable Efficient Re-encryption Mixnet. *Electronic Voting* [online]. (vol. 167), 241-254 [cit. 2023-12-12]. Dostupné z: <https://dl.gi.de/server/api/core/bitstreams/634861de-abd7-4079-8651-8c443957aebc/content>
- PUIGGALÍ, Jordi, Jordi CUCURULL, Sandra GUASCH a Robert KRIMMER, 2017. Verifiability Experiences in Government Online Voting Systems. In: KRIMMER, Robert, Melanie VOLKAMER, Nadja BRAUN BINDER, Norbert KERSTING, Olivier PEREIRA a Carsten SCHÜRMANN, ed. *Electronic Voting* [online]. Cham: Springer International Publishing, s. 248-263 [cit. 2023-02-17]. Lecture Notes in Computer Science. ISBN 978-3-319-68686-8. Dostupné z: doi:10.1007/978-3-319-68687-5_15

- PUIGGALI, Jorgi a Victor MORALES-ROCHA, 2007. Remote Voting Schemes: A Comparative Analysis: A Comparative Analysis. In: E-Voting and Identity. Vote-ID 2007. Lecture Notes in Computer Science [online]. 4896. Berlin, Heidelberg: Springer, s. 16-28 [cit. 2023-11-14]. ISBN 978-3-540-77493-8. Dostupné z: doi:10.1007/978-3-540-77493-8_2
- RIVEST, R. L., A. SHAMIR a L. ADLEMAN, 1978. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM [online]. 21(2), 120-126 [cit. 2023-12-11]. ISSN 0001-0782. Dostupné z: doi:10.1145/359340.359342
- RIVEST, Ronald, 1992. RFC1321: The MD5 message-digest algorithm: The MD5 message-digest algorithm. RFC Editor.
- RODRÍGUEZ-PÉREZ, Adrià, 2020. My Vote, My (Personal) Data: Remote Electronic Voting and the General Data Protection Regulation. In: KRIMMER, Robert, Melanie VOLKAMER, Bernhard BECKERT, Ralf KÜSTERS, Oksana KULYK, David DUENAS-CID a Mihkel SOLVAK, ed. Electronic Voting [online]. Cham: Springer International Publishing, s. 167-182 [cit. 2023-02-17]. Lecture Notes in Computer Science. ISBN 978-3-030-60346-5. Dostupné z: doi:10.1007/978-3-030-60347-2_11
- RODRÍGUEZ-PÉREZ, Adrià, 2022a. The Council of Europe's CM/Rec(2017)5 on e-voting and Secret Suffrage: Time for yet Another Update? In: KRIMMER, Robert, Melanie VOLKAMER, David DUENAS-CID, Peter RØNNE a Micha GERMANN, ed. Electronic Voting [online]. 13553. Cham: Springer International Publishing, s. 90-105 [cit. 2023-02-17]. Lecture Notes in Computer Science. ISBN 978-3-031-15910-7. Dostupné z: doi:10.1007/978-3-031-15911-4_6
- RODRÍGUEZ-PÉREZ, Adrià, Jordi CUCURULL a Jordi PUIGGALÍ, 2022b. Voter Authentication in Remote Electronic Voting Governmental Experiences: Requirements and Practices. In: KRIMMER, Robert, Marius ROHDE JOHANNESSEN, Thomas LAMPOLTSHAMMER, Ida LINDGREN, Peter PARYCEK, Gerhard SCHWABE a Jolien UBACHT, ed. Electronic Participation [online]. Cham: Springer Nature Switzerland, s. 3-18 [cit. 2024-08-18]. Lecture Notes in Computer Science. ISBN 978-3-031-23212-1. Dostupné z: doi:10.1007/978-3-031-23213-8_1
- ROEDER, Tom, 2007. Asymmetric-Key Cryptography. Cornell University [online]. [cit. 2023-12-11]. Dostupné z: <https://www.cs.cornell.edu/courses/cs5430/2013sp/TL04.asymmetric.html>
- ROMANOV, Bogdan a Yury KABANOV, 2020. The Oxymoron of the Internet Voting in Illiberal and Hybrid Political Contexts. In: KRIMMER, Robert, Melanie VOLKAMER, Bernhard BECKERT, Ralf KÜSTERS, Oksana KULYK, David DUENAS-CID a Mihkel SOLVAK, ed. Electronic Voting [online]. Cham: Springer International Publishing, s. 183-195 [cit. 2023-02-17]. Lecture Notes in Computer Science. ISBN 978-3-030-60346-5. Dostupné z: doi:10.1007/978-3-030-60347-2_12
- RUPNIK, Jacques, 2022. How Viktor Orbán Wins. Journal of Democracy [online]. [cit. 2023-11-17]. Dostupné z: <https://www.journalofdemocracy.org/articles/how-viktor-orban-wins/>
- RYAN, P.Y.A., D. BISMARCK, J. HEATHER, S. SCHNEIDER a ZHE XIA, 2009. Prêt À Voter: a Voter-Verifiable Voting System. IEEE Transactions on Information Forensics and Security [online]. 4(4), 662-673 [cit. 2023-12-31]. ISSN 1556-6013. Dostupné z: doi:10.1109/TIFS.2009.2033233
- SAKO, Kazuo a Joe KILIAN, 1995. Receipt-Free Mix-Type Voting Scheme. In: Advances in Cryptology — EUROCRYPT '95 [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995-7-13, s. 393-403 [cit. 2023-10-12]. Lecture Notes in Computer Science. ISBN 978-3-540-59409-3. Dostupné z: doi:10.1007/3-540-49264-X_32
- SAMPIGETHAYA, Krishna a Radha POOVENDRAN, 2006. A framework and taxonomy for comparison of electronic voting schemes [online]. 25(2), 137-153 [cit. 2024-06-23]. ISSN 01674048. Dostupné z: doi:10.1016/j.cose.2005.11.003
- SAUER, Pjotr, 2021. Rusové říkají, že jsou nuceni volit ve volbách, tentokrát online. The Moscow Times [online]. [cit. 2024-09-15]. Dostupné z: <https://www.themoscowtimes.com/2021/09/08/russians-say-they-are-being-forced-to-vote-in-elections-this-time-online-a74999>
- SCHLAUFER, Caroline, 2021. Why do nondemocratic regimes promote e-participation? The case of Moscow's active citizen online voting platform. Governance [online]. 34(3), 821-836 [cit. 2024-06-29]. ISSN 0952-1895. Dostupné z: doi:10.1111/gove.12531
- SCHMIDT, Axel, Dennis HEINSON, Lucie LANGER, Zoi OPITZ-TALIDOU, Philipp RICHTER, Melanie VOLKAMER a Johannes BUCHMANN, 2009. Developing a Legal Framework for Remote Electronic Voting. In: RYAN, Peter Y. A. a Berry SCHOENMAKERS, ed. E-Voting and Identity [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 92-105 [cit. 2024-06-28]. Lecture Notes in Computer Science. ISBN 978-3-642-04134-1. Dostupné z: doi:10.1007/978-3-642-04135-8_6
- SCHNEIER, Bruce, 2015. Applied cryptography: protocols, algorithms, and source code in C. 20th anniversary edition. Indianapolis: Wiley. ISBN 978-1-119-09672-6.

- SCHWARTZ, Bryan a Dan GRICE, 2013. Establishing a Legal Framework for E-Voting in Canada. Elections Canada [online]. [cit. 2024-06-28]. Dostupné z: https://www.elections.ca/res/rec/tech/elfec/pdf/elfec_e.pdf
- SEKIBUULE, Richard, 2007. Security analysis of remote e-voting. In: Strengthening the Role of ICT in Development. Fountain Publishers Kampala. ISBN 9970027301.
- SHAHZAD, Basit a Jon CROWCROFT, 2019. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access [online]. 7, 24477-24488 [cit. 2024-06-28]. ISSN 2169-3536. Dostupné z: doi:10.1109/ACCESS.2019.2895670
- SHAMIR, Adi, 1979. How to share a secret. Commun. ACM. 22, 612-613.
- SHAPIRO, Samuel Sanford a Martin B WILK, 1965. An analysis of variance test for normality (complete samples). Biometrika. Oxford University Press, 52(3-4), 591-611. ISSN 1464-3510.
- SHEER HARDWICK, Freya, Apostolos GIOULIS, Raja NAEEM AKRAM a Konstantinos MARKANTONAKIS, 2018. E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) [online]. IEEE, s. 1561-1567 [cit. 2024-06-26]. ISBN 978-1-5386-7975-3. Dostupné z: doi:10.1109/Cybermatics_2018.2018.00262
- SOLVAK, Mihkel, 2020. Does Vote Verification Work: Usage and Impact of Confidence Building Technology in Internet Voting. In: KRIMMER, Robert, Melanie VOLKAMER, Bernhard BECKERT, Ralf KÜSTERS, Oksana KULYK, David DUENAS-CID a Mihkel SOLVAK, ed. Electronic Voting [online]. Cham: Springer International Publishing, s. 213-228 [cit. 2023-02-17]. Lecture Notes in Computer Science. ISBN 978-3-030-60346-5. Dostupné z: doi:10.1007/978-3-030-60347-2_14
- SOLVAK, Mihkel, Kristjan VASSIL a Tartu ÜLIKOOL, 2016. E-voting in Estonia: technological diffusion and other developments over ten years (2005-2015). In: DIGAR [online]. University of Tartu [cit. 2024-01-05]. Dostupné z: <https://www.digar.ee/arhiiv/en/books/62510>
- SPCSS, 2024. Státní pokladna Centrum sdílených služeb, s. p [online]. [cit. 2024-09-12]. Dostupné z: <https://www.spcss.cz/>
- SPECTER, Michael a J. Alex HALDERMAN, 2021. Security Analysis of the Democracy Live Online Voting System. 30th USENIX Security Symposium (USENIX Security 21) [online]. [cit. 2024-01-07]. Dostupné z: <https://www.usenix.org/conference/usenixsecurity21/presentation/specter-security>
- SPRINGALL, Drew, Travis FINKENAUER, Zakir DURUMERIC, Jason KITCAT, Harri HURSTI, Margaret MACALPINE a J. Alex HALDERMAN, 2014. Security Analysis of the Estonian Internet Voting System. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security [online]. New York, NY, USA: ACM, 2014-11-03, s. 703-715 [cit. 2023-02-17]. ISBN 9781450329576. Dostupné z: doi:10.1145/2660267.2660315
- SSSVD, 2024. Správa státních služeb vytvářejících důvěru, s. p. o. [online]. [cit. 2024-09-12]. Dostupné z: <https://sssvd.gov.cz/>
- STALLINGS, William, 2020. Cryptography and network security: principles and practice. Eighth edition. Harlow: Pearso. ISBN 978-1-292-43748-4.
- SWISS POST, 2024. E-voting Online voting and elections. Swiss Post [online]. [cit. 2024-02-22]. Dostupné z: <https://digital-solutions.post.ch/en/e-government/digitization-solutions/e-voting>
- TAŞ, Ruhi a Ömer Özgür TANRIÖVER, 2020. A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting. Symmetry [online]. 12(8) [cit. 2024-07-02]. ISSN 2073-8994. Dostupné z: doi:10.3390/sym12081328
- TE TARI TAIWHENUA | DEPARTMENT OF INTERNAL AFFAIRS, 2019. Online voting. In: Dia.govt.nz [online]. [cit. 2023-10-13]. Dostupné z: <https://www.dia.govt.nz/online-voting>
- THE BELL, 2024. Online voting, electronic manipulation. The Bell [online]. [cit. 2024-09-15]. Dostupné z: <https://en.thebell.io/online-voting-electronic-manipulation/>
- THE CARTER CENTER, 2014. Summary: Expert Study Mission Report The Carter Center Internet Voting Pilot : Norway's 2013 Parliamentary Elections [online]. [cit. 2023-10-12]. Dostupné z: https://www.regjeringen.no/globalassets/upload/krd/kampanjer/valgportal/valgobservatorer/2013/rapport_cartersenteret2013.pdf
- THE COMMON CRITERIA RECOGNITION AGREEMENT, 2009. Common criteria for information technology security evaluation part 1: Introduction and general model july 2009. In: Nist [online]. Vol. 49. [cit. 2023-10-13].
- THE SWISS FEDERAL CHANCELLERY, 2022. Federal Chancellery Ordinance on Electronic Voting. Fedlex [online]. [cit. 2024-02-21]. Dostupné z: <https://www.fedlex.admin.ch/eli/cc/2022/336/en>
- THE SWISS FEDERAL CHANCELLERY, 2018. Federal Chancellery Ordinance on Electronic Voting. Fedlex.admin.ch [online]. [cit. 2024-01-07]. Dostupné z: <https://www.fedlex.admin.ch/eli/cc/2013/859/en>

- TIDEMAN, Nicolaus, 2006. Collective Decisions and Voting: The Potential for Public Choice. In: Routledge [online]. London [cit. 2024-06-14]. ISBN 9781315259963. Dostupné z: doi:10.4324/9781315259963
- TOEPFL, Florian, 2018. Innovating consultative authoritarianism: Internet votes as a novel digital tool to stabilize non-democratic rule in Russia. *New Media & Society* [online]. 20(3), 956-972 [cit. 2024-09-15]. ISSN 1461-4448. Dostupné z: doi:10.1177/1461444816675444
- TOOB, 2009. File: Digital Signature diagram cs.svg. Wikimedia Commons [online]. [cit. 2023-12-20]. Dostupné z: https://commons.wikimedia.org/wiki/File:Digital_Signature_diagram_cs.svg
- TRANSPARENCY INTERNATIONAL, 2014. Masová manipulace u voleb potvrzena. *Transparency.cz* [online]. [cit. 2023-12-22]. Dostupné z: <https://www.transparency.cz/masova-manipulace-u-voleb-potvrzena/>
- TSOUKALAS, Georgios, Kostas PAPADIMITRIOU a Panos LOURIDAS, 2013. From helios to zeus. *USENIX Journal of Election Technology and Systems (JETS)* [online]. 1(1), 1-17 [cit. 2024-09-26]. ISSN 2328-2797. Dostupné z: <https://www.usenix.org/system/files/jets/issues/jets-0101-tsoukalas.pdf>
- U.S. VOTE FOUNDATION, 2015. E2E-VIV Project: The Future of Voting: End-to-End Verifiable Internet Voting - Specification and Feasibility Study. In: U.S. Vote Foundation [online]. [cit. 2023-10-16]. Dostupné z: <https://www.usvotefoundation.org/E2E-VIV>
- VALIMISED, 2024. IVXV online voting system. GitHub [online]. [cit. 2024-01-06]. Dostupné z: <https://github.com/valimised/ivxv>
- VALIMISED.EE, 2023. Statistics about Internet voting in Estonia. *Valimised.ee* [online]. [cit. 2024-01-05]. Dostupné z: <https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia>
- VALIMISED.EE, 2024a. Internet voting in Estonia. Elections in Estonia [online]. [cit. 2024-09-03]. Dostupné z: <https://www.valimised.ee/index.php/en/internet-voting-estonia>
- VALIMISED.EE, 2024b. Introduction to i-voting. Elections in Estonia [online]. [cit. 2024-09-03]. Dostupné z: <https://www.valimised.ee/index.php/en/internet-voting/more-about-i-voting/introduction-i-voting>
- VAN ECK, Nees Jan a Ludo WALTMAN, 2010. Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics* [online]. 84(2), 523-538 [cit. 2024-10-14]. ISSN 0138-9130. Dostupné z: doi:10.1007/s11192-009-0146-3
- VOLKAMER, Melanie, 2009. Evaluation of Electronic Voting [online]. [cit. 2024-06-23]. Dostupné z: doi:10.1007/978-3-642-01662-2
- VOLKAMER, Melanie a Rüdiger GRIMM, 2009. Determine the Resilience of Evaluated Internet Voting Systems. In: 2009 First International Workshop on Requirements Engineering for e-Voting Systems [online]. IEEE, s. 47-54 [cit. 2024-08-02]. ISBN 978-1-4244-7698-5. Dostupné z: doi:10.1109/RE-VOTE.2009.2
- VOLKAMER, Melanie a Margaret MCGALEY, 2007. Requirements and Evaluation Procedures for eVoting. In: The Second International Conference on Availability, Reliability and Security (ARES'07) [online]. IEEE, s. 895-902 [cit. 2024-06-23]. ISBN 0-7695-2775-2. Dostupné z: doi:10.1109/ARES.2007.124
- VOLKAMER, Melanie, Oliver SPYCHER a Eric DUBUIS, 2011. Measures to establish trust in internet voting. Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance [online]. New York, NY, USA: ACM, 2011-09-26, 1-10 [cit. 2024-05-08]. ISBN 9781450307468. Dostupné z: doi:10.1145/2072069.2072071
- VON NOSTITZ, Felix, Giulia SANDRI a Jordi Barrat i ESTEVE, 2021. Regulating i-Voting Within Countries and Parties. In: BARBERÀ, Oscar, Giulia SANDRI, Patricia CORREA a Juan RODRÍGUEZ-TERUEL, ed. Digital Parties [online]. Cham: Springer International Publishing, s. 43-66 [cit. 2024-02-25]. Studies in Digital Politics and Governance. ISBN 978-3-030-78667-0. Dostupné z: doi:10.1007/978-3-030-78668-7_3
- VRANA, Ivan, Jan TYRYCHTR a Martin PELIKÁN, 2021. BeCoMe: Easy-to-implement optimized method for best-compromise group decision making: Flood-prevention and COVID-19 case studies: Easy-to-implement optimized method for best-compromise group decision making. *Environmental Modelling & Software* [online]. 136, 104953 [cit. 2024-09-26]. ISSN 1364-8152. Dostupné z: doi:10.1016/j.envsoft.2020.104953
- VRANA, Ivan, Jiří VANÍČEK, Pavel KOVÁŘ, Jiří BROŽEK a Shady ALY, 2012. A group agreement-based approach for decision making in environmental issues. *Environmental Modelling & Software* [online]. 36, 99-110 [cit. 2024-08-08]. ISSN 13648152. Dostupné z: doi:10.1016/j.envsoft.2011.12.007
- W3C, 2008. Web Content Accessibility Guidelines (WCAG) 2.0. W3C [online]. [cit. 2024-09-16]. Dostupné z: <https://www.w3.org/TR/WCAG20/>
- W3C, 2024. Web Accessibility Evaluation Tools List. Web Accessibility Initiative (WAI) [online]. [cit. 2024-09-16]. Dostupné z: <https://www.w3.org/WAI/test-evaluate/tools/list/>
- W3C, 2023. Web Content Accessibility Guidelines (WCAG) 2.2. W3C [online]. [cit. 2024-09-16]. Dostupné z: <https://www.w3.org/TR/WCAG22/>
- W3C WEB ACCESSIBILITY INITIATIVE (WAI), 2023. Zásady přístupnosti. Web Accessibility Initiative (WAI) [online]. [cit. 2023-12-27]. Dostupné z: <https://www.w3.org/WAI/fundamentals/accessibility-principles/cs>

- WACK, John, 2014. IEEE VSSC/1622: Voting System Standards. In: National Institute of Standards and Technology [online]. [cit. 2023-11-15]. Dostupné z: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=916378
- WALSH, Paul, 2008. U student who offered his vote on eBay gets community service. Star Tribune [online]. [cit. 2023-12-22]. Dostupné z: <https://www.startribune.com/u-student-who-offered-his-vote-on-ebay-gets-community-service/26063069/>
- WANG, Xiaoyun a Hongbo YU, 2005. How to Break MD5 and Other Hash Functions. In: CRAMER, Ronald, ed. Advances in Cryptology – EUROCRYPT 2005 [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 19-35 [cit. 2023-12-20]. Lecture Notes in Computer Science. ISBN 978-3-540-25910-7. Dostupné z: doi:10.1007/11426639_2
- WEDOS, 2022. Wedos Global Protection. Wedos.com [online]. [cit. 2024-01-02]. Dostupné z: <https://www.wedos.com/cs/protection>
- WIKSTRÖM, Douglas, 2004. Five Practical Attacks for “Optimistic Mixing for Exit-Polls.” In: MATSUI, Mitsuru a Robert J. ZUCCHERATO, ed. Selected Areas in Cryptography [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 160-174 [cit. 2023-12-12]. Lecture Notes in Computer Science. ISBN 978-3-540-21370-3. Dostupné z: doi:10.1007/978-3-540-24654-1_12
- WIKSTRÖM, Douglas, 2007. Verificatum [online]. [cit. 2023-12-12]. Dostupné z: <https://www.verificatum.com/>
- WILLEMSON, Jan, 2017. Bits or Paper: Which Should Get to Carry Your Vote? In: KRIMMER, Robert, Melanie VOLKAMER, Nadja BRAUN BINDER, Norbert KERSTING, Olivier PEREIRA a Carsten SCHÜRMANN, ed. Electronic Voting [online]. Cham: Springer International Publishing, s. 292-305 [cit. 2024-08-02]. Lecture Notes in Computer Science. ISBN 978-3-319-68686-8. Dostupné z: doi:10.1007/978-3-319-68687-5_18
- WILLEMSON, Jan a Kristjan KRIPS, 2023. Estimating Carbon Footprint of Paper and Internet Voting. Electronic Voting [online]. Cham: Springer Nature Switzerland, 2023-09-22, 140-155 [cit. 2024-01-05]. Lecture Notes in Computer Science. ISBN 978-3-031-43755-7. Dostupné z: doi:10.1007/978-3-031-43756-4_9
- WOLCHOK, Scott, Eric WUSTROW, Dawn ISABEL a J. Alex HALDERMAN, 2012. Attacking the Washington, D.C. Internet Voting System. In: KEROMYTIS, Angelos D., ed. Financial Cryptography and Data Security [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 114-128 [cit. 2023-12-29]. Lecture Notes in Computer Science. ISBN 978-3-642-32945-6. Dostupné z: doi:10.1007/978-3-642-32946-3_10
- XU, Rui, Liusheng HUANG, Wei YANG a Libao HE, 2011. Quantum group blind signature scheme without entanglement. Optics Communications [online]. 284(14), 3654-3658 [cit. 2024-06-26]. ISSN 00304018. Dostupné z: doi:10.1016/j.optcom.2011.03.083
- ZAHRADNICKÝ, Tomáš a Jiří BUČEK, 2015. Stanovisko Fakulty informačních technologií Českého vysokého učení technického v Praze k dotazům Ministerstva vnitra České republiky v rámci pracovní skupiny k problematice distančního hlasování ve volbách v České republice. České vysoké učení technické v Praze, Fakulta informačních technologií. Praha.
- ZISSIS, Dimitrios a Dimitrios LEKKAS, 2014. Design, Development, and Use of Secure Electronic Voting Systems. In: Advances in Electronic Government, Digital Divide, and Regional Development [online]. IGI Global [cit. 2023-10-13]. ISSN 2326-9103. Dostupné z: doi:10.4018/978-1-4666-5820-2.ch004
- ZISSIS, Dimitrios a Dimitrios LEKKAS, 2011. Securing e-Government and e-Voting with an open cloud computing architecture. Government Information Quarterly [online]. 28(2), 239-251 [cit. 2024-06-29]. ISSN 0740624X. Dostupné z: doi:10.1016/j.giq.2010.05.010
- ZOLLINGER, Marie-Laure, Ehsan ESTAJI, Peter Y. A. RYAN a Karola MARKY, 2021. “Just for the Sake of Transparency”: Exploring Voter Mental Models of Verifiability. In: KRIMMER, Robert, Melanie VOLKAMER, David DUENAS-CID, Oksana KULYK, Peter RØNNE, Mihkel SOLVAK a Micha GERMANN, ed. Electronic Voting [online]. Cham: Springer International Publishing, s. 155-170 [cit. 2023-02-17]. Lecture Notes in Computer Science. ISBN 978-3-030-86941-0. Dostupné z: doi:10.1007/978-3-030-86942-7_11

Přílohy

Příloha A: Požadavky na vzdálené hlasovací systémy dle Marcos del Blanco (2018)

V celé této příloze jsou citovány přeložené požadavky na vzdálené hlasovací systémy tak, jak je definuje Marcos del Blanco (2018). Příloha je doplněna o subjektivní hodnocení systému Belenios s využitím kvalifikovaných označení "splněno" (○), "nesplněno" (×) nebo "splněno za určitých podmínek" (Δ) u jednotlivých bodů a bodového hodnocení u kategorií požadavků.

Kritérium	H	Kód	Vysvětlení
Ověřitelnost konec-konec	Δ	E2Ev	Systém pro vzdálené elektronické hlasování je end-to-end verifikovatelný, pokud je každý hlas odevzdán dle plánu, zaznamenan jako odevzdaný a započítán jako zaznamenaný, (Popoveniuc, 2010; Benaloh, 2015; Chaum, 2004; Benaloh, 2006; Jonker, 2013; Castelló, 2016), nebo-li: Odevzdán dle plánu: Voliči mají přístup k důkazům, že jejich zašifrovaný hlas přesně odráží jejich volbu. Proto je vyžadováno, aby proces hlasování používal zabezpečené komunikační kanály, které zaručí, že žádný útok nezmění hlasování a že vše je ověřitelné. Zaznamenan jako odevzdaný: Voliči nebo delegáti mohou ověřit, že jejich hlasy byly řádně zahrnuty, přičemž konkrétní zašifrované hodnoty hlasů lze ověřit ve veřejném seznamu zašifrovaných hlasů. V tomto případě je voliči obvykle poskytnut určitý typ informace formy stvrzenky, aby si později v seznamu ověřil, že jeho hlas byl správně zaregistrován. Započítán jako zaznamenaný: Každý si může ověřit, že všechny zveřejněné zašifrované hlasy jsou správné a že byly zahrnuty do sčítání, ačkoliv neexistuje způsob, jak zjistit, jak kterýkoliv volič hlasoval. K tomuto se používají mixnety nebo homomorfni šifrování. Tyto vlastnosti společně s ověřením způsobilosti (Kremer, 2010), kdy hlasy byly předloženy verifikovaně pouze oprávněnými voliči, tvoří dle Marcos del Blanco (2018) princip konec-konec, nebo-li ověřitelnost end-to-end, zkráceně E2Ev. Volič či pozorovatel musí také být schopen ověřit svůj hlas bez ohledu na použitý software a bez potřeby zvláštních znalostí kryptografie.
Soukromí a odolnost nátlaku	×	CR	Protože hlasování probíhá v nekontrolovaném prostředí na různých nekontrolovaných zařízeních zvyšuje se složitost spojená se zachováním soukromí. Ochrana soukromí v rámci vzdálených elektronických systémů zahrnuje 3 úrovně od nejnižší: Tajnost při hlasování: Hlas voliče není nikomu prozrazen. Absence potvrzení: Volič nemůže získat potvrzení, které by mohl zneužít útočník pro zjištění konkrétní podoby hlasovacího lístku. Odolnost vůči nátlaku: Volič nemá možnost prokázat osobě, která vyvíjí nátlak na voliče ohledně hlasování, jak volič hlasoval i v případě, že by volič dobrovolně aktivně spolupracoval s osobou, která nátlak vyvíjí.
Nedotknutelnost	6,5	I-n	
	Δ	I-1	Ochrana softwaru a pomocných systémů pomocí dostatečně bezpečných systémů ověřování. Přístup z aplikací třetích stran/webových nebo zranitelných serverů není povolen. (Chápe se jako myšlenka, že jak software, tak pomocné systémy musí být přiměřeně chráněny dostatečně bezpečnými autentizačními protokoly, jako jsou hesla, jednorázové přístupové kódy, čipové karty, elektronická dokumentace atd., i prokazatelnou spolehlivostí, zabraňující přístupu přes aplikace třetích stran nebo zranitelné servery.)
	Δ	I-2	Existence protokolů pro opatření v případě narušení nedotknutelnosti. (Rovněž je oceňována existence podrobných a ověřených protokolů, které mají být použity v případě, že nedotknutelnost je ohrožena nebo dokonce porušena.)
	Δ	I-3	K dispozici jsou nástroje pro sledování a offline zálohy. (Musí existovat nástroje pro lokalizaci a rekonstrukci stopy útoku, stejně jako záložní kopie všech relevantních volebních informací zcela oddělených od připojených komponent systému vzdáleného elektronického hlasování.)
	Δ	I-4	Distribuované řízení kritických uzlů se sdílením rolí pro minimalizaci rizika tajných dohod. (Kontrola kritických uzlů je prováděna distribuovaným způsobem a nikdy ne skupinou příbuzných lidí nebo stejnými týmy lidí.)
	Δ	I-5	Existence protokolů o hodnocení rizik a modelování hrozeb.
	Δ	I-6	Implementace principů modularity s cílem co nejvíce omezit chyby nebo útoky. (Jsou implementovány principy modularity v maximální možné míře tak, aby potenciální chyby nebo útoky byly co možná nejvíce omezeny.)
	○	I-7	Správná aktualizace položek I-1...I-6 (Provádí se správně aktualizace výše uvedených akcí a zásad.)
Použitelnost	6	U-n	Důležitým přínosem elektronického hlasování může být zlepšení přístupnosti a použitelnosti volebního systému například pro osoby se sníženou pohyblivostí, zrakově postižené nebo jinak zdravotně handicapované, obyvatele odlehklých oblastí včetně zahraničí a jiné. Volič má specifické znalosti v oblasti ICT, použitelnost systému je proto důležitá s ohledem na technickou gramotnost voličů i dle různých publikací (U.S. Vote Foundation, 2015; Popoveniuc, 2010; Li, 2014; Benaloh, 2015; Zissis, 2014).
	Δ	U-1	Jednoduchost procesů ověřování, hlasování a ověřování. (Jednoduchost v procesech autentizace, hlasování i ověřování - bez ohrožení ověřitelnosti a soukromí)

	Δ	U-2	Zvláštní pozornost skupinám osob se zdravotním postižením/negramotných osob v souladu s ustanoveními Rady Evropy a OSN. (Pokud jde o osoby s tělesným postižením a skupiny bez gramotnosti (právo v případě osob s mentálním postižením je nejednoznačné a je předmětem sporů), je nutné, aby byly považovány za skupiny zvláštního zájmu. Zohledňovat požadavky přístupnosti je nutné i s ohledem na Úmluvu o právech osob se zdravotním postižením (OSN, 2006), která specifikuje požadavky pro volební právo handicapovaných ve článku 29, i doporučení Rady Evropy Rec(2004)11 (Council of Europe, 2004), které konkrétně uvádí v bodě 3: "Systémy elektronického hlasování musí být navrženy, pokud je to možné, tak, aby maximalizovaly příležitosti, které tyto systémy mohou poskytnout osobám se zdravotním postižením" a v bodě 63: "Uživatelům musí být poskytnuty, kdykoli je to nutné a možné, další zařízení, jako jsou speciální rozhraní nebo jiné rovnocenné zdroje, jako je osobní asistence. Uživatelská zařízení musí co nejvíce splňovat pokyny stanovené v iniciativě Web Accessibility Initiative (WAI)." Z hlediska použitelnosti je nutné zvažovat i Zásady přístupnosti)
	Δ	U-3	Elektronické hlasovací systémy musí jasným a jednoznačným způsobem ukazovat, kdy byl hlas úspěšně sečten a proces hlasování ukončen. V tomto bodě existují precedenty pro výrazná selhání (Locher, 2015)
	Δ	U-4	Upřednostňování integrity a soukromí před použitelností. (Soukromí a integrita hlasování mají přednost před použitelností v případě konfliktu.)
	○	U-5	Intuitivní a snadné vytváření a řízení voleb pro administrátory, a to i bez specifických ICT znalostí.
Monitorování/audit	4	MA-n	Kvůli obtížnosti replikace hlasovacího procesu prostřednictvím elektronických hlasovacích systémů je nutné věnovat pozornost vývoji a implementaci monitorovacích a auditních protokolů pro celý volební proces (Puiggalí, 2009; Aceto, 2012), aby se zabránilo zainteresovaným stranám ve zneužití zranitelnosti ve svůj prospěch. Monitorování a audit zahrnuje:
	Δ	MA-1	Externí, nezávislé a distribuované. (Monitorování/audit musí zajistit nepřetržitou kontrolu nad systémem a všemi jeho zúčastněnými stranami, přičemž musí splňovat tři hlavní požadavky: být externí, nezávislý a distribuovaný, aby se minimalizovala rizika tajných dohod mezi odpovědnými stranami, jak popisují některé práce (U.S. Vote Foundation, 2015; Zissis, 2014; The Carter Center, 2014).)
		MA-2	Existence auditního protokolu od fáze návrhu. Možnost pozdější implementace se nedoporučuje.
		MA-3	Zvláštní kontrola strategií posuzování rizik a modelování hrozeb. (Nástroje pro tento účel musí také kontrolovat, zda jsou dodržovány strategie hodnocení rizik a modelování hrozeb (pokud existují), zejména v případě nehody nebo útoku.)
	Δ	MA-4	Budou generovány periodické neměnné a nesmazatelné zprávy o činnosti, které budou uchovávány v prostorách fyzicky oddělených od ostatních objektů a střeženy distribuovaným způsobem jinými pracovníky než těmi, kteří mají na starosti bezpečnost zbývajících hlasovacích činností (registrace, hlasování, přepočítání atd.).
	Δ	MA-5	Praktické provádění od registrace voličů až po povolební údržbu. (Monitoring/audit musí pokrývat všechny fáze voleb, od získání seznamu voličů až po jeho ověření, zaslání pověření, hlasování, sčítání, protokol o riziku a útoku, údržbu systému atd.)
	○	MA-6	Podrobné a dobře zdokumentované informace v příslušném formátu. (Informace musí být podrobné, dobře zdokumentované, v příslušném formátu a musí respektovat soukromí voliče.)
		MA-7	Existence „diagnostické testovací banky“ nebo v případě potřeby k dispozici test (např. v případě podezření na útok během voleb, k ověření správného fungování ochranných opatření atd.).
	Δ	MA-8	Členové monitorovacího/auditního týmu nezávislí na ostatních orgánech/správě. (Práce auditora musí být nezávislá a rozložená tak, aby žádný z nich nebyl ve vztahu k ostatním orgánům/správcům voleb ani k žádné ze stran či kandidátů účastnících se voleb.)
		MA-9	Existence protokolu pro auditování útoků a protokolu pro auditování samotného systému. (V případě vážného selhání je životně důležité auditovat útok a způsob, jakým na něj bylo reagováno. Proto musí existovat protokol pro audit rizik, chyb a útoků a další pro auditování samotného auditního systému.)
		MA-10	V případě úspěšného útoku je pro systém na prvním místě soukromí voliče a jeho hlasu, a to i za cenu, že bude muset zrušit volby. (V případě úspěšného útoku, kdy aplikace auditních protokolů znamená nutnost vzdát se některé vlastnosti systému vzdáleného elektronického hlasování, bude upřednostněno soukromí voliče a jeho hlasu, i když budou muset být volby zcela zrušeny, budou odloženy nebo se budou opakovat.)
Vývoj softwaru	8	SWD-n	
	○	SWD-1	Typické požadavky na návrh, implementaci a dokumentaci softwarového inženýrství. (Kromě obvyklých požadavků na návrh, implementaci a dokumentaci softwarového inženýrství pro jakýkoli typ programu existuje v případě vzdáleného elektronického hlasování řada bodů zvláštního zájmu:)
	Δ	SWD-2	Distribuovaný přístup k softwaru, zejména pro kritické softwarové operace. (Distribuovaný přístup bude uplatňován zejména v úlohách nastavení voleb a kritických úpravách systému. Cílem je, aby neexistovala žádná autorita, která by mohla jednostranně provádět zásadní změny.)

	Δ	SWD-3	Přestože se jedná o velmi složitý software, musí být jednoduchý na používání a musí mít uživatelskou a administrátorskou příručku, která je řádně zdokumentována a dostupná s dostatečným předstihem. Cílem je vyhnout se již dříve zmíněným problémům s použitelností (Acemyan, 2015).
	○	SWD-4	Existence dostatečně bezpečných a přístupných webových stránek s přehlednou sekci nejčastějších dotazů. (V ideálním případě by měl existovat bezpečný web s jasnou a intuitivní sekci FAQ.)
	○	SWD-5	Informace o různých politických možnostech hlasování musí být prezentovány zcela objektivním a nestranným způsobem.
	Δ	SWD-6	Hlasovací systém nesmí poskytnout voliči žádný důkaz o jeho hlasování, který by mohl být použit k vyvození zvolené možnosti.
	○	SWD-7	Systém musí zaručit soukromí hlasování ve všech krocích a neumožňovat rekonstrukci vazby mezi hlasem a voličem.
	○	SWD-8	Hlasovací proces musí být možné kdykoli zrušit bez uchování jakéhokoli typu informací o možnosti (možnostech), které byly vybrány.
	Δ	SWD-9	Software musí být testován na platformách, operačních systémech a prohlížečích, které představují více než 1 % podílu na trhu.
	Δ	SWD-10	Software nesmí umožňovat přístup prostřednictvím jakéhokoli programu třetích stran, např. sociálních médií, ani neobsahuje ani nenačítá odkazy na adresy nebo jiné programy spravované servery, které nejsou řádně kontrolovány.
	○	SWD-11	Kryptografické primitiva se testují s dostatečným předstihem za náročnějších podmínek, než budou reálné. (Co se týče kryptografických primitiv, jejich návrh a implementace musí být jasná a budou předem testována za náročnějších podmínek, než jsou vlastní volby. Navíc je to obvykle ta část kódu, která spotřebává nejvíce zdrojů, a proto je třeba co nejpřísněji ověřit (a pomocí zařízení obdobného těm, které se budou používat ve volbách), že úkoly jsou splněny v přiměřeném čase a slučitelné s běžným průběhem voleb.)
	○	SWD-12	Přístup nezávislých odborníků/vyšetřovatelů ke zdrojovému kódu za účelem kontroly (Doporučuje se, aby týmy nezávislých výzkumníků měly přístup ke zdrojovému kódu, aby jej zkontrolovaly a ověřily nepřítomnost chyb, které by mohly ohrozit bezpečnost systému. Pohled společnosti zabývajících se vývojem softwaru na zdrojový kód jako na vysoce hodnotné aktivum je pochopitelný. Existují však přijatelné možnosti, jako je povolení přístupu ke kódu nezávislým výzkumným skupinám po podepsání smlouvy NDA (dohoda o mlčenlivosti), která zajistí ochranu duševního vlastnictví společnosti a zároveň provedení nestranné kontroly softwaru.)
	○	SWD-13	Kdykoli to bude možné, budou za účelem usnadnění interoperability implementovány otevřené protokolované nebo standardizované modely.
	Δ	SWD-14	Správná aktualizace systému, zejména s ohledem na nejčastější útoky v této problematice. (Systém je nutné udržovat plně aktualizovaný, zejména proti nejběžnějším útokům na systémy elektronických voleb (man-in-the-middle, odposlech, Denial of Service, FREAK, Logjam, apod..))
	Škálovatelnost	5 E-n	Jednou z největších výzev, které elektronické hlasovací systémy čelí, je zakrýt mezeru mezi tím, co naznačuje teorie, a tím, co se děje ve skutečných volbách (Achenbach, 2015; Kocher, 1996; FREAK Attack, 2015; Beurdouche, 2017; Adrian, 2015; Witteman, 2011), což zahrnuje:
	Δ	E-1	Zásadní myšlenkou je ověřit škálovatelnost systému reálnými testy v prostředích co nejpodobnějších volbám, ve kterých bude použit.
		E-2	Existence specifických testů pro nejkritičtější operace systému. (Zvláštní pozornost by měla být věnována nejkritičtějším operacím, jako je ověřování uživatelů, šifrování a dešifrování hlasů, počítání hlasů, primitiva mix-netů atd.)
		E-3	Existence zkušebních míst náročnějších než volby, které je třeba spravovat. (Systém by měl být testován za podmínek ještě tvrdších, než je nejnáročnější použitý volební předpoklad. Den, kdy začíná volební období, nemůže být prvním okamžikem, kdy je systém vystaven této úrovni poptávky. Tento požadavek se může zdát triviální, ale někdy omezení času a zdrojů spolu s nedostatkem plánování vedou k nechtěné situaci. Tento požadavek proto posuzuje rozsah, v jakém soubor protokolů systému předvídá, počítá, podrobně popisuje a testuje limity a možnosti schématu elektronických hlasovacích systémů.)
	Δ	E-4	Musí být také jasně uvedena maximální velikost nebo složitost voleb, které systém dokáže zvládnout - ze softwarových aspektů (podle způsobu voleb, matematických a kryptografických schopností) a ex-softwaru (infrastruktura, přístup, náklady, logistika prostřednictvím druhého kanálu, lidské zdroje atd.).
	Δ	E-5	Škálovatelnost je chápána i ve smyslu schopnosti zvládnout závazné veřejné volby v politické sféře, nejsložitější a nejnáročnější.
Ex-Software Development		4 ESWD-n	Studie analyzující proběhlé volby v Estonsku, Norsku, Švýcarsku i jinde (Springall, 2014; Heiberg, 2015; The Carter Center, 2014; Koenig, 2013; Office for Democratic Institutions and Human Rights, 2016; Westfall, 2014; Wolchok, 2012) ukázaly, že neadekvátní řízení vývoje ex-softwaru, který zahrnuje protokoly a činnosti systému nesouvisající přímo se samotným volebním softwarem, může vést k velmi negativním důsledkům, které podkopávají bezpečnost a důvěru v elektronické volební systémy. Proto musí být:

		ESWD-1	Návrh, vývoj, implementace a revize protokolů ex softwaru souběžně s projektem. (Vývoj ex-software navržen, implementován a přezkoumán souběžně se software elektronického hlasovacího systému. Pouze tehdy, bude-li ex-software považován za nedílnou součást vývoje software, bude možné získat kompletní, integrovaný a dostatečně bezpečný systém pro vzdálené elektronické hlasování. Konkrétně tak musí ex-software obsahovat.)
	o	ESWD-2	Protokol pro distribuci pověření, oprávnění a odpovědností se zvláštním důrazem na zamezení tajných dohod mezi aktéry. Za tímto účelem by nemělo být povoleno shromažďování pravomocí u jedné osoby, a to zavedením politiky rozdělení odpovědností, zejména v kritických uzlech systému.
		ESWD-3	Automatizovaný protokol pro řízení přístupu a dohled nad zařízeními a infrastrukturami systému vzdáleného elektronického hlasování, s jednou nebo několika posílenými úrovněmi přístupu v závislosti na kritičnosti subsystému.
	Δ	ESWD-4	Auditní protokol a nezávislé pozorovatele. Kromě předpisů platných pro úřady musí existovat podrobný protokol pro nezávislé auditory a pozorovatele volebního procesu. Jejich práce musí mít svobodu pohybu i dohledu, pokud nenarušují bezpečnost nebo soukromí hlasování.
	Δ	ESWD-5	Zálohovací protokol. V praxi není možné dosáhnout 100 % bezpečného systému, i když je za tímto účelem navržen a implementován. Někdy jsou nedostatky a zranitelnosti odhaleny po skončení voleb, dokonce i po letech. Proto je důležité vyvinout záložní protokol. V ideálním případě by se série pravidelných záložních kopií měla vytvářet automaticky podle postupu distribuovaného mezi orgány. Následně by byly uloženy na místě, které není připojeno k hlasovacímu systému a je izolováno od zbytku zařízení.
	Δ	ESWD-6	Soubor protokolů a úkonů se musí řídit zásadou rozdělení pravomocí a odpovědností, aby se zabránilo jejich koncentraci v jedné osobě nebo skupině příbuzných osob. Riziko tajné dohody mezi stranami musí být vždy zvažováno.
	Δ	ESWD-7	Existence volebních systémů doplňujících hlasovací systém.
	Δ	ESWD-8	Voliči musí být informováni s dostatečným předstihem a prostředky o konkrétním způsobu, jakým to bude formulováno ve volebním systému, a mají být zpřístupněny kanály pro vyřešení pochybností a získání zpětné vazby.
		ESWD-9	O možnosti opakovaného hlasování budou voliči informováni v dostatečném předstihu, pokud možnost existuje, s uvedením postupu a předností papírového hlasování před elektronickým v případě konfliktu.
		ESWD-10	Organizování názorových a technických průzkumů u vybraných kohort profilů voličů s cílem získat co nejspolehlivější zpětnou vazbu o trendech, použitelnosti, chybách a budoucích zlepšeních.
	Δ	ESWD-11	Zasílání ověřovacích pověření alternativními kanály. (Odeslání autentizačních údajů bude probíhat prostřednictvím dvou různých kanálů, aby se posílila bezpečnost.)
		ESWD-12	Existence hlavního inicializačního protokolu, který má být spuštěn bezprostředně před zahájením. (Bezprostředně před začátkem období elektronických voleb musí existovat inicializační protokol, který bude zahrnovat závěrečný test správné funkce hlasovací infrastruktury a prostředků.)
		ESWD-13	Kdykoliv to bude možné, budou implementovány protokolované nebo standardizované systémy, aby se usnadnila vzájemná interoperabilita.
		ESWD-14	Existence bezplatné telefonické asistenční služby před zahájením voleb a během nich bude zhodnocena.
	Δ	ESWD-15	Budou zohledněny veškeré aktivity realizované za účelem propagace systému vzdáleného elektronického hlasování, stejně jako kontaktní dny otevřených dveří a webináře za účelem školení obyvatel v jeho správu.
Protokoly incidentů a útoků	4	IAP-n	Zkušenosti ukazují, že závazné volební procesy využívající systémy vzdáleného elektronického hlasování jsou pravidelně vystaveny útokům (U.S. Vote Foundation, 2015; Wolchok, 2012; Springall, 2014; Halderman, 2015; Tsoukalas, 2013). Mezi zeměmi, které se staly oběťmi, se nacházejí Spojené státy americké, Austrálie nebo Ukrajina (Clayton, 2014). V rostoucím pokroku a složitosti útoků bylo dosaženo bodu, kdy existují společnosti a hackeři specializující se na prodej nástrojů připravených zaútočit na zranitelná místa v prohlížeči, operačním systému nebo programu, který je vybrán jako „útok a la carte“ na konkrétní datum (Greenberg, 2012). Proto je nezbytné, aby systém pro elektronické hlasování byl vyvíjen se zřetel na dosavadních útocích a navrhl a implementoval aktualizované bezpečnostní protokoly až do okamžiku voleb. To nezaručuje, že je systém imunní, ale představuje to minimální požadavek v prostředí se skutečnou historií pokusů o útok. V této části je třeba hodnotit následující body:
		IAP-1	V ideálním případě budou vytvořeny následující dokumenty: Posouzení rizik (RA), Posouzení dopadu na soukromí (PIAS), Penetrační testování (PT), Prohlášení o použitelnosti (SoA), Plán validace kontrol (CVP) a Audit validace kontrol (CVA).
		IAP-2	Existence specifických protokolů proti útokům a politika prevence založená na systémovém schématu elektronického systému pro vzdálené hlasování (např. specifické protokoly proti útokům typu DDoS v řešených využívajících mix-nety).

	Δ	IAP-3	Informace a infrastruktury jsou v co největší míře uchovávány na území, kde se konají volby. (Doporučuje se, aby veškeré informace a infrastruktura byly v zemi, kde se volby konají, kromě nezbytně nutné části související s hlasováním občanů pobývajících v zahraničí.)
		IAP-4	Budou implementovány protokoly, které zaručí netrvalou ztrátu informací v případě útoku s redundancí zařízení a systémů.
	Δ	IAP-5	Distribuovaný přístup antiútočného protokolu, takže k deaktivaci systému vzdáleného hlasování nestačí zaútočit na jediný zdroj/místo.
	Δ	IAP-6	Akce pro zvýšení povědomí občanů. Je důležité, aby voliči byli vzdělaní a byli si vědomi útoků, jichž jsou cílem (phishing, sociální inženýrství atd.).
	Δ	IAP-7	Najímání hackerů a nezávislých odborníků, aby otestovali systém před jeho nasazením ve skutečných volbách.
Všestrannost	6	V-n	Z hlediska vývoje systému pro elektronické volby představuje rozmanitost hlasování dle možnosti výběru obrovský rozdíl. Systém, který má několik verzí upravených podle typologie hlasování, bude mít větší všestrannost.
	Δ	V-1	Verze upravené podle typologie hlasování budou mít větší všestrannost a budou v této sekci bodovány lépe.
		V-2	Existence specifických řešení pro nejzranitelnější skupiny. (Všestrannost systému souvisí také s použitelností. Jednou z hlavních motivací pro volbu elektronického hlasování na dálku je umožnit skupinám populace s určitým typem omezení s tradičním volebním systémem (zrakové nebo sluchové postižení, problémy s pohyblivostí, pokročilý věk atd.) uplatnit své volební právo jednodušším a přizpůsobenějším způsobem. Bude proto oceněno, že systém elektronického hlasování na dálku nabízí řešení speciálně navržená pro tyto skupiny. Další aspekty, které je třeba vzít v úvahu, jsou:)
	o	V-3	Volič musí mít možnost hlasovat pomocí svého osobního vybavení, s konvenčním připojením k internetu a bez instalace dalšího softwaru.
	Δ	V-4	Systém musí být vyvinut a testován na prohlížečích a zařízeních, které jsou využívány u více než 1 % celkového počtu voličů.
	Δ	V-5	Rozhraní by mělo splňovat požadavky WCAG 2.0 AA.
Nákladovost	10	C-n	Nákladový aspekt systému je i s ohledem na mlčenlivost špatně dokumentován i přesto, že cena je důležitým parametrem při výběru řešení. Požadovaná cena nebývá zahrnuta mezi tradiční požadavky na elektronické volební systémy, přesto elektronické hlasování má svůj rozpočet stejně jako jiné projekty, proto je vhodné zvážit i nákladovost. Je také známo, že největší společnosti v tomto odvětví nabízejí různé úrovně zabezpečení softwaru v závislosti na typu výběru a dostupném rozpočtu. Čím větší bezpečnost a komplexnost, tím vyšší cena produktu. Toto kritérium proto oceňuje:
	o	C-1	Transparentnost a srozumitelnost prezentace nákladů na implementaci systému pro vzdálené elektronické hlasování (buď v celkových hodnotách nebo v nákladech na jednoho voliče).
	o	C-2	Náklady na systém ve vztahu k jeho kvalitě, výkonu a srovnání s alternativními možnostmi. (Cenu, kdy při stejné úrovni zabezpečení bude v této sekci logicky lépe ohodnocen ekonomičtější systém.)
Údržba	6	M-n	Údržba je často ve vědeckých článcích ignorována, ačkoli ve skutečných projektech je velmi důležitá, jak lze mimo jiné vidět v případě Austrálie (Halderman, 2015). Údržba je chápána ze dvou hledisek:
	Δ	M-1	Ve vztahu k samotnému systému (jak software, tak ex-software). Tedy jak je systém aktuální, a tedy jak je zabezpečený proti nejnovějším odhalovaným útokům. Čím častější a důslednější aktualizace systému, tím lepší bude skóre v této sekci. Existence nemodifikovatelného logu přístupného pouze oprávněným agentům se doporučuje proto, aby vždy byla informace o stavu aktualizace každé součásti systému. Tento aspekt je velmi důležitý, protože úkoly údržby jsou někdy ve více akademických systémech opuštěny i na roky, jako v případě Helios Voting (Adida, 2008).
		M-2	Údržba jako věčné soukromí. (Existence protokolu pro uchování a zálohování dat pro volby za dostatečně solidních bezpečnostních podmínek, aby bylo zaručeno soukromí hlasů a voličů i v budoucnu, kdy by mohli získat nové schopnosti protivníci, kteří chtějí ohrožit systém. Cílem je tzv. „věčné soukromí“ (Locher, 2015; Arapinis, 2013; Moran, 2006). Požadavek na zachování elektronického hlasování na dálku nabývá zvláštního významu, protože může nastat situace, že po skončení voleb bude odhalen útok. To nutně znamená zachování výsledků voleb a hlasování (i když jsou zašifrovány a zbařeny spojení s voličem) na rozdíl od tradičních voleb, ve kterých jsou po určité době hlasovací lístky zničeny.)
	Δ	M-3	Náklady spojené s údržbou.
(H - hodnocení)			

Reference:

- ACEMYAN, Claudia Z., Philip KORTUM, Michael D. BYRNE a Dan S. WALLACH, 2015. From Error to Error: Why Voters Could not Cast a Ballot and Verify Their Vote With Helios, Prêt à Voter, and Scantegrity II. In: *USENIX Journal of Election Technology and Systems (JETS)* 3 [online]. s. 1-25 [cit. 2023-10-12]. Dostupné z: <https://www.usenix.org/jets/issues/0302/acemyan>
- ACETO, I. Jay, Michelle M SHAFER, Edwin B SMITH III, a Cyrus J WALKER, 2012. Internet voting system security auditing from system development through implementation: Best practices from electronic voting deployments: Best practices from electronic voting deployments. In: 5th International Conference on Electronic Voting 2012 (EVOTE2012) [online]. Gesellschaft für Informatik eV [cit. 2024-09-24]. ISBN 3885792990. Dostupné z: <https://subs.emis.de/LNI/Proceedings/Proceedings205/145.pdf>
- ACHENBACH, Dirk, Carmen KEMPKA, Bernhard LÖWE a Jörn MÜLLER-QUADE, 2015. Improved coercion-resistant electronic elections through deniable re-voting. *{USENIX} Journal of Election Technology and Systems (JETS)* [online]. 3, 26-45 [cit. 2024-09-24]. ISSN 2328-2797. Dostupné z: https://www.usenix.org/system/files/conference/jets15/jets_0302-achenbach.pdf
- ADIDA, Ben, 2008. Helios: Web-based Open-Audit Voting. In: *USENIX security symposium* [online]. Vol. 17. s. 335-348 [cit. 2023-10-12]. Dostupné z: https://www.usenix.org/legacy/event/sec08/tech/full_papers/adida/adida.pdf
- ADRIAN, David, Karthikeyan BHARGAVAN, Zakir DURUMERIC, et al., 2015. Imperfect Forward Secrecy. In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* [online]. New York, NY, USA: ACM, 2015-10-12, s. 5-17 [cit. 2023-12-19]. ISBN 9781450338325. Dostupné z: doi:10.1145/2810103.2813707
- ARAPINIS, Myrto, Véronique CORTIER, Steve KREMER a Mark RYAN, 2013. Practical Everlasting Privacy. In: BASIN, David a John C. MITCHELL, ed. *Principles of Security and Trust* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 21-40 [cit. 2023-12-29]. *Lecture Notes in Computer Science*. ISBN 978-3-642-36829-5. Dostupné z: doi:10.1007/978-3-642-36830-1_2
- BENALOH, Josh, 2006. Simple Verifiable Elections. *USENIX Association*. Dostupné také z: <https://www.usenix.org/conference/evt-06/simple-verifiable-elections>
- BENALOH, Josh, Ronald RIVEST, Peter YA RYAN, Philip STARK, Vanessa TEAGUE a Poorvi VORA, 2015. End-to-end verifiability. *ArXiv preprint arXiv:1504.03778* [online]. [cit. 2024-09-24]. Dostupné z: doi:10.48550/arXiv.1504.03778
- BEURDOUCHE, Benjamin, Karthikeyan BHARGAVAN, Antoine DELIGNAT-LAUDAUD, Cédric FOURNET, Markulf KOHLWEISS, Alfredo PIRONTI, Pierre-Yves STRUB a Jean Karim ZINZINDOHOU, 2017. A messy state of the union. *Communications of the ACM* [online]. 2017-01-23, 60(2), 99-107 [cit. 2023-12-27]. ISSN 0001-0782. Dostupné z: doi:10.1145/3023357
- CASTELLÓ, Sandra Guasch, 2016. Individual Verifiability in Electronic Voting. In: *Universitat Politècnica de Catalunya* [online]. [cit. 2023-10-12]. Dostupné z: <https://upcommons.upc.edu/bitstream/handle/2117/96245/TSGC1de1.pdf>
- CHAUM, David, 2004. Secret-ballot receipts: true voter-verifiable elections. *IEEE Security & Privacy Magazine* [online]. 2(1), 38-47 [cit. 2023-12-22]. ISSN 1540-7993. Dostupné z: doi:10.1109/MSECP.2004.1264852
- CLAYTON, Mark, 2014. Ukraine election narrowly avoided 'wanton destruction' from hackers. *The Christian Science Monitor* [online]. [cit. 2023-12-29]. Dostupné z: <https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers>
- COUNCIL OF EUROPE, 2004. Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. *Brussels: Council of Europe, Committee of Ministers*, [online]. [cit. 2023-11-14]. Dostupné z: [https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/00Rec\(2004\)11_rec_adopted_en.asp](https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/00Rec(2004)11_rec_adopted_en.asp)
- FREAK ATTACK, 2015. Tracking the FREAK Attack [online]. [cit. 2023-10-12]. Dostupné z: <https://freakattack.com/>
- GREENBERG, Andy, 2012. Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits. *Forbes* [online]. [cit. 2023-12-29]. Dostupné z: <https://www.forbes.com/sites/andyygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/>
- HALDERMAN, J. Alex a Vanessa TEAGUE, 2015. The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. In: *ArXiv.org* [online]. [cit. 2023-12-29]. Dostupné z: doi:10.48550/arXiv.1504.05646
- HEIBERG, Sven, Arnis PARSOVS a Jan WILLEMSON, 2015. Log Analysis of Estonian Internet Voting 2013–2015 [online]. 2015-08-13 [cit. 2024-01-05]. *Lecture Notes in Computer Science*. Dostupné z: <https://eprint.iacr.org/2015/1211>
- JONKER, Hugo, Sjouke MAUW a Jun PANG, 2013. Privacy and verifiability in voting systems: Methods, developments and trends: Methods, developments and trends. *Computer Science Review* [online]. Elsevier, 10, 1-30 [cit. 2024-09-24]. ISSN 1574-0137. Dostupné z: <https://eprint.iacr.org/2013/615.pdf>
- KOCHER, Paul C., 1996. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: KOBLITZ, Neal, ed. *Advances in Cryptology — CRYPTO '96* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 104-113 [cit. 2023-12-27]. *Lecture Notes in Computer Science*. ISBN 978-3-540-61512-5. Dostupné z: doi:10.1007/3-540-68697-5_9
- KOENIG, Reto E., Philipp LOCHER a Rolf HAENNI, 2013. Attacking the Verification Code Mechanism in the Norwegian Internet Voting System. In: HEATHER, James, Steve SCHNEIDER a Vanessa TEAGUE, ed. *E-Voting and Identify* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 76-92 [cit. 2023-12-29]. *Lecture Notes in Computer Science*. ISBN 978-3-642-39184-2. Dostupné z: doi:10.1007/978-3-642-39185-9_5
- KREMER, Steve, Mark RYAN a Ben SMYTH, 2010. Election Verifiability in Electronic Voting Protocols. In: GRITZALIS, Dimitris, Bart PRENEEL a Marianthi THEOHARIDOU, ed. *Computer Security – ESORICS 2010* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 389-404 [cit. 2024-06-23]. *Lecture Notes in Computer Science*. ISBN 978-3-642-15496-6. Dostupné z: doi:10.1007/978-3-642-15497-3_24
- LI, Huian, Abhishek Reddy KANKANALA a Xukai ZOU, 2014. A taxonomy and comparison of remote voting schemes. In: 2014 23rd International Conference on Computer Communication and Networks (ICCCN) [online]. IEEE, s. 1-8 [cit. 2023-12-27]. ISBN 978-1-4799-3572-7. Dostupné z: doi:10.1109/ICCCN.2014.6911807
- LOCHER, Philipp a Rolf HAENNI, 2015. Verifiable Internet Elections with Everlasting Privacy and Minimal Trust. In: *E-Voting and Identity* [online]. Cham: Springer International Publishing, 2015-08-13, s. 74-91 [cit. 2023-12-27]. *Lecture Notes in Computer Science*. ISBN 978-3-319-22269-1. Dostupné z: doi:10.1007/978-3-319-22270-7_5
- MARCOS DEL BLANCO, David Yeregui, 2018. Cybersecurity applied to e-democracy: Cryptographic analysis and development of a Practical Evaluation Methodology for i-voting systems and its application to the most relevant solutions. *Universidad de León*.
- MORAN, Tal a Moni NAOR, 2006. Receipt-Free Universally-Verifiable Voting with Everlasting Privacy. In: DWORK, Cynthia, ed. *Advances in Cryptology - CRYPTO 2006* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 373-392 [cit. 2023-12-29]. *Lecture Notes in Computer Science*. ISBN 978-3-540-37432-9. Dostupné z: doi:10.1007/11818175_22
- OFFICE FOR DEMOCRATIC INSTITUTIONS AND HUMAN RIGHTS, 2016. Swiss Confederation: Federal Assembly Elections. 18 October 2015. Final Report [online]. Varšava [cit. 2023-12-29]. Dostupné z: <https://www.osce.org/files/f/documents/8/e/222556.pdf>
- PUIGGALLÍ, Jordi, Jesús CHÓLIZ a Sandra GUASCH, 2009. Best Practices in Internet Voting. In: *ScytI Secure Electronic Voting* [online]. [cit. 2023-12-27]. Dostupné z: https://csrc.nist.gov/csrc/media/events/workshop-on-uocava-remote-voting-systems/documents/papers/puiggalli_bestpracticesinternetworking.pdf
- SPRINGALL, Drew, Travis FINKENAUER, Zakir DURUMERIC, Jason KITCAT, Harri HURSTI, Margaret MACALPINE a J. Alex HALDERMAN, 2014. Security Analysis of the Estonian Internet Voting System. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* [online]. New York, NY, USA: ACM, 2014-11-03, s. 703-715 [cit. 2023-02-17]. ISBN 9781450329576. Dostupné z: doi:10.1145/2660267.2660315
- THE CARTER CENTER, 2014. Summary: Expert Study Mission Report The Carter Center Internet Voting Pilot : Norway's 2013 Parliamentary Elections [online]. [cit. 2023-10-12]. Dostupné z: https://www.regjeringen.no/globalassets/upload/krd/kampanjer/valgportal/valgobservatorer/2013/rapport_cartersenteret2013.pdf
- TSOUKALAS, Georgios, Kostas PAPADIMITRIOU a Panos LOURIDAS, 2013. From helios to zeus. *USENIX Journal of Election Technology and Systems (JETS)* [online]. 1(1), 1-17 [cit. 2024-09-24]. ISSN 2328-2797. Dostupné z: <https://www.usenix.org/system/files/jets/issues/jets-0101-tsoukalas.pdf>
- U.S. VOTE FOUNDATION, 2015. E2E-VIV Project: The Future of Voting: End-to-End Verifiable Internet Voting - Specification and Feasibility Study. In: *U.S. Vote Foundation* [online]. [cit. 2023-10-16]. Dostupné z: <https://www.usvotefoundation.org/E2E-VIV>
- WESTFALL, Brittany, 2014. Internet Voting. West Virginia Secretary of State's Office [online]. [cit. 2023-12-29]. Dostupné z: <https://bowencenterforpublicaffairs.org/wp-content/uploads/2014/06/Internet-Voting-West-Virginia.pdf>
- WITTEMAN, Marc E, Jasper G. J. VAN WOUDEMBERG a Federico MENARINI, 2011. Defeating RSA Multiply-Always and Message Blinding Countermeasures. In: KIAYIAS, Angelos, ed. *Topics in Cryptology – CT-RSA 2011* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 77-88 [cit. 2023-12-27]. *Lecture Notes in Computer Science*. ISBN 978-3-642-19073-5. Dostupné z: doi:10.1007/978-3-642-19074-2_6
- WOLCHOK, Scott, Eric WUSTROW, Dawn ISABEL a J. Alex HALDERMAN, 2012. Attacking the Washington, D.C. Internet Voting System. In: KEROMYTIS, Angelos D., ed. *Financial Cryptography and Data Security* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 114-128 [cit. 2023-12-29]. *Lecture Notes in Computer Science*. ISBN 978-3-642-32945-6. Dostupné z: doi:10.1007/978-3-642-32946-3_10
- ZISSIS, Dimitrios a Dimitrios LEKKAS, 2014. Design, Development, and Use of Secure Electronic Voting Systems. In: *Advances in Electronic Government, Digital Divide, and Regional Development* [online]. IGI Global [cit. 2023-10-13]. ISSN 2326-9103. Dostupné z: doi:10.4018/978-1-4666-5820-2.ch004

Příloha B: Komparace software pro tajnou vzdálenou elektronickou volbu

V této příloze je provedeno vyhodnocení několika vybraných softwarů pro vzdálenou elektronickou volbu prostřednictvím dříve publikovaných článků (Marcos del Blanco, 2019; Marcos del Blanco, 2020) a vlastního hodnocení systému Belenios.

V příloze je provedena komparace oficiální verze systému Helios Voting (Helios Voting, 2023), systému nVotes od Agora Voting SL a systému iVote vyvinutého společností ScytL SA (ScytL, 2023). Novější verze Helios, jako je KTV-Helios (Kulyk, 2015), ještě nebyly plně nasazeny v závazných volbách, proto nejsou předmětem hodnocení (Marcos del Blanco, 2019).

Helios Voting

Systém Helios Voting je podrobně popisován v publikovaném článku (Martínek, 2024a) a dalších pracích (Adida, 2008; Adida, 2009), je používán i mezinárodní kryptografickou asociací (Haber, 2010). Kryptografie systému byla prozkoumána v mnoha odborných publikacích (Bernhard, 2012; Cortier, 2013; Kulyk, 2015; Cortier, 2014). Použitelnost systému Helios hodnotil Acemyan (2015).

Belenios

Francouzský systém Belenios vychází ze systému Helios Voting a je podrobněji popisován v článku (Martínek, 2024b). Autoři ho sami popisují v mnoha odborných článcích (Cortier, 2018; Cortier, 2019a; Baloglu 2021a; Baloglu 2021b; Glondou, 2023)

ScytL iVote

ScytL je celosvětově uznávaná společnost, která se specializuje na volební řešení. Má sídlo v Barceloně a byla založena v roce 2001. Zaměstnává více než 250 lidí. Společnost má zkušenosti s organizováním více než 100 000 volebních akcí ve více než 20 zemích. Vlastní přes 40 mezinárodních patentů v oblasti bezpečnosti volebních procesů. ScytL přizpůsobuje svůj nástroj iVote specifickým požadavkům každé země, a to jak z hlediska návrhu, tak i kryptografické bezpečnosti, podle příslušné jurisdikce a typu voleb. Při hodnocení je vždy brána v úvahu nejvýkonnější verze iVote pro každou konkrétní položku (Marcos del Blanco, 2019).

nVotes

nVotes je vzdálený systém elektronického hlasování, který vyvinula španělská společnost Agora Voting SL v roce 2014. Tento systém má své kořeny již v roce 2009 a je spojen s Internet Party, avšak vývojářský tým se od té doby distancoval

od jakékoliv politické příslušnosti a nyní je nVotes apolitickým komerčním projektem (Marcos del Blanco, 2020).

Další systémy

Existují další elektronické volební systémy, které již v rámci této přílohy nehodnotíme. Mezi ně patří například Civitas, který pro zvýšení odolnosti nátlaku využívá falešné přihlašovací údaje (Clarkson, 2007; Clarkson, 2008).

Výsledná evaluace volebních software

Výsledné bodové hodnocení je založeno na odborných článcích (Marcos del Blanco, 2019; Marcos del Blanco, 2020), kde proběhla evaluace systému Helios Voting, iVote, nVotes, a na základě vlastního hodnocení systému Belenios, které je v příloze A, v článku (Martínek, 2024b) i ve slovním hodnocení v této příloze. Výsledky lze shrnout takto:

Požadavek	Kód	Váha	Helios	Belenios	iVote	nVotes
E2Ev	E2Ev	-	Δ	Δ	Δ	Δ
Odolnost nátlaku	CR	-	X	X	X	X
Nedotknutelnost	(I-n)	1,2	$6 * 1,2 = 7,2$	$6,5 * 1,2 = 7,7$	$8 * 1,2 = 9,6$	$4 * 1,2 = 4,8$
Použitelnost	(U-n)	0,8	$4 * 0,8 = 3,2$	$6 * 0,8 = 4,8$	$7,5 * 0,8 = 6$	$6 * 0,8 = 4,8$
Monitoring a audit	(MA-n)	1,2	$4 * 1,2 = 4,8$	$4 * 1,2 = 4,8$	$8,5 * 1,2 = 10,2$	$3 * 1,2 = 3,6$
Vývoj software	(SWD-n)	1,2	$7,5 * 1,2 = 9$	$8 * 1,2 = 9,6$	$8,5 * 1,2 = 10,2$	$7 * 1,2 = 8,4$
Škálovatelnost	(S-n)	0,8	$4 * 0,8 = 3,2$	$5 * 0,8 = 4$	$9,5 * 0,8 = 7,6$	$5,5 * 0,8 = 4,4$
Ex-Software Development	(ESWD-n)	1,2	$3 * 1,2 = 3,6$	$4 * 1,2 = 4,8$	$9 * 1,2 = 10,8$	$4 * 1,2 = 4,8$
Protokoly incidentů a útoků	(IAP-n)	1,2	$4 * 1,2 = 4,8$	$4 * 1,2 = 4,8$	$8 * 1,2 = 9,6$	$4 * 1,2 = 4,8$
Všestrannost	(V-n)	0,6	$4 * 0,6 = 2,4$	$6 * 0,6 = 2,4$	$8 * 0,6 = 4,8$	$5 * 0,6 = 3$
Nákladovost	(C-n)	1,0	$9 * 1 = 9$	$10 * 1 = 10$	$7 * 1,0 = 7$	$7 * 1,0 = 7$
Údržba	(M-n)	0,8	$5 * 0,8 = 4$	$6 * 0,8 = 4,8$	$8,5 * 0,8 = 6,8$	$6,5 * 0,8 = 5,2$
Celkem		10	51,2	57,7	82,6	50,8

Tabulka B1: Vyhodnocení bodování systémů Helios, Belenios, iVote a nVotes

Podrobné vyhodnocení systémů Helios Voting, iVote a nVotes lze najít v článcích (Marcos del Blanco, 2019; Marcos del Blanco, 2020), vyhodnocení systému Belenios lze shrnout:

Vlastní instalace systému Belenios umožňuje autentizaci prostřednictvím vlastního CAS, což eliminuje potřebu přihlášení přes systémy třetích stran. U vlastní instalace je možné provádět úpravy a přizpůsobení volebního procesu, což může zlepšit jeho použitelnost. Pro menší volby představuje dobrý kompromis mezi náklady a výkonem. Kvalitní metodika volebního procesu může splňovat mnoho požadavků na monitorování a audit.

Belenios podporuje vlastní instalaci, což umožňuje uchování dat v zemi a vlastní validaci a testování postupů. Aktivní akademická komunita neustále vyvíjí a zdokonaluje systém Belenios. Vlastní instalace může být upravena podle konkrétních potřeb a přístup může být omezen na vlastní server CAS, bez použití kódů třetích stran. Na rozdíl od systému Helios umožňuje Belenios různé typy voleb, včetně alternativních systémů.

Oficiální instalace omezuje počet voličů v jedné volbě na 2500, zatímco vlastní instalace může podporovat i rozsáhlejší volby. Vlastní metodický postup umožňuje splnění specifických požadavků a distribuci přístupových klíčů vlastním systémem. Provoz udržovaného systému je ekonomicky výhodný, přičemž oficiální instalace je zdarma a obsahuje veřejně dostupné návody. Vývoj a údržba systému Belenios těží z práce aktivní akademické komunity, která i přes omezené finanční zdroje dokáže udržovat systém na kvalitativní úrovni.

Vlastní hodnocení systému Belenios autorem práce přináší 57,7 bodů a s výrazným odstupem druhé místo. To značí, že lze systém využít pro méně významné volby malého rozsahu, ale není připraven pro plnohodnotné nasazení v závazných politických volbách velkého rozsahu. Zlepšit vlastnosti by mohl systém BeleniosRF (Chaidos, 2016) nebo BeleniosVS (Cortier, 2019b). Nově představený protokol BeleniosCal by měl zlepšit univerzální ověřitelnost, i když by to bylo na úkor použitelnosti (Cortier, 2024).

Reference

- ACEMYAN, Claudia Z., Philip KORTUM, Michael D. BYRNE a Dan S. WALLACH, 2015. From Error to Error: Why Voters Could not Cast a Ballot and Verify Their Vote With Helios, Prêt à Voter, and Scantegrity II. In: USENIX Journal of Election Technology and Systems (JETS) 3 [online]. s. 1-25 [cit. 2023-10-12]. Dostupné z: <https://www.usenix.org/jets/issues/0302/acemyan>
- ADIDA, Ben, 2008. Helios: Web-based Open-Audit Voting. In: USENIX security symposium [online]. Vol. 17. s. 335-348 [cit. 2023-10-12]. Dostupné z: https://www.usenix.org/legacy/event/sec08/tech/full_papers/adida/adida.pdf
- ADIDA, Ben, Olivier DE MARNEFFE, Olivier PEREIRA a Jean-Jacques QUISQUATER, 2009. Electing a University President using Open-Audit Voting: Analysis of real-world use of Helios. In: Proceedings of the 2009 Conference on Electronic Voting Technology/Workshop on Trustworthy Elections [online]. EVT/WOTE [cit.

2023-10-12].

Dostupné

z:

https://www.usenix.org/legacy/event/evtwote09/tech/full_papers/adida-helios.pdf

- BALOGLU, Sevdenur, Sergiu BURSUC, Sjouke MAUW a Jun PANG, 2021a. Election Verifiability Revisited: Automated Security Proofs and Attacks on Helios and Belenios. 2021 IEEE 34th Computer Security Foundations Symposium (CSF) [online]. IEEE, 1-15 [cit. 2023-03-17]. ISBN 978-1-7281-7607-9. Dostupné z: doi:10.1109/CSF51468.2021.00019
- BALOGLU, Sevdenur, Sergiu BURSUC, Sjouke MAUW a Jun PANG, 2021b. Provably Improving Election Verifiability in Belenios. In: KRIMMER, Robert, Melanie VOLKAMER, David DUENAS-CID, Oksana KULYK, Peter RØNNE, Mihkel SOLVAK a Micha GERMANN, ed. Electronic Voting [online]. 12900. Cham: Springer International Publishing, s. 1-16 [cit. 2023-02-17]. Lecture Notes in Computer Science. ISBN 978-3-030-86941-0. Dostupné z: doi:10.1007/978-3-030-86942-7_1
- BERNHARD, David, Olivier PEREIRA a Bogdan WARINSCHI, 2012. How Not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios. In: Advances in Cryptology – ASIACRYPT 2012 [online]. Berlin, Heidelberg: Springer, s. 626-643 [cit. 2023-10-12]. Lecture Notes in Computer Science. ISBN 978-3-642-34960-7. Dostupné z: doi:10.1007/978-3-642-34961-4_38
- CLARKSON, Michael, Stephen CHONG a Andrew MYERS, 2007. Civitas. Cornell.edu [online]. [cit. 2023-12-30]. Dostupné z: <https://www.cs.cornell.edu/Projects/civitas/>
- CLARKSON, Michael R, Stephen CHONG a Andrew C. MYERS, 2008. Civitas: Toward a Secure Voting System. In: 2008 IEEE Symposium on Security and Privacy (sp 2008) [online]. IEEE, s. 354-368 [cit. 2024-07-02]. ISBN 978-0-7695-3168-7. ISSN 1081-6011. Dostupné z: doi:10.1109/SP.2008.32
- CORTIER, Veronique, Constantin Catalin DRAGAN, Francois DUPRESSOIR a Bogdan WARINSCHI, 2018. Machine-Checked Proofs for Electronic Voting: Privacy and Verifiability for Belenios. In: 2018 IEEE 31st Computer Security Foundations Symposium (CSF) [online]. Oxford, UK: IEEE, s. 298-312 [cit. 2023-03-17]. ISBN 978-1-5386-6680-7. ISSN 2374-8303. Dostupné z: doi:10.1109/CSF.2018.00029
- CORTIER, Véronique, David GALINDO, Stéphane GLONDU a Malika IZABACHÈNE, 2014. Election Verifiability for Helios under Weaker Trust Assumptions. In: Computer Security - ESORICS 2014 [online]. SpringerLink [cit. 2023-10-12]. Dostupné z: doi:10.1007/978-3-319-11212-1_19
- CORTIER, Véronique, Pierrick GAUDRY a Stéphane GLONDU, 2019a. Belenios: A Simple Private and Verifiable Electronic Voting System. In: GUTTMAN, Joshua D, Carl E. LANDWEHR, José MESEGUER a Dusko PAVLOVIC, ed. Foundations of Security, Protocols, and Equational Reasoning, Lecture Notes in Computer Science [online]. 11565. Cham: Springer International Publishing, 2019-04-28, s. 214-238 [cit. 2023-03-17]. Lecture Notes in Computer Science. ISBN 978-3-030-19052-1. Dostupné z: doi:10.1007/978-3-030-19052-1_14
- CORTIER, Veronique, Alicia FILIPIAK a Joseph LALLEMAND, 2019b. BeleniosVS: Secrecy and Verifiability Against a Corrupted Voting Device. In: 2019 IEEE 32nd Computer Security Foundations Symposium (CSF) [online]. Hoboken, NJ, USA: IEEE, s. 367-36714 [cit. 2023-03-17]. ISBN 978-1-7281-1407-1. Dostupné z: doi:10.1109/CSF.2019.00032
- CORTIER, Véronique a Ben SMYTH, 2013. Attacking and fixing Helios: An analysis of ballot secrecy. In: Journal of Computer Security [online]. [cit. 2023-10-12]. Dostupné z: <https://dl.acm.org/doi/10.5555/2595846.2595849>
- CORTIER, Véronique, Alexandre DEBANT, Pierrick GAUDRY a Stéphane GLONDU, 2024. Belenios with Cast as Intended. In: ESSEX, Aleksander, Shin'ichiro MATSUO, Oksana KULYK, et al., ed. Financial Cryptography and Data Security. FC 2023 International Workshops [online]. Cham: Springer Nature Switzerland, s. 3-18 [cit. 2024-10-04]. Lecture Notes in Computer Science. ISBN 978-3-031-48805-4. Dostupné z: doi:10.1007/978-3-031-48806-1_1

- GLONDU, Stéphane, 2023. Belenios specification: Version 2.1 [online]. France [cit. 2023-04-08]. Dostupné z: <https://www.belenios.org/specification.pdf>
- HABER, Stuart, Josh BENALOH a Shai HALEVI, 2010. The Helios e-Voting Demo for the IACR [online]. International association for cryptologic research [cit. 2023-10-12]. Dostupné z: <https://www.iacr.org/elections/eVoting/heliosDemo.pdf>
- HELIOS VOTING, 2023. Helios Voting [online]. [cit. 2023-10-12]. Dostupné z: <https://vote.heliosvoting.org/>
- CHAIIDOS, Pyrros, Véronique CORTIER, Georg FUCHSBAUER a David GALINDO, 2016. BeleniosRF: A Non-interactive Receipt-Free Electronic Voting Scheme. In: ACM Conferences [online]. CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. s. 1614-1625 [cit. 2023-10-18]. Dostupné z: doi:10.1145/2976749.2978337
- KULYK, Oksana, Vanessa TEAGUE a Melanie VOLKAMER, 2015. Extending helios towards private eligibility verifiability. In: E-Voting and Identity: 5th International Conference, VoteID 2015, September 2-4. Proceedings 5. Bern, Switzerland: Springer International Publishing, s. 57-73.
- MARCOS DEL BLANCO, David Yeregui, David DUENAS-CID a Héctor ALÁIZ MORETÓN, 2020. E-Voting System Evaluation Based on the Council of Europe Recommendations: nVotes. In: KRIMMER, Robert, Melanie VOLKAMER, Bernhard BECKERT, Ralf KÜSTERS, Oksana KULYK, David DUENAS-CID a Mihkel SOLVAK, ed. Electronic Voting [online]. Cham: Springer International Publishing, s. 147-166 [cit. 2023-02-17]. Lecture Notes in Computer Science. ISBN 978-3-030-60346-5. Dostupné z: doi:10.1007/978-3-030-60347-2_10
- MARCOS DEL BLANCO, D. Y. a M. GASCÓ, 2019. A Protocolized, Comparative Study of Helios Voting and Scytl/iVote. In: 2019 Sixth International Conference on eDemocracy & eGovernment (ICEDEG) [online]. Quito, Ecuador: IEEE, s. 31-38 [cit. 2024-09-25]. ISBN 978-1-7281-1704-1. ISSN 2573-1998. Dostupné z: doi:10.1109/ICEDEG.2019.8734351
- MARTÍNEK, Tomáš a Michal MALÝ, 2024a. Evaluation of the I-Voting System for Remote Primary Elections of the Czech Pirate Party. Acta Informatica Pragensia [online]. 13(3), 395-417 [cit. 2024-07-28]. ISSN 1805-4951. Dostupné z: doi:10.18267/j.aip.249
- MARTÍNEK, Tomáš, Martin PELIKÁN, Jan TYRYCHTR a Jakub KONOPÁSEK, 2024b. Implementation of a Secret and Verifiable Personal Remote Electronic Election of an Agrarian Organization per the Recommendation of the Council of Europe. AGRIS on-line Papers in Economics and Informatics [online]. 16(3), 59-73 [cit. 2024-09-30]. ISSN 1804-1930. Dostupné z: doi:10.7160/aol.2024.160305
- SCYTL, 2023. Secure Online Voting Designed for You. Scytl [online]. [cit. 2023-10-12]. Dostupné z: <https://scytl.com/>

Příloha C: Formulář pro experty s pokyny

Zobrazen je úvod formuláře zakončen prvním požadavkem pro určení úrovně, následně je 141 řádků jednotlivých požadavků (viz Kapitola 4.5) nahrazeno [...] a zobrazen je následně poslední požadavek a možnost slovního komentáře:

Šetření: Určení úrovně požadavku CMRec(2017)5

Vážený experte, děkuji, že jste se rozhodl zúčastnit šetření, které má pomoci určit nejlepší kompromis pro stanovení úrovně, od který má být vyžadováno splnění určitého požadavku doporučení CMRec(2017)5 Rady Evropy.

Získané údaje budou použity v disertační práci Tomáše Martínka. U každého experta bude uvedena odbornost nebo pracovní zařazení. Vyplněním tohoto dotazníku souhlasíte se zpracováním zadaných údajů pro zmíněné účely.

Bylo stanoveno těchto 6 úrovní (0-5) významnosti voleb prováděných prostřednictvím internetového hlasovacího systému:

0 - Testovací - tato úroveň nemusí splňovat žádný požadavek.

1 - Nezávazná hlasování - tato úroveň zahrnuje nezávazná konzultační referenda a nevýznamné volby (anketa Miss sympatie apod.).

2 - Volby nižší významnosti informovanými voliči - tato úroveň zahrnuje volby do orgánů s nižším významem pro celou společnost (volby akademického senátu, volby v soukromých společnostech, volby v SVJ, vnitrostranické volby apod.), kde se volby účastní technicky gramotní voliči, alternativně je možnost pomoci s odevzdáním hlasu elektronicky nebo jiným volebním kanálem.

3 - Závazná lokální referenda, volby nižší významnosti bez ohledu na technickou zdatnost voliče - tato úroveň zahrnuje závazná místní referenda, volby do orgánů s nižším významem pro celou společnost (volby akademického senátu, volby v soukromých společnostech, volby v SVJ, vnitrostranické volby apod.), které se mohou účastnit i méně technicky zdatní a méně informovaní voliči.

4 - Hybridní závazná celonárodní referenda a omezené celonárodní volby - tato úroveň zahrnuje celonárodní referenda, kde lze hlasovat i papírově, dále celonárodní volby, kde může hlasovat přes internet maximálně 10 % voličů (např. celonárodní volby pouze pro voliče v zahraničí) a volby, kde se nevolí do orgánů s vlivem na volební zákony (komunální a krajské volby).

5 - Volby splňující požadavky Rady Evropy - tato úroveň musí splňovat všechny požadavky, jedná se například o závazné celonárodní volby pro celou populaci.

Pro další informace je k dispozici organizátor šetření Tomáš Martínek, podrobnější informace v češtině jsou také na www.odvolit.cz. V následujícím formuláři určujete úroveň, od které má být daný požadavek povinný. Do formuláře vyplňujete číslo (1-5) jako Nejlepší návrh (nutné vyplnit vždy), který určuje dle Vás optimální úroveň, od které by mělo být splnění požadavku povinné. Pokud si přesnou úroveň nejste jisti, můžete vyplnit dolní mez a horní mez určující úroveň, mezi kterými se rozhodujete. Například, pokud se domníváte, že by měl být požadavek povinný

od úrovně 2 až 3 (a více se kloníte k úrovni 3), můžete zadat Nejlepší návrh 3, Dolní mez 2, Horní mez 3. Pokud Dolní a horní mez nevyplníte, bude do obou zadána úroveň z Nejlepší návrh.

Datum vyplnění:					
Expert:					
Kontakt:					
ID	Požadavek	Nejlepší návrh	Dolní mez	Horní mez	Podrobněji
1	Uživatelské rozhraní by mělo být snadno použitelné				Voličské rozhraní systému elektronického hlasování musí být snadno srozumitelné a použité pro všechny voliče.
[..]	[..]				[..]
49	Systém potvrdí odevzdání hlasů v (a) časovém limitu				Skutečnost, že se hlasovalo v předepsaných lhůtách, by měla být zjistitelná.
Možnost pro slovní komentář:					
Pokud máte k elektronické volby, stanovení úrovně a jinému dodatečný komentář, můžete zde doplnit.					

Příloha D: Ukázka vyhodnocení dat metodou BeCoMe

Tato příloha obsahuje ukázkou vyhodnocení prvního požadavku Doporučení CM/Rec(2017)5 výboru ministrů členským státům o standardech pro elektronické hlasování i s popisem specializací 13 expertů (stejným způsobem bylo vyhodnoceno i zbylých 142 požadavků) pomocí aplikace rozhodovací metody BeCoMe:

Best compromise/agreement of experts' proposals								
for the question:								
1 - Uživatelské rozhraní by mělo být snadno použitelné							Date:	9/9/2024
							BEST COMPROMISE:	Max. Error of estimate
							1,95	0,05
Number of experts:		13						
Experts		Best proposal	Lower limit	Upper limit				
E1: expert na e-government		2	2	3				
E2: IT expert, akademik		1	1	1				
E3: Expert na volební systémy		3	1	3				
E4: IT expert, programátor		2	2	2				
E5: IT expert na kryptografii		3	2	3				
E6: Expert na IT projektování, akademik		2	1	2				
E7: IT expert na internetové technologie		1	1	1				
E8: Matematicka		3	2	3				
E9: Expert na AI		1	1	1				
E10: IT expert ve veřejné správě		2	2	3				
E11: ústavní právník		2	2	2				
E12: IT expert, vývojář		1	1	2				
E13: politolog		2	2	3				

Příloha E: Agregovaná data s určením úrovně požadavku

Agregovaná tabulka obsahuje vyplněné hodnoty od 13 expertů (E) ke každému požadavku (B - Best, L - Lower, U - Upper), sloupec BC obsahuje hodnotu nejlepšího kompromisu a MEoE obsahuje vypočtenou maximální chybu odhadu vypočtenou metodou BeCoMe. Sloupec Min obsahuje hodnotu nejlepšího kompromisu poníženou o maximální chybu odhadu a sloupec $\approx$ obsahuje zaokrouhlení na celé číslo:

Expert:	E1		E2		E3		E4		E5		E6		E7		E8		E9		E10		E11		E12		E13																				
ID	B	L	U	B	L	U	B	L	U	B	L	U	B	L	U	B	L	U	B	L	U	B	L	U	B	L	U	BC	MEoE	Min	≡														
1	2	2	3	1	1	1	3	1	3	2	2	2	3	2	3	2	1	1	1	1	3	2	3	1	1	1	2	2	3	1,95	0,05	1,9	2												
1(a)	2	2	3	1	1	1	1	1	3	2	2	2	1	1	1	2	1	2	1	1	1	2	2	3	3	3	2	2	2	1,88	0,12	1,76	2												
1(b)	3	3	4	2	2	3	3	3	4	2	2	2	1	1	1	2	2	5	5	5	2	2	2	1	1	1	3	2	3	3	3	2	4	3	3	4									
1(c)	5	4	5	1	1	1	1	1	2	2	2	2	3	3	3	2	2	3	1	1	1	4	4	4	1	1	1	3	3	4	4	4	4	3	5	3	3	3							
2	2	2	3	1	1	1	2	1	3	2	2	2	3	3	3	2	1	3	2	2	2	4	4	4	3	3	3	2	1	2	1	1	1	2	2	3	4	3	4						
2(a)	3	3	4	4	3	4	2	2	3	2	2	2	4	3	4	3	3	4	3	3	3	4	4	4	3	3	3	3	5	4	4	4	3	3	4	4	4	4	3,33	0	3,33	3			
2(b)	3	3	4	3	3	4	1	1	3	2	2	2	3	3	3	3	3	4	2	2	2	2	2	2	3	3	3	1	1	1	1	1	1	3	3	4	4	4	4	2,77	0,23	2,54	3		
3	3	3	3	3	3	3	3	2	2	3	2	2	2	3	3	3	3	3	4	3	3	3	2	2	2	3	3	3	2	2	2	3	3	3	3	4	3	3	3	2,88	0,12	2,76	3		
4	3	3	3	3	3	3	1	1	2	4	4	5	3	2	3	3	3	3	3	2	2	2	3	3	3	3	3	2	2	3	5	5	5	3	3	4	3	3	3	3	3	3	3		
5	3	2	3	3	3	3	1	1	2	2	2	2	3	3	3	3	2	3	2	2	2	2	2	2	1	1	1	3	3	4	3	3	3	3	3	4	3	3	3	2,58	0,09	2,49	2		
5(a)	3	2	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	2	2	2	4	4	4	3	3	3	4	4	5	3	3	3	3	2	2	3	4	4	4	3,06	0,06	3	3	
5(b)	2	1	2	2	2	2	1	1	2	3	3	3	3	3	3	2	1	2	2	2	2	4	4	4	1	1	1	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
6	2	1	2	2	1	2	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	1	1	2	2	2	4	4	4	2	1	2	3	3	3	3	2,01	0,01	2	2		
7	2	2	2	2	1	2	1	1	2	1	1	1	2	2	2	1	2	2	2	2	4	4	4	1	1	1	2	2	3	3	3	3	2	1	2	2	2	2	1,99	0,01	1,98	2			
8	2	2	2	2	1	2	2	1	2	2	2	2	2	2	2	2	2	3	2	2	2	3	3	3	1	1	1	3	2	3	3	3	3	2	2	2	2	2	2,05	0,05	2	2			
9	2	2	2	2	1	2	2	1	2	1	1	1	2	2	2	2	1	2	2	2	2	2	2	2	1	1	1	2	1	2	2	2	2	2	2	2	2	2	1,87	0,13	1,74	2			
9(a)	2	2	2	2	2	2	1	2	1	1	1	2	2	2	2	1	2	2	2	2	3	3	3	1	1	1	3	2	4	2	2	2	2	2	2	2	2	2	1,97	0,03	1,94	2			
9(b)	2	2	2	2	2	2	1	2	1	1	1	2	2	2	2	1	2	2	2	2	2	2	2	1	1	1	3	2	4	2	2	2	2	2	2	2	2	1,94	0,06	1,88	2				

9(c)	2	2	2	2	2	2	2	1	2	1	1	1	1	2	2	2	2	2	2	2	2	2	3	3	3	1	1	1	1	5	4	5	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
------	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

23(c)	3	3	3	1	1	1	2	2	3	3	3	3	2	2	2	3	2	3	4	4	4	4	4	3	3	3	3	4	4	4	4	3	3	3	3	3	3	2,97	0,03	2,94	3			
23(d)	5	4	5	1	1	1	3	3	3	3	3	4	3	2	3	5	4	5	5	5	5	5	5	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	3,92	0,08	3,84	4		
24	2	2	2	3	3	3	3	3	3	1	1	1	2	2	3	2	1	2	4	4	4	4	2	3	4	1	1	1	4	4	4	3	3	2	2	3	3	3	3	2,78	0,22	2,56	3	
25	2	1	2	2	2	2	3	3	3	2	2	2	2	2	2	2	1	2	4	4	4	4	4	3	5	1	1	1	3	2	3	3	3	3	2	2	3	4	4	4	2,45	0,12	2,33	2
26	2	2	2	2	2	2	2	2	2	2	2	2	1	1	1	2	1	2	4	4	4	2	1	3	1	1	1	2	1	2	3	3	3	2	2	3	4	4	4	2,1	0,1	2	2	
26(a)	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	4	4	4	3	3	1	1	1	2	1	2	3	3	3	2	2	3	4	4	4	2,18	0,18	2	2		
26(b)	3	2	3	2	2	2	3	3	3	3	3	3	2	1	2	3	2	3	4	4	4	4	4	4	1	1	1	4	3	4	5	5	5	3	2	4	4	4	4	3,03	0,03	3	3	
26(c)	3	3	4	3	3	3	1	1	1	2	2	2	1	1	1	3	2	3	4	4	4	4	4	4	3	3	3	4	4	5	3	3	3	3	3	4	3	3	3	2,95	0,05	2,9	3	
27	3	3	4	3	3	3	3	3	3	4	3	4	3	3	3	3	3	4	4	4	4	4	4	4	3	3	3	4	3	5	3	3	3	3	3	4	3	3	4	3,36	0,03	3,33	3	
27(a)	3	3	3	2	2	2	3	3	3	4	4	5	3	3	3	3	3	4	4	4	4	4	4	4	3	3	3	2	4	4	4	4	4	3	2	3	3	3	3	3,13	0,13	3	3	
27(b)	3	3	3	2	2	2	3	3	3	4	3	4	2	2	2	3	3	4	4	4	4	4	3	3	3	2	2	1	1	1	5	5	5	3	2	3	3	3	3	2,95	0,05	2,9	3	
27(c)	2	2	2	2	2	2	3	3	3	4	3	4	1	1	1	3	2	3	4	4	4	4	3	3	3	2	2	2	3	2	3	5	5	5	2	3	2	4	4	4	2,77	0,1	2,67	3
27(d)	5	4	5	4	4	4	3	3	3	4	4	5	2	2	2	4	4	5	4	4	4	4	3	3	3	3	3	4	4	4	5	5	5	5	4	5	4	4	4	3,92	0,08	3,84	4	
28	3	3	4	3	3	3	3	3	3	4	3	4	3	3	3	2	3	3	4	4	4	4	4	4	3	3	3	2	2	2	3	3	3	3	3	4	4	4	4	3,12	0,12	3	3	
28(a)	3	3	3	3	3	3	3	3	3	4	3	4	2	2	2	3	3	3	4	4	4	4	4	4	3	3	3	3	3	5	5	5	5	3	3	4	4	4	4	3,19	0,19	3	3	
28(b)	3	3	3	3	3	3	3	3	3	4	3	4	2	2	2	3	3	3	4	4	4	4	4	4	3	3	3	3	3	4	4	4	3	3	4	3	3	3	3	3,12	0,12	3	3	
28(c)	3	3	3	3	3	3	3	3	3	4	3	4	2	2	2	3	3	3	4	4	4	4	4	4	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3,08	0,08	3	3	
28(d)	3	3	3	3	3	3	3	3	4	3	4	1	1	1	1	3	3	3	4	4	4	4	4	4	3	3	3	3	3	3	3	3	3	3	3	4	4	4	4	3,08	0,08	3	3	
28(e)	3	3	3	3	3	3	3	3	3	4	3	4	3	3	3	3	3	3	4	4	4	4	4	4	3	3	3	3	3	3	4	4	4	3	3	4	5	5	5	3,23	0,23	3	3	
28(f)	3	3	3	3	3	3	3	3	3	4	3	4	1	1	1	3	3	3	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3	3	3	4	4	4	3,1	0,1	3	3	
28(g)	3	3	3	3	3	3	1	1	1	4	3	4	2	2	2	3	3	3	3	3	3	4	4	4	1	1	1	3	3	3	3	3	3	3	3	3	3	3	3	3	2,87	0,13	2,74	3
28(h)	3	3	3	3	3	3	2	2	4	3	4	1	1	1	1	3	3	3	3	3	3	4	4	4	1	1	1	3	3	3	3	3	3	3	3	3	4	4	4	2,92	0,08	2,84	3	
28(i)	3	3	3	3	3	3	2	2	3	1	1	1	2	2	2	3	3	3	3	3	3	4	4	4	1	1	1	3	3	3	3	3	3	3	3	3	4	4	4	2,86	0,14	2,72	3	
28(j)	3	3	4	2	2	2	3	2	3	1	1	1	2	2	2	3	3	4	3	3	3	4	4	4	1	1	1	3	3	4	3	3	3	3	2	4	3	3	3	2,83	0,17	2,66	3	
28(k)	3	3	3	2	2	2	2	2	2	2	2	4	4	4	4	3	3	4	3	3	3	3	4	4	1	1	1	3	3	3	3	3	3	3	4	4	3	4	4	2,95	0,05	2,9	3	
29	2	2	3	2	2	2	3	2	3	3	3	3	3	3	3	2	2	3	2	2	2	2	4	4	4	3	3	4	4	4	3	3	3	4	4	4	3	3	3	2,96	0,04	2,92	3	
29(a)	2	2	3	2	2	2	3	3	3	2	2	2	2	2	2	1	3	4	4	4	4	3	3	3	3	3	3	2	2	2	2	2	3	2	3	3	3	3	2,44	0,1	2,34	2		

29(b)	2	2	2	2	2	2	3	3	3	2	2	2	2	1	2	2	1	2	3	3	3	4	4	4	2	2	2	4	4	4	2	2	2	2	3	2	3	3	2,24	0,24	2	2	
29(c)	2	2	2	2	2	2	3	2	3	2	2	2	2	2	2	2	2	3	3	3	3	3	2	2	2	4	4	4	4	4	4	2	2	3	3	3	3	2,47	0,14	2,33	2		
29(d)	2	2	3	2	2	2	3	2	3	2	2	3	3	3	2	2	3	4	4	4	4	4	3	3	3	2	4	2	2	2	2	2	3	2	3	3	2,69	0,03	2,66	3			
30	3	3	3	3	3	3	3	2	3	2	2	2	2	2	2	3	2	3	4	4	4	3	3	2	2	2	3	3	3	3	3	3	3	4	4	4	4	2,95	0,05	2,9	3		
30(a)	3	3	3	3	3	3	3	2	3	2	2	2	2	2	3	2	3	3	3	3	4	4	4	2	2	2	3	3	3	3	3	3	3	2	3	4	4	4	2,92	0,08	2,84	3	
30(b)	3	3	3	3	3	3	3	2	3	2	2	2	3	2	3	3	3	4	3	3	3	4	4	4	2	2	2	3	3	3	3	3	3	2	3	4	4	4	2,97	0,03	2,94	3	
30(c)	3	3	3	3	3	3	3	3	3	2	2	2	2	2	2	3	3	4	3	3	3	4	4	4	2	2	2	3	3	3	3	3	3	2	3	3	3	3	2,92	0,08	2,84	3	
30(d)	3	3	3	3	3	3	3	2	3	2	2	2	2	2	2	3	3	3	3	3	4	4	4	2	2	2	3	3	3	3	3	3	3	2	3	4	4	4	2,94	0,06	2,88	3	
31	2	2	2	2	2	2	3	3	3	4	2	4	1	1	1	2	1	2	3	3	3	4	4	4	2	2	2	3	2	3	3	3	3	2	2	2	2	2	2,22	0,22	2	2	
31(a)	2	2	2	1	1	1	3	3	3	1	1	2	3	2	3	2	2	2	3	3	3	4	4	4	2	2	2	4	4	5	2	2	2	2	3	2	2	2	2,22	0,22	2	2	
31(b)	3	2	3	3	3	3	3	3	3	1	1	2	3	3	3	2	2	3	4	4	4	4	4	4	2	2	2	3	4	3	3	3	3	2	2	3	3	3	2,92	0,08	2,84	3	
31(c)	2	2	3	2	2	2	3	3	3	2	2	3	3	3	3	2	2	3	4	4	4	4	4	4	3	3	3	3	4	2	2	2	2	2	3	3	3	2,91	0,09	2,82	3		
32	2	2	2	1	1	1	2	2	2	2	2	2	2	2	2	1	2	2	2	2	4	4	4	1	1	1	2	1	2	2	2	2	2	2	3	2	2	2	1,99	0,01	1,98	2	
32(a)	2	2	2	1	1	1	2	2	2	2	2	2	2	2	2	2	2	3	3	3	4	4	4	2	2	2	1	2	3	3	3	2	2	3	2	2	2	2,12	0,12	2	2		
32(b)	3	3	3	1	1	1	2	2	3	2	2	2	3	3	3	2	2	3	3	3	3	4	4	4	3	3	3	3	3	3	3	3	3	3	3	2	2	2	2,83	0,17	2,66	3	
32(c)	2	2	3	2	2	2	3	2	3	2	2	2	3	2	3	2	2	3	4	4	4	4	4	4	3	3	3	2	3	4	4	4	2	2	3	2	2	2	2,72	0,05	2,67	3	
33	2	2	3	2	2	2	3	2	3	2	2	2	3	3	3	2	2	3	3	3	3	3	3	3	3	3	2	2	3	3	3	3	2	2	3	3	3	2,64	0,03	2,61	3		
33(a)	3	3	3	2	2	2	3	3	3	2	2	2	3	2	3	3	3	3	4	4	4	3	3	3	3	3	3	3	3	4	4	4	3	3	4	3	3	3	3	0	3	3	
33(b)	2	2	2	2	2	2	3	3	3	2	2	2	3	3	3	2	2	3	4	4	4	4	3	3	3	3	3	2	2	2	4	4	4	3	3	4	3	3	2,91	0,09	2,82	3	
33(c)	2	2	3	2	2	2	3	3	3	2	2	2	4	4	4	2	2	2	4	4	4	4	2	2	4	4	4	2	2	3	3	3	3	3	3	4	4	4	2,95	0,05	2,9	3	
33(d)	3	3	3	3	3	3	3	4	2	2	2	4	4	4	3	2	3	4	4	4	4	2	2	2	4	4	4	3	3	3	4	4	4	3	4	4	4	3,29	0,04	3,25	3		
33(e)	4	4	4	3	3	3	3	3	4	2	2	2	4	4	4	3	3	4	4	4	4	4	2	2	2	4	4	4	3	4	4	4	4	4	4	3	4	4	3,55	0,12	3,43	3	
33(f)	4	4	4	3	3	3	3	3	3	3	3	4	4	4	3	3	4	4	4	4	4	2	2	2	3	3	3	4	4	4	4	4	4	4	5	4	4	3,76	0,24	3,52	4		
34	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	2	2	2	3	3	3	3	3	3	4	4	4	3	3	4	4	4	3,1	0,1	3	3	
35	5	4	5	3	3	3	3	3	3	3	3	3	3	3	3	4	4	5	3	3	3	3	3	3	3	3	3	4	3	4	3	3	3	5	4	5	4	4	3,24	0,24	3	3	
36	4	3	4	2	2	2	3	2	3	4	4	4	3	3	3	4	4	5	4	4	4	4	3	3	3	3	3	4	3	4	3	3	3	4	4	5	3	3	3	3,18	0,18	3	3
36(a)	4	4	4	2	2	2	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	4	4	4	4	4	5	3	3	3	3,78	0,22	3,56	4	

37	4	4	4	4	4	4	3	3	3	2	2	2	2	3	3	3	4	4	4	4	4	4	4	3	3	4	4	5	5	5	5	4	4	5	4	4	4	3,87	0,13	3,74	4			
37(a)	4	4	4	4	4	4	3	3	3	4	4	5	4	3	4	4	4	4	4	4	4	4	4	4	4	4	5	4	5	5	5	5	4	4	5	4	4	4	4,04	0,04	4	4		
37(b)	4	4	4	3	3	3	3	3	4	4	4	3	3	3	4	4	4	4	4	4	4	4	4	3	3	3	4	4	4	4	4	4	4	5	4	4	4	4	3,86	0,14	3,72	4		
37(c)	4	4	4	4	4	4	3	3	3	4	4	4	3	3	3	4	4	4	4	4	4	4	4	3	3	3	4	4	4	4	4	4	4	4	5	4	4	4	3,9	0,1	3,8	4		
37(d)	4	4	4	4	4	4	3	3	3	4	4	4	3	3	3	4	4	4	4	4	4	4	4	3	3	3	4	4	4	4	4	4	4	4	5	4	4	4	3,9	0,1	3,8	4		
37(e)	4	4	4	2	2	2	3	3	3	4	4	4	3	3	3	4	4	4	4	4	4	4	4	3	3	3	4	4	4	4	4	4	4	5	3	3	3	3,78	0,22	3,56	4			
38	4	4	4	2	2	2	2	2	2	3	3	3	3	3	3	4	4	4	4	4	4	5	5	5	3	3	3	4	4	4	4	4	4	5	2	2	2	3,71	0,29	3,42	3			
39	4	4	4	3	3	3	3	3	3	2	2	2	3	2	3	4	4	4	4	4	4	4	3	3	3	3	3	4	4	4	4	4	4	5	2	2	2	3,15	0,15	3	3			
39(a)	4	4	4	3	3	3	3	3	3	2	2	2	3	2	3	4	4	4	4	4	4	4	4	3	3	3	4	4	4	4	4	4	4	3	5	2	2	2	3,68	0,32	3,36	3		
39(b)	4	4	4	3	3	3	3	3	3	1	1	1	2	2	2	4	4	4	4	4	4	4	4	3	3	3	4	4	5	4	4	4	4	4	5	2	2	2	3,64	0,36	3,28	3		
39(c)	4	4	4	3	3	3	3	3	3	2	2	2	2	2	2	4	4	4	4	4	4	3	3	3	3	3	3	3	3	4	4	4	4	3	4	2	2	2	3,06	0,06	3	3		
40	3	3	3	3	3	3	4	3	4	2	2	2	2	2	2	3	3	4	4	4	4	3	3	3	1	1	1	3	3	3	4	4	4	3	3	4	3	3	3	2,97	0,03	2,94	3	
40(a)	5	5	5	3	3	3	4	3	4	2	2	2	2	2	3	3	5	3	3	3	4	4	4	2	2	2	3	2	3	3	3	3	5	4	5	2	2	2	3,06	0,06	3	3		
40(b)	3	3	3	1	1	1	3	3	4	2	2	2	1	1	1	3	2	3	3	3	3	2	2	2	1	1	1	3	2	3	3	3	3	3	3	4	2	2	2	2,49	0,18	2,31	2	
40(c)	2	2	2	1	1	1	3	3	4	2	2	2	1	1	1	2	2	2	2	2	2	2	2	1	1	1	2	1	2	2	2	2	2	2	2	2	2	2	1,92	0,08	1,84	2		
40(d)	1	1	1	1	1	1	3	2	3	1	1	1	2	2	2	1	1	1	2	2	2	3	3	1	1	1	1	1	2	2	2	2	1	1	1	2	2	2	1,47	0,14	1,33	1		
40(e)	5	5	5	2	2	2	3	2	3	1	1	1	2	2	2	3	3	4	2	2	2	4	4	4	2	2	2	4	4	5	3	3	3	5	4	5	2	3	3	2,82	0,15	2,67	3	
40(f)	3	3	3	2	2	2	3	3	3	4	3	4	3	2	3	3	3	4	2	2	2	4	4	4	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3		
40(g)	3	3	4	3	3	3	3	3	3	2	2	2	2	2	2	3	3	4	2	2	2	3	3	3	3	3	3	3	3	3	4	3	3	3	3	4	2	3	3	2,92	0,08	2,84	3	
40(h)	2	2	2	2	2	2	3	2	3	1	1	1	2	2	2	2	3	2	2	2	2	3	3	3	3	3	2	2	2	3	3	3	2	2	3	2	2	2	2,13	0,13	2	2		
40(i)	3	3	4	2	2	2	4	3	4	3	2	3	3	2	3	3	2	4	3	3	3	3	4	4	4	3	3	3	3	3	4	3	3	3	3	3	4	3	3	3	3,04	0,04	3	3
40(j)	3	3	3	2	2	2	3	3	3	2	2	2	3	3	3	3	3	4	4	4	5	5	5	3	3	3	3	2	3	3	3	3	3	3	4	3	4	4	3,06	0,06	3	3		
40(k)	3	3	4	3	3	3	3	3	3	2	2	2	2	2	2	3	3	4	4	4	4	5	5	5	3	3	3	2	3	3	3	3	3	3	4	4	4	4	3,1	0,1	3	3		
40(l)	2	2	3	2	2	2	3	3	3	2	2	2	2	2	2	3	2	4	4	4	4	5	5	5	3	3	2	2	3	3	3	3	3	3	4	4	4	4	3	0	3	3		
40(m)	2	2	2	2	2	2	3	2	3	2	2	2	2	2	2	1	2	4	4	4	4	4	4	2	2	2	1	2	3	3	3	3	2	2	3	2	2	2	2,21	0,21	2	2		
41	2	2	3	2	2	2	3	2	3	1	1	1	2	1	2	2	1	2	4	4	4	4	4	4	1	1	1	2	2	3	3	3	2	2	3	4	4	4	2,4	0,06	2,34	2		
41(a)	3	3	3	2	2	2	2	3	1	1	1	1	1	1	2	2	3	4	4	4	4	4	4	1	1	1	1	2	2	3	3	3	3	3	4	3	3	3	2,41	0,08	2,33	2		

41(b)	3	3	3	3	3	3	3	2	3	2	2	2	2	2	2	2	3	4	4	4	4	4	4	2	2	2	4	4	5	4	4	4	3	3	4	4	4	4	3,08	0,08	3	3			
41(c)	3	3	3	3	3	3	3	4	2	2	2	2	2	2	2	2	3	4	4	4	4	4	4	3	3	3	4	4	5	4	4	4	4	3	3	4	4	4	4	3,29	0,04	3,25	3		
42	3	3	3	3	3	3	3	3	2	2	3	1	1	1	3	3	3	4	4	4	4	4	4	1	1	1	5	5	5	2	2	2	3	3	4	2	2	2	2,91	0,09	2,82	3			
42(a)	3	3	4	3	3	3	3	3	2	2	3	2	2	2	3	3	3	4	4	4	4	4	4	2	2	2	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3				
43	3	3	4	1	1	1	3	3	3	2	2	3	3	2	3	3	3	3	4	4	4	4	3	3	3	2	2	2	4	4	4	3	3	3	3	3	4	3	3	3	2,95	0,05	2,9	3	
43(a)	3	3	3	1	1	1	3	3	3	2	2	3	3	3	3	3	3	4	4	4	4	4	4	2	2	2	4	3	4	3	3	3	3	3	3	4	3	3	3	2,97	0,03	2,94	3		
44	2	2	2	2	2	2	3	2	3	2	2	2	1	1	1	3	2	3	4	4	4	4	5	5	5	1	1	1	2	1	2	3	3	3	3	2	2	3	3	3	3	2,41	0,08	2,33	2
45	3	3	3	2	2	2	3	3	3	2	2	2	1	1	1	2	2	3	4	4	4	4	4	4	2	2	2	3	3	3	3	3	3	3	2	2	3	2	2	2	2,46	0,13	2,33	2	
46	2	2	2	2	2	2	3	2	3	2	2	2	1	1	1	2	2	3	4	4	4	4	5	5	5	1	1	1	4	4	4	3	3	3	3	2	2	3	2	2	2	2,45	0,12	2,33	2
46(a)	5	5	5	5	5	5	3	3	3	2	2	2	3	3	3	5	4	5	5	5	5	5	5	5	3	3	5	5	5	4	4	4	4	5	4	5	3	3	3	4,36	0,31	4,05	4		
47	2	2	3	1	1	1	3	3	3	2	2	2	1	1	1	2	2	3	2	2	2	4	4	4	1	1	1	3	3	4	3	3	3	3	3	3	2	3	2	2	2	2,31	0,03	2,28	2
47(a)	3	3	4	2	2	2	3	3	4	2	2	2	3	3	3	3	2	3	4	4	4	4	4	4	3	3	3	3	3	3	3	3	3	3	3	4	2	2	2	2,99	0,01	2,98	3		
47(b)	3	3	3	1	1	1	3	3	5	2	2	2	2	2	2	3	2	3	3	3	3	4	4	4	3	3	3	3	3	3	3	3	3	3	3	4	2	2	2	2,87	0,13	2,74	3		
48	1	1	2	1	1	1	1	1	2	2	2	2	2	2	2	1	1	2	1	1	1	1	4	4	4	2	2	2	4	4	4	3	3	3	3	1	1	2	2	2	2	2,01	0,01	2	2
48(a)	3	3	3	3	3	3	5	5	5	3	3	3	3	2	3	3	3	3	3	3	3	5	5	5	3	3	3	3	3	3	3	3	3	3	3	4	4	4	4	3,19	0,19	3	3		
49	3	3	3	2	2	2	4	4	5	3	3	3	2	1	2	3	3	3	3	3	3	5	5	5	1	1	1	3	2	3	3	3	3	3	3	4	2	2	2	2,92	0,08	2,84	3		
49(a)	3	3	3	1	1	1	3	3	3	1	1	1	2	2	2	3	3	3	3	3	3	3	3	4	1	1	1	2	2	2	2	2	2	3	3	4	2	2	2	2,14	0,14	2	2		

Příloha F: Vyplněný technický pracovní list pro hodnocení internetového hlasovacího systému pro tajnou volbu České pirátské strany

Evaluace internetového hlasování pomocí - Doporučení CMRec(2017)5 Rady Evropy				
Tento pracovní technický list umožňuje provést hodnocení tajného vzdáleného elektronického hlasování přes Internet. Instrukce jsou k dispozici na druhém listu a Odvolit.cz.				
Hodnocený systém:		Helios Voting nasazený Českou pirátskou stranou		
Datum hodnocení:		15.6.2024 - 22.9.2024		
Hodnotitel:		Ing. Tomáš Martínek		
Kontakt:		info@odvolit.cz		
ID	Požadavek	H	Podrobněji	Ú
1	Uživatelské rozhraní by mělo být snadno použitelné	1	Voličské rozhraní systému elektronického hlasování musí být snadno srozumitelné a použitelné pro všechny voliče.	2
1(a)	Snadná interpretace možností hlasování	1	Prezentace možností hlasování na zařízení používaném voličem by měla být optimalizována pro běžného voliče, který nemá specializované počítačové znalosti.	2
1(b)	Voliči zapojení do designu	1	Voliči by měli být zapojeni do návrhu systémů elektronického hlasování, zejména s cílem identifikovat omezení a otestovat snadnost použití v každé hlavní fázi procesu vývoje.	3
1(c)	Kompatibilita systému	1	Při vývoji nových IT produktů je třeba vzít v úvahu jejich kompatibilitu se stávajícími.	3
2	Nezávislost pro zdravotně postižené voliče	1	Systém elektronického hlasování je navržen tak, aby umožňoval osobám se zdravotním postižením a zvláštními potřebami volit nezávisle.	2
2(a)	Zvláštní hlasovací rozhraní	0	Voliči by měli mít k dispozici, kdykoli je to nutné a možné, další zařízení, jako jsou speciální rozhraní nebo jiné ekvivalentní prostředky, jako je osobní asistence.	3
2(b)	Shoda WCAG 2.0 AA	0.5	Internetová hlasovací rozhraní by měla co nejvíce odpovídat pokynům stanoveným v iniciativě Web Accessibility Initiative (WAI).	3
3	Pokud elektronické hlasování není všeobecně dostupné, jsou k dispozici další hlasovací kanály	1	Nejsou-li kanály elektronického hlasování na dálku všeobecně přístupné, jsou pouze doplňkovým a volitelným způsobem hlasování.	3
4	Živé volební rozhraní je explicitní	1	Před hlasováním pomocí systému elektronického hlasování na dálku musí být voliči výslovně upozorněni na to, že elektronická volba, ve které podávají své rozhodnutí elektronickými prostředky, je skutečnými volbami nebo referendem.	3
5	Informace o hlasování prezentovány jednotně	1	Všechny oficiální informace o hlasování jsou prezentovány stejným způsobem, v rámci hlasovacích kanálů i mezi nimi.	2
5(a)	Žádné nadbytečné informace o hlasování	1	Elektronický hlasovací listek používaný pro elektronické hlasování by neměl obsahovat žádné informace o možnostech hlasování, kromě těch, které vyžaduje zákon.	3
5(b)	Žádné zkreslené informace o kandidátech	1	Pokud jsou informace o možnostech hlasování dostupné ze stránky elektronického hlasování, musí být prezentovány spravedlivým způsobem.	2
6	Bezpečná agregace napříč kanály	1	Jsou-li při stejných volbách nebo referendu použity elektronické a neelektronické hlasovací kanály, musí existovat bezpečná a spolehlivá metoda pro sečtení všech hlasů a pro výpočet výsledku.	2
7	Jednoznačně identifikovatelní voliči	1	Zajistí se jednoznačná identifikace voličů tak, aby je bylo možné nezaměnitelně odlišit od ostatních osob.	2
8	Ověřování voličů	1	Systém elektronického hlasování udělí uživateli přístup pouze po jeho ověření jako osoby s hlasovacím právem.	2
9	Jeden hlas na hlasujícího...	1	Systém elektronického hlasování zajistí, aby byl odevzdán pouze příslušný počet hlasů na jednoho voliče, uložen do elektronické volební schránky a zahrnut do výsledku voleb.	2
9(a)	...i když je povoleno více hlasování	1	Pokud je voliči umožněno odevzdat elektronický hlas vícekrát, měla by být přijata vhodná opatření, která zajistí, že bude započítán pouze jeden hlas.	2
9(b)	...i když je více kanálů	1	Pokud je voliči umožněno hlasovat více než jedním hlasovacím kanálem, měla by být přijata vhodná opatření, aby se zajistilo, že se započítává pouze jeden hlas.	2
9(c)	Jinak je zabráněno vícenásobným hlasováním	1	Ve všech ostatních případech by měla být přijata vhodná opatření, která zabrání voliči odevzdat více než jeden hlas.	2

9(d)	Informace o možnostech hlasování	1	Volič by měl být ve všech případech jasně informován o nabízených možnostech hlasování a o pravidlech pro sčítání hlasů.	2
10	Hlasovací systém je chráněn	1	Úmysl voliče nesmí být ovlivněn systémem hlasování ani žádným nepatřičným vlivem.	2
10(a)	Volič se učil ověřovat spojení	0,5	V případě elektronického hlasování na dálku by měl být volič informován o prostředcích, jak ověřit, že bylo navázáno spojení s oficiálním serverem a že byl předložen pravý hlasovací lístek.	3
10(b)	Pouze oficiální informace o hlasování	1	Systém elektronického hlasování by neměl při hlasování umožňovat jakýkoli manipulativní vliv na voliče. Zejména elektronický hlasovací lístek, kterým se provádí elektronické hlasování, by neměl obsahovat žádné neoficiální informace.	2
10(c)	Odevzdané hlasovací lístky jsou odolné proti neoprávněné manipulaci	1	Systém elektronického hlasování by měl zavést všechna možná opatření, aby se zabránilo jakémukoli manipulativnímu ovlivňování hlasování po jeho odevzdání, a bude zahrnovat opatření, která umožní ověřit, že žádný takový vliv nebyl uplatněn.	2
10(d)	Odolnost vůči nátlaku	0,5	Je-li to považováno za nutné, měl by systém elektronického hlasování nabízet mechanismy (například vícenásobné hlasování), které voliče ochrání před nátlakem, aby hlasovali určitým způsobem.	3
11	Postupy zajišťují autentické hlasování	1	Zajistí se, aby systém elektronického hlasování předložil voliči autentický hlasovací lístek a autentické informace.	2
12	Správné zachycení úmyslu voličů	1	Způsob, jakým jsou voliči vedeni procesem elektronického hlasování, je nesmí vést k tomu, aby hlasovali ukvapeně nebo bez potvrzení.	3
12(a)	Hlasovací lístek lze před vhozením upravit	1	Volič by měl mít možnost změnit svou volbu v kterémkoli bodě procesu elektronického hlasování na dálku před odevzdáním svého hlasu nebo postup přerušit.	2
13	Voliči se mohou zdržet hlasování	1	Systém elektronického hlasování poskytne voliči prostředky k účasti ve volbách nebo referendu, aniž by volič upřednostnil některou z možností hlasování.	2
14	Voliči jsou upozorněni na neplatnost hlasů	1	Systém elektronického hlasování upozorní voliče, pokud odevzdá neplatný elektronický hlas.	2
15	Individuální ověřitelnost	1	Volič musí mít možnost ověřit si, že jeho úmysl je při hlasování přesně zastoupen a že zapečetěný hlas vstoupil do elektronické volební schránky beze změn. Jakýkoli nepatřičný vliv, který změnil hlasování, musí být zjistitelný.	2
15(a)	Papírové kopie hlasování ve volbách	1	Při používání zařízení pro elektronické hlasování ve volebních místnostech by členské státy měly zvážit použití papírových hlasovacích lístků jako druhého média pro uložení hlasu pro účely ověření.	5
15(b)	Statistické audity (např. RLA)	1	Povinné sčítání hlasů ve druhém médiu ve statisticky významném počtu náhodně vybraných volebních místností by mělo být provedeno zejména u elektronických hlasovacích zařízení a optických skenerů.	4
16	Potvrzení odevzdaného hlasu	1	Volič obdrží potvrzení od systému, že hlasování bylo úspěšně odevzdáno a že celý postup hlasování byl dokončen.	2
17	Dokáže ověřit všechny platné hlasy	1	Systém elektronického hlasování poskytne spolehlivé důkazy o tom, že každý autentický hlas je přesně zahrnut do příslušných výsledků voleb. Důkazy by měly být ověřitelné prostředky, které jsou nezávislé na systému elektronického hlasování.	3
18	Dokáže ověřit zahrnutí pouze platných hlasů	1	Systém poskytne spolehlivý důkaz, že do příslušného konečného výsledku byly zahrnuty pouze hlasy oprávněných voličů. Důkazy by měly být ověřitelné prostředky, které jsou nezávislé na systému elektronického hlasování.	3
19	Tajnost hlasování	1	Elektronické hlasování je organizováno tak, aby bylo zajištěno zachování tajnosti hlasování ve všech fázích postupu hlasování.	2
19(a)	Seznam voličů oddělený od hlasovacích částí	1	Údaje v registru voličů by měly být jasně odděleny od složek hlasování.	2
20	Minimalizace dat	1	Systém elektronického hlasování zpracovává a uchovává po dobu nezbytně nutnou pouze osobní údaje potřebné pro průběh elektronické volby.	3
21	Autentizační data jsou chráněna	1	Systém elektronického hlasování a jakákoliv oprávněná strana chrání autentizační údaje tak, aby neoprávněné osoby nemohly tyto údaje zneužít, zachytit, upravit nebo jinak získat znalosti.	1
21(a)	Autentizace používá kryptografii	1	Autentizace by měla používat kryptografické mechanismy.	2

22	Seznam voličů má kontrolu přístupu	1	Rejstříky voličů uložené v systému elektronického hlasování nebo sdělované systémem elektronického hlasování jsou přístupné pouze oprávněným stranám.	2
23	Žádný přenosný doklad o odevzdání hlasů	0,5	Systém elektronického hlasování neposkytne voliči důkaz o obsahu odevzdaného hlasu pro použití třetími stranami.	3
23(a)	Ověření založené na papíru	1	Pokud je voliči poskytnut papírový doklad o elektronickém hlasování v kontrolovaném prostředí, nemělo by být voliči dovoleno jej ukazovat jiné osobě nebo tento doklad odnést mimo volební místnost.	4
23(b)	Žádné zbytkové informace po odhlasování	1	Po odevzdání hlasu by se neměly zobrazovat žádné zbytkové informace související s rozhodnutím voliče.	3
23(c)	Voliči byli informováni o rizicích a zmírněních utajování hlasování	1	V případě elektronického hlasování na dálku by měl být volič před hlasováním informován o možných rizicích pro tajnost hlasování a doporučených prostředcích, jak je omezit.	3
23(d)	Voliči se učili odstraňovat stopy ze zařízení	0,5	V případě elektronického hlasování na dálku by měl být volič informován o tom, jak odstranit, pokud je to možné, stopy hlasu ze zařízení použitého k odevzdání hlasu.	4
24	Žádné zveřejnění předčasných výsledků	1	Systém elektronického hlasování nedovolí nikomu sdělit počet odevzdaných hlasů pro jakoukoli možnost hlasování až do uzavření elektronické volební schránky. Tyto informace budou zveřejněny až po skončení období hlasování.	3
25	Utajeny jsou i předchozí hlasy voliče	1	Elektronické hlasování zajistí, že bude respektováno tajemství předchozích voleb zaznamenaných a vymazaných voličem před vydáním jeho konečného hlasování.	2
26	Anonymizace voličů během sčítání	1	Proces elektronického hlasování, zejména fáze počítání, musí být organizován tak, aby nebylo možné rekonstruovat spojení mezi nezapечатěným hlasem a voličem. Hlasy jsou a zůstávají anonymní.	2
26(a)	Identita a volba voliče odděleny	1	Informace o voličích by měly být odděleny od rozhodnutí voliče v předem definované fázi procesu sčítání.	2
26(b)	Hlasovací lístky dekódovány ASAP po uzavření	1	Jakékoli dekódování požadované pro sčítání hlasů by mělo být provedeno co nejdříve po skončení volebního období.	3
26(c)	Důvěrnost během auditu	0,5	Členské státy by měly přijmout nezbytná opatření, aby zajistily, že bude zaručena důvěrnost veškerých informací získaných jakoukoli osobou při výkonu auditorských funkcí.	3
27	Postupné zavádění elektronického hlasování	1	Členské státy, které zavedou elektronické hlasování, tak učiní postupně a progresivně.	3
27(a)	Veřejná studie proveditelnosti předem	1	Před výběrem a zavedením jakékoli technologie elektronického hlasování by měla být vypracována a zveřejněna formální studie proveditelnosti. Měla by obsahovat důvody pro přijetí tohoto systému, analýzu rizik, posouzení právního rámce, plánování pilotních projektů a jejich hodnocení, jakož i analýzu nákladů a přínosů.	3
27(b)	Prvně piloti	1	Jakákoli implementace pilotních projektů elektronického hlasování by měla začít s dostatečným předstihem před volbami a zahrnovat základní přípravy, jako je v případě potřeby přijetí podrobných předpisů pro pilotní projekty a testování systému.	3
27(c)	Konečný systém testovaný před volbami	1	Finální verze systému elektronického hlasování by měla být otestována před jeho použitím v řádných, závazných volbách.	3
27(d)	Komplexní piloti	0	Pilotní projekty by měly být prováděny na základě jasných a komplexních kritérií pro hodnocení účinnosti a integrity systému elektronického hlasování, včetně předávání výsledků.	4
28	Předem přijatá legislativa	1	Před zavedením elektronického hlasování členské státy zavedou požadované změny do příslušných právních předpisů.	3
28(a)	Zákon: Implementovat/provozovat/počítat	1	Právní rámec by měl zahrnovat postupy pro provádění elektronického hlasování od zřízení a provozu až po sčítání.	3
28(b)	Zákon: Platnost hlasování	1	Právní rámec by měl obsahovat pravidla pro stanovení platnosti elektronického hlasování.	3
28(c)	Zákon: Nesrovnalosti v ověřování	1	Právní rámec by měl zahrnovat pravidla zabývající se problémy, selháními a nesrovnalostmi vyplývajícími z používání ověřovacích nástrojů.	3
28(d)	Zákon: Ničení dat	1	Právní rámec by měl zahrnovat postupy pro proces likvidace údajů, zejména za účelem sladění zpracování, uchovávání a likvidace údajů (a vybavení) technologie hlasování s právními předpisy o ochraně osobních údajů.	3
28(e)	Zákon: Domácí/mezinárodní pozorovatelé	0	Právní rámec by měl zahrnovat ustanovení pro domácí a mezinárodní pozorovatele.	3

28(f)	Zákon: Časové osy	1	Legislativa by měla stanovit jasné harmonogramy všech fází e-voleb.	3
28(g)	Žádné hlasování před obdobím hlasování	1	Lhůta, ve které lze odevzdat elektronické hlasování, by neměla začít před oznámením voleb nebo referenda.	3
28(h)	Elektronické hlasování před osobním hlasováním povoleno	1	Dálkové elektronické hlasování může začít a/nebo skončit dříve, než je otevření jakékoli volební místnosti.	3
28(i)	Žádné elektronické hlasování po období hlasování	1	Období, ve kterém lze odevzdat elektronický hlas, by po skončení období hlasování nemělo pokračovat.	3
28(j)	Systémová zpoždění neruší platnost hlasování	1	Vkládání elektronických hlasů do elektronické volební schránky by mělo být umožněno po dostatečně dlouhou dobu po skončení období elektronického hlasování, aby se umožnilo jakékoli zpoždění při předávání zpráv dálkovým kanálem elektronického hlasování.	3
28(k)	Systém po volbách nepřístupný	1	Po skončení období elektronického hlasování by žádnému voliči neměl být umožněn přístup do systému elektronického hlasování.	3
29	Řídící volební orgán má kontrolu nad systémem	1	Príslušné právní předpisy upraví odpovědnost za fungování systémů elektronického hlasování a zajistí, aby nad nimi měl kontrolu řídící volební orgán.	3
29(a)	Transparentní zadávání zakázek	1	Procesy zadávání zakázek pro elektronické hlasování by měly být prováděny transparentním způsobem.	2
29(b)	Omezte střety zájmů	1	Měla by být přijata opatření, která zabrání možným střetům zájmů soukromých zúčastněných stran zapojených do procesu.	2
29(c)	Rozdělení povinností	1	Musí být zachováno a zdokumentováno přísné oddělení povinností.	2
29(d)	Není nadměrně závislý na prodejci	1	Členské státy by měly přijmout vhodná opatření, aby se vyhnuly okolnostem, kdy jsou volby nepřiměřeně závislé na prodejci.	3
30	Pozorovatelnost počtu	0,5	Každý pozorovatel může sledovat sčítání hlasů. Za proces sčítání odpovídá volební řídící orgán.	3
30(a)	Záznamy o procesu sčítání hlasů	1	O průběhu sčítání elektronických hlasů by měl být veden záznam, včetně informací o začátku a konci sčítání a osobách, které se sčítání účastní.	3
30(b)	Počty hlasů založené na důkazech	1	Sčítání hlasů by mělo být reprodukovatelné. Měla by existovat možnost získat spolehlivý důkaz, že postup počítání byl proveden uspokojivě, včetně nezávislého přepočtu.	3
30(c)	Vlastnosti přesnosti jsou ověřitelné	1	Ostatní funkce, které mohou ovlivnit přesnost výsledků systému elektronického hlasování, by měly být ověřitelné.	3
30(d)	Dostupnost/integrita volební urny	1	Systém elektronického hlasování by měl zachovat dostupnost a integritu elektronické volební urny a výstup z procesu sčítání tak dlouho, jak je potřeba.	3
31	Transparentnost	1	Členské státy musí být transparentní ve všech aspektech elektronického hlasování.	2
31(a)	Zveřejněný seznam použitého softwaru	1	Príslušné volební orgány by měly zveřejnit oficiální seznam softwaru použitého při e-volbách. Přinejmenším by měly uvádět použitý software, verzi, datum instalace a stručný popis.	2
31(b)	Veřejný přístup ke zdrojovému kódu, docs	1	Veřejný přístup ke složkám systému elektronického hlasování a informacím o nich, zejména dokumentaci, zdrojovému kódu a dohodám o mlčenlivosti, by měly být zpřístupněny zainteresovaným stranám a široké veřejnosti v dostatečném předstihu před volebním obdobím.	3
31(c)	Komplexní procedurální příručky	1	Zavedení technologií elektronického hlasování by mělo zahrnovat vypracování komplexních, podrobných pokynů krok za krokem včetně procedurální příručky.	3
32	Voličům poskytnuty informace o volbách	1	Veřejnost, zejména voliči, musí být v dostatečném předstihu před začátkem hlasování jasným a jednoduchým jazykem informována o: jakýchkoli krocích, které může volič učinit, aby se mohl zúčastnit a hlasovat; správném používání a fungování systému elektronického hlasování; harmonogramu elektronického hlasování, včetně všech fází.	2
32(a)	Dokumenty a podpora, jak hlasovat	1	Voličům by měl být zpřístupněn podpůrný a poradenský materiál o postupech hlasování.	2
32(b)	Informace voličům široce dostupné	1	V případě elektronického hlasování na dálku by měl být informační materiál pro voliče dostupný také prostřednictvím jiného, široce dostupného komunikačního kanálu.	3
32(c)	Veřejná ukázka systému elektronického hlasování	1	Voličům by měla být poskytnuta příležitost procvičit se před a odděleně od okamžiku odevzdání elektronického hlasování. V takovém případě by měli být účastníci výslovně upozorněni na to, že se neúčastní skutečných voleb nebo referenda.	3
33	Zveřejnění součástí systému	1	Součásti systému elektronického hlasování se zveřejní pro účely ověření a certifikace.	3

39(c)	Závěry auditu zvažované v budoucích volbách	1	Závěry vyvozené z procesu auditu by měly být zohledněny v budoucích e-volbách.	3
40	Řídící volební orgán je odpovědný za shodu, dostupnost, spolehlivost, použitelnost a bezpečnost	1	Za respektování a dodržování všech požadavků i v případě selhání a útoků odpovídá volební řídicí orgán. Řídící volební orgán odpovídá za dostupnost, spolehlivost, použitelnost a bezpečnost systému elektronického hlasování.	3
40(a)	Žádné prostoje	0,5	Dostupnost služeb elektronického hlasování pro všechny voliče během celého procesu elektronického hlasování musí být zachována.	3
40(b)	Informování voličů o incidentech	1	Voliči by měli být neprodleně informováni vhodnými prostředky v případě přerušení, pozastavení nebo restartu elektronického hlasovacího systému.	2
40(c)	Nevyloučení žádní oprávnění voličů	1	Hlasovací systém nevylučuje oprávněné voliče z odevzdání svého hlasu.	2
40(d)	Odevzdané hlasy jsou dostupné, bezpečné a přesné	1	Systém elektronického hlasování by měl zachovat dostupnost a integritu hlasů.	1
40(e)	Žádná ztráta dat v případě technických problémů	0,5	Měla by být přijata technická a organizační opatření, která zajistí, že v případě poruchy nebo závady ovlivňující systém elektronického hlasování nebudou trvale ztracena žádná data.	3
40(f)	Bezpečnostní mechanismy berou v úvahu použitelnost	1	Členské státy by měly zvážit použitelnost během vývoje bezpečnostních mechanismů.	3
40(g)	V době provozuschopnosti systému pravidelně kontrolován	0,5	Měly by být prováděny pravidelné kontroly, aby bylo zajištěno, že součásti systému elektronického hlasování fungují v souladu s technickými specifikacemi systému a že jeho služby jsou dostupné.	3
40(h)	Infrastruktura elektronického hlasování je bezpečná	1	Klíčové zařízení pro elektronické hlasování by mělo být umístěno v zabezpečené oblasti a tato oblast musí být po dobu voleb nebo referenda chráněna proti jakémukoliv neoprávněnému zásahu nebo přístupu.	2
40(i)	Existují plány obnovy po havárii	1	Během volebního období nebo období referenda by měl být zaveden plán obnovy po havárii.	3
40(j)	Možnost kontroly stavu ochrany hlasovacího zařízení	0,5	Stav ochrany hlasovacího zařízení by mělo být možné kdykoli zkontrolovat. Osoby odpovědné za zařízení by měly používat speciální monitorovací postupy, aby se zajistilo, že během období hlasování bude hlasovací zařízení a jeho použití splňovat požadavky.	3
40(k)	K dispozici jsou trvalé plány zálohování	1	Měla by existovat dostatečná záložní opatření, která by měla být trvale k dispozici, aby bylo zajištěno, že hlasování bude probíhat hladce. Jakýkoli záložní systém by měl odpovídat stejným standardům a požadavkům jako původní systém.	3
40(l)	Protokoly reakce na incidenty dostupné personálu	1	Dotčení zaměstnanci by měli být připraveni rychle zasáhnout v souladu s postupem vypracovaným příslušnými volebními orgány.	3
40(m)	Po volbách bezpečně uloženo	1	Veškeré údaje uchovávané po volbách nebo referendu by měly být bezpečně uloženy.	2
41	Přístup k infrastruktuře mají pouze oprávněné osoby	1	K centrální infrastruktuře, serverům a volebním datům mají přístup pouze osoby pověřené volebním řídicím orgánem. Jmenování osob oprávněných k elektronickému hlasování bude jasně upraveno.	2
41(a)	Přístup do systému omezen na nezbytnou funkci	1	Jmenované osoby mají omezený přístup ke službám elektronického hlasování v závislosti na jejich uživatelské identitě nebo uživatelské roli. Autentizace uživatele by měla být účinná před provedením jakékoli akce. Oddělení povinností by mělo být jasné a přísně vynucované prostřednictvím technických opatření.	2
41(b)	Pravidlo dvou osob, povinné podávání zpráv a monitorování během hlasování	1	V době, kdy je otevřena elektronická volební urna, by jakékoli oprávněné zásahy ovlivňující systém měly být provedeny týmy nejméně dvou lidí, měly by být předmětem zprávy, být sledovány zástupci řídicího volebního orgánu a případnými volebními pozorovateli.	3
41(c)	Pravidlo dvou osob pro jinou kritickou technickou činnost	0	Jakákoli jiná kritická technická činnost by měla být prováděna týmy nejméně dvou lidí. Složení týmů by se mělo pravidelně obměňovat. Tyto aktivity by měly být pokud možno prováděny mimo volební období. Měly by být předmětem zprávy.	3
42	Nasazený hlasovací systém je originální a funguje správně	0,5	Před konáním elektronických voleb se řídicí volební orgán přesvědčí, že systém elektronického hlasování je pravý a správně funguje.	3
42(a)	Kontrola vybavení před každými volbami	0	Před každými volbami by mělo být vybavení zkontrolováno a schváleno v souladu s protokolem vypracovaným příslušnými volebními orgány. Zařízení by mělo být zkontrolováno, aby bylo zajištěno, že odpovídá technickým specifikacím. Zjištění by měla být předložena příslušným volebním orgánům.	3

33(a)	Podrobné/spolehlivé údaje z pozorování	0,5	Systémy elektronického hlasování by měly vytvářet spolehlivé a dostatečně podrobné údaje z pozorování, aby bylo možné provádět pozorování voleb. Mělo by být možné spolehlivě určit čas, kdy událost vygenerovala pozorovací data. Měla by být zachována pravost, dostupnost a integrita údajů.	3
33(b)	Pozorovatelé mají přístup k dokumentům	1	Domácí a mezinárodní pozorovatelé by měli mít přístup k veškeré relevantní dokumentaci o procesech elektronického hlasování.	3
33(c)	Dokumenty v běžném jazyce	1	Členské státy by měly pozorovatelům zpřístupnit příslušnou dokumentaci, pokud je to možné, v jazyce běžně používaném v mezinárodních vztazích.	3
33(d)	Pozorovatelé vyškolení provozovateli	0	Členské státy by měly poskytovat školicí programy pro domácí a mezinárodní skupiny pozorovatelů.	3
33(e)	Pozorovatelé testování hardwaru a softwaru	0	Domácí a mezinárodní pozorovatelé a média by měli mít možnost sledovat testování softwaru a hardwaru.	3
33(f)	Pozorovatelé certifikační proces	0	Volební pozorovatelé by měli mít přístup ke všem krokům procesu hodnocení a certifikace.	4
34	Pozorovatelé volby	0	Pozorování a připomínkování e-voleb, včetně sestavování výsledků, bude umožněno každému pozorovateli v zákonem povoleném rozsahu.	3
35	Interoperabilita součástí	1	Otevřené normy se použijí k tomu, aby různé technické součásti nebo služby, případně odvozené z různých zdrojů, mohly vzájemně spolupracovat.	3
36	Pro elektronické hlasování musí existovat standardy	0,5	Členské státy vypracují technické požadavky, požadavky na hodnocení a certifikaci a zajistí, aby plně odrážely příslušné právní a demokratické zásady. Členské státy budou požadavky aktualizovat.	3
36(a)	Cíle a metody certifikace	0	Členské státy by měly stanovit cíle certifikace a metody certifikace.	4
37	Nezávislá kontrola souladu	0,5	Před zavedením systému elektronického hlasování a poté ve vhodných intervalech, a zejména po jakýchkoli významných změnách v systému, nezávislý a kompetentní orgán vyhodnotí soulad systému elektronického hlasování a veškerých informací a komunikačních prostředků komponentu technologie (ICT) s technickými požadavky. To může mít formu formální certifikace nebo jiné vhodné kontroly.	4
37(a)	Náklady na certifikaci stanoveny	0	Členské státy by měly určit rozdělení nákladů spojených s procesem certifikace. Měli by definovat odpovědnost, včetně finanční, certifikačního orgánu za kvalitu jejich práce.	4
37(b)	Certifikační orgány obdrží relevantní informace a dostatek času	0	Hodnotící a certifikační orgány by měly mít plný přístup ke všem relevantním informacím a měly by mít dostatek času na provedení certifikačního procesu před volbami.	4
37(c)	Pravidelně přezkoumávaný mandát k certifikaci	0	Mandát hodnotících a certifikačních orgánů by měl být pravidelně znovu potvrzován v předepsaných intervalech.	4
37(d)	Zprávy o certifikaci jsou samozřejmé	0	Závěry dosažené v certifikační zprávě by měly být samozřejmé s informacemi obsaženými v této zprávě.	4
37(e)	Zveřejnění certifikačních dokumentů	0	Členské státy by měly stanovit a zveřejnit jasná pravidla, pokud jde o zveřejňování závěrečné certifikační zprávy a všech příslušných dokumentů, s ohledem na důležitost transparentnosti.	4
38	Certifikát je neměnný	0	Certifikát nebo jakýkoli jiný příslušný vydaný dokument musí jasně identifikovat předmět hodnocení a musí obsahovat záruky zabraňující jeho tajné nebo neúmyslné změně.	3
39	Otevřený a komplexní audit	0,5	Systém elektronického hlasování musí být kontrolovatelný. Auditní systém musí být otevřený a komplexní a aktivně informovat o potenciálních problémech a hrozbách.	3
39(a)	Podrobné požadavky na audit	0	Auditní systém by měl zaznamenávat časy, události a akce, včetně: veškeré informace související s hlasováním, včetně počtu oprávněných voličů, počtu odevzdaných hlasů, počtu platných a neplatných hlasů, sčítání a přepočítávání atd.; jakékoli útoky na provoz systému elektronického hlasování a jeho komunikační infrastruktury; systémové poruchy, chyby a další ohrožení systému. Automatizované nástroje a systémové postupy by měly umožňovat rychlou a přesnou analýzu dat a podávání zpráv, a tím umožnit rychlou nápravnou akci. Auditní systém by měl poskytovat ověřitelné zprávy o: křížové kontrole údajů; systémové nebo síťové útoky; detekce a hlášení narušení; manipulace s daty; podvody a pokusy o podvod.	3
39(b)	Komponenty mají synchronizované zdroje času	1	Systém elektronického hlasování by měl udržovat spolehlivé synchronizované zdroje času. Přesnost zdroje času by měla být dostatečná pro zachování časových značek pro auditní záznamy a pozorovací údaje, jakož i pro zachování časových limitů pro registraci, nominaci, hlasování nebo sčítání.	3

43	Aktualizace softwaru jsou znovu certifikovány	0	Stanoví se postup pro pravidelnou instalaci aktualizovaných verzí a oprav veškerého příslušného softwaru.	3
43(a)	Postupy zavádění infrastruktury včetně aktualizace	0	Měly by být vyvinuty formální postupy pro nasazení softwaru a konfiguraci technologie hlasování. Měly by být stanoveny termíny pro aktualizace. Aktualizace, které jsou distribuovány, by měly být ověřeny (podepsány).	3
44	Po odevzdání je zašifrovaný hlas neměnný	1	Jsou-li hlasování uložena nebo sdělována mimo kontrolovaná prostředí, musí být zašifrována.	2
45	Před zahájením sčítání byly zapečetěny informace o hlasech a voličích	1	Hlasy a informace o voličích musí být zapečetěny až do zahájení procesu sčítání.	2
46	Bezpečná manipulace s kryptografickým materiálem volebním orgánem	1	Řídící volební orgán nakládá s veškerým kryptografickým materiálem bezpečně.	2
46(a)	Ceremonie generování kryptografického klíče přístupná veřejnosti	0	Soukromé kryptografické klíče by měly být vygenerovány na veřejné schůzce a měly by být rozděleny na samostatné části a sdíleny alespoň dvěma lidmi, u kterých je nepravděpodobné, že by se domluvili.	4
47	Incidenty integrity jsou hlášeny	1	Pokud dojde k incidentům, které by mohly ohrozit integritu systému, osoby odpovědné za provoz zařízení neprodleně informují volební řídicí orgán.	2
47(a)	Ohrožení integrity specifikované předem	0,5	Druhy incidentů jsou předem specifikovány volebními orgány.	3
47(b)	Specifikováno zmírnění následků incidentu	1	V případě incidentu by příslušné volební orgány měly přijmout nezbytná opatření ke zmírnění dopadů incidentu.	3
48	Autentičnost, dostupnost, integrity seznamů voličů/kandidátů, GDPR	1	Autenticita, dostupnost a integrity seznamů voličů a seznamů kandidátů bude zachována. Zdroj údajů musí být ověřen. Je třeba dodržovat ustanovení o ochraně údajů.	2
48(a)	Zabezpečení procesu tisku voličských průkazů	1	Tisk identifikačních údajů voličů, jako jsou volební karty, by měl být přezkoumán, aby byla zajištěna bezpečnost citlivých údajů.	3
49	Systém identifikuje hlasování s nesrovnalostí	1	Systém elektronického hlasování identifikuje hlasy, které jsou ovlivněny nesrovnalostí.	3
49(a)	Systém potvrdí odevzdání hlasů v časovém limitu	1	Skutečnost, že se hlasovalo v předepsaných lhůtách, by měla být zjištělná.	2
Celkem systém plně splňuje		106	požadavků ze 143.	
To činí splnění		74,13	% požadavků.	
Alespoň částečně splňuje		123	požadavků ze 143.	
To činí částečné splnění		86,01	% požadavků.	
Vyjádřené mírou splnění		114,5	ze celkových 143.	
To činí		80,07	%.	
		2	. úroveň	
ID	Doplňující požadavek	H	Podrobněji	
50(a)	Hlasovací proces musí nabízet možnost být kdykoli ukončen bez záznamu	1	Hlasovací systém může volič kdykoliv ukončit, aniž by se ukládaly jakékoliv informace ohrožující soukromí voliče.	
50(b)	Bez odkazů na třetí strany	1	Software nesmí umožňovat přístup třetích stran (včetně sociálních médií) ani obsahovat odkazy na programy/stránky mimo infrastrukturu elektronického hlasování.	
50(c)	Systém zajišťuje "věčné soukromí"	0,5	V rámci věčného soukromí nesmí být umožněno nikdy, včetně vzdálené budoucnosti, prolomit tajnost hlasování.	
50(d)	Systém zajišťuje škálovatelnost	1	Každý volič může odevzdat hlas kdykoliv během doby hlasování bez ohledu na zatížení systému či systémové nároky na odevzdání hlasu.	

Příloha G: Vyplněný technický pracovní list pro hodnocení internetového hlasovacího systému pro tajnou volbu agrárních organizací

Evaluace internetového hlasování pomocí - Doporučení CMRec(2017)5 Rady Evropy				
Tento pracovní technický list umožňuje provést hodnocení tajného vzdáleného elektronického hlasování přes Internet. Instrukce jsou k dispozici na druhém listu a Odvolit.cz.				
Hodnocený systém:		Belenios dle metodického postupu pro zemědělské podniky		
Datum hodnocení:		10.5.2024 - 18.9.2024		
Hodnotitel:		Ing. Tomáš Martínek		
Kontakt:		info@odvolit.cz		
ID	Požadavek	H	Podrobněji	Ú
1	Uživatelské rozhraní by mělo být snadno použitelné	1	Voličské rozhraní systému elektronického hlasování musí být snadno srozumitelné a použitelné pro všechny voliče.	2
1(a)	Snadná interpretace možností hlasování	1	Prezentace možností hlasování na zařízení používaném voličem by měla být optimalizována pro běžného voliče, který nemá specializované počítačové znalosti.	2
1(b)	Voliči zapojení do designu	1	Voliči by měli být zapojeni do návrhu systémů elektronického hlasování, zejména s cílem identifikovat omezení a otestovat snadnost použití v každé hlavní fázi procesu vývoje.	3
1(c)	Kompatibilita systému	1	Při vývoji nových IT produktů je třeba vzít v úvahu jejich kompatibilitu se stávajícími.	3
2	Nezávislost pro zdravotně postižené voliče	1	Systém elektronického hlasování je navržen tak, aby umožňoval osobám se zdravotním postižením a zvláštními potřebami volit nezávisle.	2
2(a)	Zvláštní hlasovací rozhraní	0	Voliči by měli mít k dispozici, kdykoli je to nutné a možné, další zařízení, jako jsou speciální rozhraní nebo jiné ekvivalentní prostředky, jako je osobní asistence.	3
2(b)	Shoda WCAG 2.0 AA	0	Internetová hlasovací rozhraní by měla co nejvíce odpovídat pokynům stanoveným v iniciativě Web Accessibility Initiative (WAI).	3
3	Pokud elektronické hlasování není všeobecně dostupné, jsou k dispozici další hlasovací kanály	1	Nejsou-li kanály elektronického hlasování na dálku všeobecně přístupné, jsou pouze doplňkovým a volitelným způsobem hlasování.	3
4	Živé volební rozhraní je explicitní	1	Před hlasováním pomocí systému elektronického hlasování na dálku musí být voliči výslovně upozorněni na to, že elektronická volba, ve které podávají své rozhodnutí elektronickými prostředky, je skutečnými volbami nebo referendem.	3
5	Informace o hlasování prezentovány jednotně	1	Všechny oficiální informace o hlasování jsou prezentovány stejným způsobem, v rámci hlasovacích kanálů i mezi nimi.	2
5(a)	Žádné nadbytečné informace o hlasování	1	Elektronický hlasovací lístek používaný pro elektronické hlasování by neměl obsahovat žádné informace o možnostech hlasování, kromě těch, které vyžaduje zákon.	3
5(b)	Žádné zkrácené informace o kandidátech	1	Pokud jsou informace o možnostech hlasování dostupné ze stránky elektronického hlasování, musí být prezentovány spravedlivým způsobem.	2
6	Bezpečná agregace napříč kanály	1	Jsou-li při stejných volbách nebo referendu použity elektronické a neelektronické hlasovací kanály, musí existovat bezpečná a spolehlivá metoda pro sečtení všech hlasů a pro výpočet výsledku.	2
7	Jednoznačně identifikovatelní voliči	1	Zajistí se jednoznačná identifikace voličů tak, aby je bylo možné nezaměnitelně odlišit od ostatních osob.	2
8	Ověřování voličů	1	Systém elektronického hlasování udělí uživateli přístup pouze po jeho ověření jako osoby s hlasovacím právem.	2
9	Jeden hlas na hlasujícího...	1	Systém elektronického hlasování zajistí, aby byl odevzdán pouze příslušný počet hlasů na jednoho voliče, uložen do elektronické volební schránky a zahrnut do výsledku voleb.	2
9(a)	...i když je povoleno více hlasování	1	Pokud je voliči umožněno odevzdat elektronický hlas vícekrát, měla by být přijata vhodná opatření, která zajistí, že bude započítán pouze jeden hlas.	2
9(b)	...i když je více kanálů	1	Pokud je voliči umožněno hlasovat více než jedním hlasovacím kanálem, měla by být přijata vhodná opatření, aby se zajistilo, že se započítává pouze jeden hlas.	2
9(c)	Jinak je zabráněno vícenásobným hlasováním	1	Ve všech ostatních případech by měla být přijata vhodná opatření, která zabrání voliči odevzdat více než jeden hlas.	2

9(d)	Informace o možnostech hlasování	1	Volič by měl být ve všech případech jasně informován o nabízených možnostech hlasování a o pravidlech pro sčítání hlasů.	2
10	Hlasovací systém je chráněn	1	Úmysl voliče nesmí být ovlivněn systémem hlasování ani žádným nepatřičným vlivem.	2
10(a)	Volič se učil ověřovat spojení	0,5	V případě elektronického hlasování na dálku by měl být volič informován o prostředcích, jak ověřit, že bylo navázáno spojení s oficiálním serverem a že byl předložen pravý hlasovací lístek.	3
10(b)	Pouze oficiální informace o hlasování	1	Systém elektronického hlasování by neměl při hlasování umožňovat jakýkoli manipulativní vliv na voliče. Zejména elektronický hlasovací lístek, kterým se provádí elektronické hlasování, by neměl obsahovat žádné neoficiální informace.	2
10(c)	Odevzdané hlasovací lístky jsou odolné proti neoprávněné manipulaci	1	Systém elektronického hlasování by měl zavést všechna možná opatření, aby se zabránilo jakémukoli manipulativnímu ovlivňování hlasování po jeho odevzdání, a bude zahrnovat opatření, která umožní ověřit, že žádný takový vliv nebyl uplatněn.	2
10(d)	Odolnost vůči nátlaku	0,5	Je-li to považováno za nutné, měl by systém elektronického hlasování nabízet mechanismy (například vícenásobné hlasování), které voliče ochrání před nátlakem, aby hlasovali určitým způsobem.	3
11	Postupy zajišťují autentické hlasování	1	Zajistí se, aby systém elektronického hlasování předložil voliči autentický hlasovací lístek a autentické informace.	2
12	Správné zachycení úmyslu voličů	1	Způsob, jakým jsou voliči vedeni procesem elektronického hlasování, je nesmí vést k tomu, aby hlasovali ukvapeně nebo bez potvrzení.	3
12(a)	Hlasovací lístek lze před vhozením upravit	1	Voliči by měli mít možnost změnit svou volbu v kterémkoli bodě procesu elektronického hlasování na dálku před odevzdáním svého hlasu nebo postup přerušit.	2
13	Voliči se mohou zdržet hlasování	1	Systém elektronického hlasování poskytne voliči prostředky k účasti ve volbách nebo referendu, aniž by volič upřednostnil některou z možností hlasování.	2
14	Voliči jsou upozorněni na neplatnost hlasů	1	Systém elektronického hlasování upozorní voliče, pokud odevzdá neplatný elektronický hlas.	2
15	Individuální ověřitelnost	1	Volič musí mít možnost ověřit si, že jeho úmysl je při hlasování přesně zastoupen a že zapečetěný hlas vstoupil do elektronické volební schránky beze změny. Jakýkoli nepatřičný vliv, který změnil hlasování, musí být zjistitelný.	2
15(a)	Papírové kopie hlasování ve volbách	1	Při používání zařízení pro elektronické hlasování ve volebních místnostech by členské státy měly zvážit použití papírových hlasovacích lístků jako druhého média pro uložení hlasu pro účely ověření.	5
15(b)	Statistické audity (např. RLA)	1	Povinné sčítání hlasů ve druhém médiu ve statisticky významném počtu náhodně vybraných volebních místností by mělo být provedeno zejména u elektronických hlasovacích zařízení a optických skenerů.	4
16	Potvrzení odevzdaného hlasu	1	Volič obdrží potvrzení od systému, že hlasování bylo úspěšně odevzdáno a že celý postup hlasování byl dokončen.	2
17	Dokáže ověřit všechny platné hlasy	1	Systém elektronického hlasování poskytne spolehlivé důkazy o tom, že každý autentický hlas je přesně zahrnut do příslušných výsledků voleb. Důkazy by měly být ověřitelné prostředky, které jsou nezávislé na systému elektronického hlasování.	3
18	Dokáže ověřit zahrnutí pouze platných hlasů	1	Systém poskytne spolehlivý důkaz, že do příslušného konečného výsledku byly zahrnuty pouze hlasy oprávněných voličů. Důkazy by měly být ověřitelné prostředky, které jsou nezávislé na systému elektronického hlasování.	3
19	Tajnost hlasování	1	Elektronické hlasování je organizováno tak, aby bylo zajištěno zachování tajnosti hlasování ve všech fázích postupu hlasování.	2
19(a)	Seznam voličů oddělený od hlasovacích částí	1	Údaje v registru voličů by měly být jasně odděleny od složek hlasování.	2
20	Minimalizace dat	1	Systém elektronického hlasování zpracovává a uchovává po dobu nezbytně nutnou pouze osobní údaje potřebné pro průběh elektronické volby.	3
21	Autentizační data jsou chráněna	1	Systém elektronického hlasování a jakákoliv oprávněná strana chrání autentizační údaje tak, aby neoprávněné osoby nemohly tyto údaje zneužít, zachytit, upravit nebo jinak získat znalosti.	1
21(a)	Autentizace používá kryptografii	1	Autentizace by měla používat kryptografické mechanismy.	2

22	Seznam voličů má kontrolu přístupu	1	Rejstříky voličů uložené v systému elektronického hlasování nebo sdělované systémem elektronického hlasování jsou přístupné pouze oprávněným stranám.	2
23	Žádný přenosný doklad o odevzdání hlasů	0,5	Systém elektronického hlasování neposkytne voliči důkaz o obsahu odevzdaného hlasu pro použití třetími stranami.	3
23(a)	Ověření založené na papíru	1	Pokud je voliči poskytnut papírový doklad o elektronickém hlasování v kontrolovaném prostředí, nemělo by být voliči dovoleno jej ukazovat jiné osobě nebo tento doklad odnést mimo volební místnost.	4
23(b)	Žádné zbytkové informace po odhlasování	1	Po odevzdání hlasu by se neměly zobrazovat žádné zbytkové informace související s rozhodnutím voliče.	3
23(c)	Voliči byli informováni o rizicích a zmírněních utajování hlasování	1	V případě elektronického hlasování na dálku by měl být volič před hlasováním informován o možných rizicích pro tajnost hlasování a doporučených prostředcích, jak je omezit.	3
23(d)	Voliči se učili odstraňovat stopy ze zařízení	0,5	V případě elektronického hlasování na dálku by měl být volič informován o tom, jak odstranit, pokud je to možné, stopy hlasu ze zařízení použitého k odevzdání hlasu.	4
24	Žádné zveřejnění předčasných výsledků	1	Systém elektronického hlasování nedovolí nikomu sdělit počet odevzdaných hlasů pro jakoukoli možnost hlasování až do uzavření elektronické volební schránky. Tyto informace budou zveřejněny až po skončení období hlasování.	3
25	Utajeny jsou i předchozí hlasy voliče	1	Elektronické hlasování zajistí, že bude respektováno tajemství předchozích voleb zaznamenaných a vymazaných voličem před vydáním jeho konečného hlasování.	2
26	Anonymizace voličů během sčítání	1	Proces elektronického hlasování, zejména fáze počítání, musí být organizován tak, aby nebylo možné rekonstruovat spojení mezi nezapecetěným hlasem a voličem. Hlasy jsou a zůstávají anonymní.	2
26(a)	Identita a volba voliče odděleny	1	Informace o voličích by měly být odděleny od rozhodnutí voliče v předem definované fázi procesu sčítání.	2
26(b)	Hlasovací listky dekódovány ASAP po uzavření	1	Jakékoli dekódování požadované pro sčítání hlasů by mělo být provedeno co nejdříve po skončení volebního období.	3
26(c)	Důvěrnost během auditu	0,5	Členské státy by měly přijmout nezbytná opatření, aby zajistily, že bude zaručena důvěrnost veškerých informací získaných jakoukoli osobou při výkonu auditorských funkcí.	3
27	Postupné zavádění elektronického hlasování	1	Členské státy, které zavedou elektronické hlasování, tak učiní postupně a progresivně.	3
27(a)	Veřejná studie proveditelnosti předem	1	Před výběrem a zavedením jakékoli technologie elektronického hlasování by měla být vypracována a zveřejněna formální studie proveditelnosti. Měla by obsahovat důvody pro přijetí tohoto systému, analýzu rizik, posouzení právního rámce, plánování pilotních projektů a jejich hodnocení, jakož i analýzu nákladů a přínosů.	3
27(b)	Prvně piloti	1	Jakákoli implementace pilotních projektů elektronického hlasování by měla začít s dostatečným předstihem před volbami a zahrnovat základní přípravy, jako je v případě potřeby přijetí podrobných předpisů pro pilotní projekty a testování systému.	3
27(c)	Konečný systém testovaný před volbami	1	Finální verze systému elektronického hlasování by měla být otestována před jeho použitím v řádných, závazných volbách.	3
27(d)	Komplexní piloti	0	Pilotní projekty by měly být prováděny na základě jasných a komplexních kritérií pro hodnocení účinnosti a integrity systému elektronického hlasování, včetně předávání výsledků.	4
28	Předem přijatá legislativa	1	Před zavedením elektronického hlasování členské státy zavedou požadované změny do příslušných právních předpisů.	3
28(a)	Zákon: Implementovat/provozovat/počítat	1	Právní rámec by měl zahrnovat postupy pro provádění elektronického hlasování od zřízení a provozu až po sčítání.	3
28(b)	Zákon: Platnost hlasování	1	Právní rámec by měl obsahovat pravidla pro stanovení platnosti elektronického hlasování.	3
28(c)	Zákon: Nesrovnalosti v ověřování	1	Právní rámec by měl zahrnovat pravidla zabývající se problémy, selháními a nesrovnalostmi vyplývajícími z používání ověřovacích nástrojů.	3
28(d)	Zákon: Ničení dat	1	Právní rámec by měl zahrnovat postupy pro proces likvidace údajů, zejména za účelem sladění zpracování, uchovávání a likvidace údajů (a vybavení) technologie hlasování s právními předpisy o ochraně osobních údajů.	3
28(e)	Zákon: Domácí/mezinárodní pozorovatelé	0	Právní rámec by měl zahrnovat ustanovení pro domácí a mezinárodní pozorovatele.	3

28(f)	Zákon: Časové osy	1	Legislativa by měla stanovit jasné harmonogramy všech fází e-voleb.	3
28(g)	Žádné hlasování před obdobím hlasování	1	Lhůta, ve které lze odevzdat elektronické hlasování, by neměla začít před oznámením voleb nebo referenda.	3
28(h)	Elektronické hlasování před osobním hlasováním povoleno	1	Dálkové elektronické hlasování může začít a/nebo skončit dříve, než je otevření jakékoli volební místnosti.	3
28(i)	Žádné elektronické hlasování po období hlasování	1	Období, ve kterém lze odevzdat elektronický hlas, by po skončení období hlasování nemělo pokračovat.	3
28(j)	Systémová zpoždění neruší platnost hlasování	1	Vkládání elektronických hlasů do elektronické volební schránky by mělo být umožněno po dostatečně dlouhou dobu po skončení období elektronického hlasování, aby se umožnilo jakékoli zpoždění při předávání zpráv dálkovým kanálem elektronického hlasování.	3
28(k)	Systém po volbách nepřístupný	1	Po skončení období elektronického hlasování by žádnému voliči neměl být umožněn přístup do systému elektronického hlasování.	3
29	Řídící volební orgán má kontrolu nad systémem	1	Příslušné právní předpisy upraví odpovědnost za fungování systémů elektronického hlasování a zajistí, aby nad nimi měl kontrolu řídicí volební orgán.	3
29(a)	Transparentní zadávání zakázek	1	Procesy zadávání zakázek pro elektronické hlasování by měly být prováděny transparentním způsobem.	2
29(b)	Omezte střety zájmů	1	Měla by být přijata opatření, která zabrání možným střetům zájmů soukromých zúčastněných stran zapojených do procesu.	2
29(c)	Rozdělení povinností	1	Musí být zachováno a zdokumentováno přísné oddělení povinností.	2
29(d)	Není nadměrně závislý na prodejci	1	Členské státy by měly přijmout vhodná opatření, aby se vyhnuly okolnostem, kdy jsou volby nepřiměřeně závislé na prodejcích.	3
30	Pozorovatelnost počtu	0,5	Každý pozorovatel může sledovat sčítání hlasů. Za proces sčítání odpovídá volební řídicí orgán.	3
30(a)	Záznamy o procesu sčítání hlasů	1	O průběhu sčítání elektronických hlasů by měl být veden záznam, včetně informací o začátku a konci sčítání a osobách, které se sčítání účastní.	3
30(b)	Počty hlasů založené na důkazech	1	Sčítání hlasů by mělo být reprodukovatelné. Měla by existovat možnost získat spolehlivý důkaz, že postup počítání byl proveden uspokojivě, včetně nezávislého přepočtu.	3
30(c)	Vlastnosti přesnosti jsou ověřitelné	1	Ostatní funkce, které mohou ovlivnit přesnost výsledků systému elektronického hlasování, by měly být ověřitelné.	3
30(d)	Dostupnost/integrita volební urny	1	Systém elektronického hlasování by měl zachovat dostupnost a integritu elektronické volební urny a výstup z procesu sčítání tak dlouho, jak je potřeba.	3
31	Transparentnost	1	Členské státy musí být transparentní ve všech aspektech elektronického hlasování.	2
31(a)	Zveřejněný seznam použitého softwaru	1	Příslušné volební orgány by měly zveřejnit oficiální seznam softwaru použitého při e-volbách. Příjemnějším by měly uvádět použitý software, verzi, datum instalace a stručný popis.	2
31(b)	Veřejný přístup ke zdrojovému kódu, docs	1	Veřejný přístup ke složkám systému elektronického hlasování a informacím o nich, zejména dokumentaci, zdrojovému kódu a dohodám o mlčenlivosti, by měly být zpřístupněny zainteresovaným stranám a široké veřejnosti v dostatečném předstihu před volebním obdobím.	3
31(c)	Komplexní procedurální příručky	1	Zavedení technologií elektronického hlasování by mělo zahrnovat vypracování komplexních, podrobných pokynů krok za krokem včetně procedurální příručky.	3
32	Voličům poskytnuty informace o volbách	1	Veřejnost, zejména voliči, musí být v dostatečném předstihu před začátkem hlasování jasným a jednoduchým jazykem informována o: jakýchkoli krocích, které může volič učinit, aby se mohl zúčastnit a hlasovat; správném používání a fungování systému elektronického hlasování; harmonogramu elektronického hlasování, včetně všech fází.	2
32(a)	Dokumenty a podpora, jak hlasovat	1	Voličům by měl být zpřístupněn podpůrný a poradenský materiál o postupech hlasování.	2
32(b)	Informace voličům široce dostupné	1	V případě elektronického hlasování na dálku by měl být informační materiál pro voliče dostupný také prostřednictvím jiného, široce dostupného komunikačního kanálu.	3
32(c)	Veřejná ukázka systému elektronického hlasování	1	Voličům by měla být poskytnuta příležitost procvičit se před a odděleně od okamžiku odevzdání elektronického hlasování. V takovém případě by měli být účastníci výslovně upozorněni na to, že se neúčastní skutečných voleb nebo referenda.	3
33	Zveřejnění součástí systému	1	Součástí systému elektronického hlasování se zveřejní pro účely ověření a certifikace.	3

33(a)	Podrobné/spolehlivé údaje z pozorování	0,5	Systémy elektronického hlasování by měly vytvářet spolehlivé a dostatečně podrobné údaje z pozorování, aby bylo možné provádět pozorování voleb. Mělo by být možné spolehlivě určit čas, kdy událost vygenerovala pozorovací data. Měla by být zachována pravost, dostupnost a integrita údajů.	3
33(b)	Pozorovatelé mají přístup k dokumentům	1	Domácí a mezinárodní pozorovatelé by měli mít přístup k veškeré relevantní dokumentaci o procesech elektronického hlasování.	3
33(c)	Dokumenty v běžném jazyce	1	Členské státy by měly pozorovatelům zpřístupnit příslušnou dokumentaci, pokud je to možné, v jazyce běžně používaném v mezinárodních vztazích.	3
33(d)	Pozorovatelé vyškolení provozovateli	0	Členské státy by měly poskytovat školicí programy pro domácí a mezinárodní skupiny pozorovatelů.	3
33(e)	Pozorovatelé testování hardwaru a softwaru	0	Domácí a mezinárodní pozorovatelé a média by měli mít možnost sledovat testování softwaru a hardwaru.	3
33(f)	Pozorovatelé certifikační proces	0	Volební pozorovatelé by měli mít přístup ke všem krokům procesu hodnocení a certifikace.	4
34	Pozorovatelé volby	0	Pozorování a připomínkování e-voleb, včetně sestavování výsledků, bude umožněno každému pozorovateli v zákonem povoleném rozsahu.	3
35	Interoperabilita součástí	0,5	Otevřené normy se použijí k tomu, aby různé technické součásti nebo služby, případně odvozené z různých zdrojů, mohly vzájemně spolupracovat.	3
36	Pro elektronické hlasování musí existovat standardy	0,5	Členské státy vypracují technické požadavky, požadavky na hodnocení a certifikaci a zajistí, aby plně odrážely příslušné právní a demokratické zásady. Členské státy budou požadavky aktualizovat.	3
36(a)	Cíle a metody certifikace	0	Členské státy by měly stanovit cíle certifikace a metody certifikace.	4
37	Nezávislá kontrola souladu	1	Před zavedením systému elektronického hlasování a poté ve vhodných intervalech, a zejména po jakýchkoli významných změnách v systému, nezávislý a kompetentní orgán vyhodnotí soulad systému elektronického hlasování a veškerých informací a komunikačních prostředků komponentu technologie (ICT) s technickými požadavky. To může mít formu formální certifikace nebo jiné vhodné kontroly.	4
37(a)	Náklady na certifikaci stanoveny	0	Členské státy by měly určit rozdělení nákladů spojených s procesem certifikace. Měly by definovat odpovědnost, včetně finanční, certifikačního orgánu za kvalitu jejich práce.	4
37(b)	Certifikační orgány obdrží relevantní informace a dostatek času	0	Hodnotící a certifikační orgány by měly mít plný přístup ke všem relevantním informacím a měly by mít dostatek času na provedení certifikačního procesu před volbami.	4
37(c)	Pravidelně přezkoumávaný mandát k certifikaci	0	Mandát hodnotících a certifikačních orgánů by měl být pravidelně znovu potvrzován v předepsaných intervalech.	4
37(d)	Zprávy o certifikaci jsou samozřejmé	0	Závěry dosažené v certifikační zprávě by měly být samozřejmé s informacemi obsaženými v této zprávě.	4
37(e)	Zveřejnění certifikačních dokumentů	0	Členské státy by měly stanovit a zveřejnit jasná pravidla, pokud jde o zveřejňování závěrečné certifikační zprávy a všech příslušných dokumentů, s ohledem na důležitost transparentnosti.	4
38	Certifikát je neměnný	0	Certifikát nebo jakýkoli jiný příslušný vydaný dokument musí jasně identifikovat předmět hodnocení a musí obsahovat záruky zabraňující jeho tajné nebo neúmyslné změně.	3
39	Otevřený a komplexní audit	0,5	Systém elektronického hlasování musí být kontrolovatelný. Auditní systém musí být otevřený a komplexní a aktivně informovat o potenciálních problémech a hrozbách.	3
39(a)	Podrobné požadavky na audit	0	Auditní systém by měl zaznamenávat časy, události a akce, včetně: veškeré informace související s hlasováním, včetně počtu oprávněných voličů, počtu odevzdaných hlasů, počtu platných a neplatných hlasů, sčítání a přepočítávání atd.; jakékoli útoky na provoz systému elektronického hlasování a jeho komunikační infrastruktury; systémové poruchy, chyby a další ohrožení systému. Automatizované nástroje a systémové postupy by měly umožňovat rychlou a přesnou analýzu dat a podávání zpráv, a tím umožnit rychlou nápravnou akci. Auditní systém by měl poskytovat ověřitelné zprávy o: křížové kontrole údajů; systémové nebo síťové útoky; detekce a hlášení narušení; manipulace s daty; podvody a pokusy o podvod.	3
39(b)	Komponenty mají synchronizované zdroje času	0,5	Systém elektronického hlasování by měl udržovat spolehlivé synchronizované zdroje času. Přesnost zdroje času by měla být dostatečná pro zachování časových značek pro auditní záznamy a pozorovací údaje, jakož i pro zachování časových limitů pro registraci, nominaci, hlasování nebo sčítání.	3

39(c)	Závěry auditu zvažované v budoucích volbách	1	Závěry vyvozené z procesu auditu by měly být zohledněny v budoucích e-volbách.	3
40	Řídicí volební orgán je odpovědný za shodu, dostupnost, spolehlivost, použitelnost a bezpečnost	1	Za respektování a dodržování všech požadavků i v případě selhání a útoků odpovídá volební řídicí orgán. Řídicí volební orgán odpovídá za dostupnost, spolehlivost, použitelnost a bezpečnost systému elektronického hlasování.	3
40(a)	Žádné prostoje	0,5	Dostupnost služeb elektronického hlasování pro všechny voliče během celého procesu elektronického hlasování musí být zachována.	3
40(b)	Informování voličů o incidentech	1	Voliči by měli být neprodleně informováni vhodnými prostředky v případě přerušení, pozastavení nebo restartu elektronického hlasovacího systému.	2
40(c)	Nevyloučení žádní oprávnění voliči	1	Hlasovací systém nevylučuje oprávněné voliče z odevzdání svého hlasu.	2
40(d)	Odevzdané hlasy jsou dostupné, bezpečné a přesné	1	Systém elektronického hlasování by měl zachovat dostupnost a integritu hlasů.	1
40(e)	Žádná ztráta dat v případě technických problémů	0,5	Měla by být přijata technická a organizační opatření, která zajistí, že v případě poruchy nebo závady ovlivňující systém elektronického hlasování nebudou trvale ztracena žádná data.	3
40(f)	Bezpečnostní mechanismy berou v úvahu použitelnost	1	Členské státy by měly zvážit použitelnost během vývoje bezpečnostních mechanismů.	3
40(g)	V době provozuschopnosti systému pravidelně kontrolován	0,5	Měly by být prováděny pravidelné kontroly, aby bylo zajištěno, že součásti systému elektronického hlasování fungují v souladu s technickými specifikacemi systému a že jeho služby jsou dostupné.	3
40(h)	Infrastruktura elektronického hlasování je bezpečná	1	Klíčové zařízení pro elektronické hlasování by mělo být umístěno v zabezpečené oblasti a tato oblast musí být po dobu voleb nebo referenda chráněna proti jakémukoliv neoprávněnému zásahu nebo přístupu.	2
40(i)	Existují plány obnovy po havárii	1	Během volebního období nebo období referenda by měl být zaveden plán obnovy po havárii.	3
40(j)	Možnost kontroly stavu ochrany hlasovacího zařízení	0,5	Stav ochrany hlasovacího zařízení by mělo být možné kdykoli zkontrolovat. Osoby odpovědné za zařízení by měly používat speciální monitorovací postupy, aby se zajistilo, že během období hlasování bude hlasovací zařízení a jeho použití splňovat požadavky.	3
40(k)	K dispozici jsou trvalé plány zálohování	1	Měla by existovat dostatečná záložní opatření, která by měla být trvale k dispozici, aby bylo zajištěno, že hlasování bude probíhat hladce. Jakýkoli záložní systém by měl odpovídat stejným standardům a požadavkům jako původní systém.	3
40(l)	Protokoly reakce na incidenty dostupné personálu	1	Dotčení zaměstnanci by měli být připraveni rychle zasáhnout v souladu s postupem vypracovaným příslušnými volebními orgány.	3
40(m)	Po volbách bezpečně uloženo	1	Veškeré údaje uchovávané po volbách nebo referendu by měly být bezpečně uloženy.	2
41	Přístup k infrastruktuře mají pouze oprávněné osoby	1	K centrální infrastruktuře, serverům a volebním datům mají přístup pouze osoby pověřené volebním řídicím orgánem. Jmenování osob oprávněných k elektronickému hlasování bude jasně upraveno.	2
41(a)	Přístup do systému omezen na nezbytnou funkci	1	Jmenované osoby mají omezený přístup ke službám elektronického hlasování v závislosti na jejich uživatelské identitě nebo uživatelské roli. Autentizace uživatele by měla být účinná před provedením jakékoli akce. Oddělení povinností by mělo být jasné a přísně vynucované prostřednictvím technických opatření.	2
41(b)	Pravidlo dvou osob, povinné podávání zpráv a monitorování během hlasování	1	V době, kdy je otevřena elektronická volební urna, by jakékoli oprávněné zásahy ovlivňující systém měly být provedeny týmy nejméně dvou lidí, měly by být předmětem zprávy, být sledovány zástupci řídicího volebního orgánu a případnými volebními pozorovateli.	3
41(c)	Pravidlo dvou osob pro jinou kritickou technickou činnost	0	Jakákoli jiná kritická technická činnost by měla být prováděna týmy nejméně dvou lidí. Složení týmů by se mělo pravidelně obměňovat. Tyto aktivity by měly být pokud možno prováděny mimo volební období. Měly by být předmětem zprávy.	3
42	Nasazený hlasovací systém je originální a funguje správně	0,5	Před konáním elektronických voleb se řídicí volební orgán přesvědčí, že systém elektronického hlasování je pravý a správně funguje.	3
42(a)	Kontrola vybavení před každými volbami	0	Před každými volbami by mělo být vybavení zkontrolováno a schváleno v souladu s protokolem vypracovaným příslušnými volebními orgány. Zařízení by mělo být zkontrolováno, aby bylo zajištěno, že odpovídá technickým specifikacím. Zjištění by měla být předložena příslušným volebním orgánům.	3

43	Aktualizace softwaru jsou znovu certifikovány	0	Stanoví se postup pro pravidelnou instalaci aktualizovaných verzí a oprav veškerého příslušného softwaru.	3
43(a)	Postupy zavádění infrastruktury včetně aktualizace	0	Měly by být vyvinuty formální postupy pro nasazení softwaru a konfiguraci technologie hlasování. Měly by být stanoveny termíny pro aktualizace. Aktualizace, které jsou distribuovány, by měly být ověřeny (podepsány).	3
44	Po odevzdání je zašifrovaný hlas neměnný	1	Jsou-li hlasování uložena nebo sdělována mimo kontrolovaná prostředí, musí být zašifrována.	2
45	Před zahájením sčítání byly zapečetěny informace o hlasech a voličích	1	Hlasy a informace o voličích musí být zapečetěny až do zahájení procesu sčítání.	2
46	Bezpečná manipulace s kryptografickým materiálem volebním orgánem	1	Řídící volební orgán nakládá s veškerým kryptografickým materiálem bezpečně.	2
46(a)	Ceremonie generování kryptografického klíče přístupná veřejnosti	0	Soukromé kryptografické klíče by měly být vygenerovány na veřejné schůzce a měly by být rozděleny na samostatné části a sdíleny alespoň dvěma lidmi, u kterých je nepravděpodobné, že by se domluvili.	4
47	Incidenty integrity jsou hlášeny	1	Pokud dojde k incidentům, které by mohly ohrozit integritu systému, osoby odpovědné za provoz zařízení neprodleně informují volební řídicí orgán.	2
47(a)	Ohrožení integrity specifikované předem	1	Druhy incidentů jsou předem specifikovány volebními orgány.	3
47(b)	Specifikováno zmírnění následků incidentu	1	V případě incidentu by příslušné volební orgány měly přijmout nezbytná opatření ke zmírnění dopadů incidentu.	3
48	Autentičnost, dostupnost, integrity seznamů voličů/kandidátů, GDPR	1	Autenticita, dostupnost a integrity seznamů voličů a seznamů kandidátů bude zachována. Zdroj údajů musí být ověřen. Je třeba dodržovat ustanovení o ochraně údajů.	2
48(a)	Zabezpečení procesu tisku voličských průkazů	1	Tisk identifikačních údajů voličů, jako jsou volební karty, by měl být přezkoumán, aby byla zajištěna bezpečnost citlivých údajů.	3
49	Systém identifikuje hlasování s nesrovnalostí	1	Systém elektronického hlasování identifikuje hlasy, které jsou ovlivněny nesrovnalostí.	3
49(a)	Systém potvrdí odevzdání hlasů v časovém limitu	1	Skutečnost, že se hlasovalo v předepsaných lhůtách, by měla být zjištělná.	2
Celkem systém plně splňuje		106	požadavků ze 143.	
To činí splnění		74,13	% požadavků.	
Alespoň částečně splňuje		122	požadavků ze 143.	
To činí částečné splnění		85,31	% požadavků.	
Vyjádřené mírou splnění		114	ze celkových 143.	
To činí		79,72	%.	
		2	. úroveň	
ID	Doplňující požadavek	H	Podrobněji	
50(a)	Hlasovací proces musí nabízet možnost být kdykoli ukončen bez záznamu	1	Hlasovací systém může volič kdykoliv ukončit, aniž by se ukládaly jakékoliv informace ohrožující soukromí voliče.	
50(b)	Bez odkazů na třetí strany	1	Software nesmí umožňovat přístup třetích stran (včetně sociálních médií) ani obsahovat odkazy na programy/stránky mimo infrastrukturu elektronického hlasování.	
50(c)	Systém zajišťuje "věčné soukromí"	1	V rámci věčného soukromí nesmí být umožněno nikdy, včetně vzdálené budoucnosti, prolomit tajnost hlasování.	
50(d)	Systém zajišťuje škálovatelnost	1	Každý volič může odevzdat hlas kdykoliv během doby hlasování bez ohledu na zatížení systému či systémové nároky na odevzdání hlasu.	

Příloha H: Článek Hodnocení i-voting systému pro vzdálené primární volby České pirátské strany

MARTÍNEK, Tomáš a Michal MALÝ, 2024. Evaluation of the I-Voting System for Remote Primary Elections of the Czech Pirate Party. *Acta Informatica Pragensia* [online]. 13(3), 395-417 [cit. 2024-07-28]. ISSN 1805-4951. Dostupné z: [doi:10.18267/j.aip.249](https://doi.org/10.18267/j.aip.249)

Evaluation of the I-Voting System for Remote Primary Elections of the Czech Pirate Party

Tomáš Martínek¹ , Michal Malý² 

¹ Department of Information Engineering, Faculty of Economics and Management, Czech University of Life Sciences Prague, Czech Republic

² Institute of Political Studies, Faculty of Social Sciences, Charles University, Prague, Czech Republic

Corresponding author: Tomáš Martínek (martinekt@pef.czu.cz)

Abstract

The integration of digital technologies into political processes represents a pivotal shift in the operational dynamics of political parties, highlighting an evolution from traditional to digital platforms. This transformation offers greater member engagement and decision-making transparency while also introducing new challenges in terms of security and control. This study presents an analytical overview of the Helios voting system as implemented by the Czech Pirate Party, used not only for primary elections, offering a critical examination of its operational framework, security measures, verification processes, and implications for intra-party democracy and member engagement. The Czech Pirate Party's engagement with Helios exemplifies a broader trend toward digitalization within political organizations, reflecting both the potential benefits and inherent challenges of such technological adoption. Drawing on theoretical insights from the literature on political party transformation in the digital age, this article assesses how i-voting systems like Helios can potentially enhance or detract from internal democracy. The discourse around digital platforms is nuanced, revealing opportunities for increased democratic engagement alongside risks of enhanced centralization and control. Empirical data from a survey of the Czech Pirate Party's membership base provides insights into perceptions of the Helios system's usability, security, and its impact on democratic processes within the party. The study further investigates Helios's technical aspects, focusing on its security protocols, verification mechanisms, and governance structures related to data and platform ownership, to understand its implications for electoral integrity and party governance. The research aims to contribute to the dialogue on e-voting platforms, highlighting the need for a careful balance between embracing technological advancements and upholding democratic principles.

Keywords

E-voting; Remote voting; Internet voting; Czech Republic; Primary election; System evaluation; Helios; Open-Source; Standards; Digital Party.

Citation: Martínek, T., & Malý, M. (2024). Evaluation of the I-Voting System for Remote Primary Elections of the Czech Pirate Party. *Acta Informatica Pragensia*, 13(3), 395–417. <https://doi.org/10.18267/j.aip.249>

Academic Editor: Zdeněk Smutný, Prague University of Economics and Business, Czech Republic

Copyright: © 2024 by the author(s). Licensee Prague University of Economics and Business, Czech Republic.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution License (CC BY 4.0).

1 Introduction

Since the 1990s, political parties around the world have been experiencing an organizational crisis, the biggest symptoms of which are the decline of the membership base and intra-party mobilization (Gerbaudo, 2019). Digital participatory technologies offer a way to easily and cheaply draw citizens' attention to and engage with intra-party events. One such trend is the use of internet-based voting systems for political party personnel elections that include primaries. This trend has been amplified by the COVID-19 pandemic due to the increased need for remote communication.

In the Czech Republic, the Czech Pirate Party uses the Helios system combined with in-house developed systems and other open-source software to organize personnel elections via the Internet for its members (Martínek & Forýtek, 2022). Other Czech political parties, including the Greens and the Mayors and Independents, have also used Internet voting for their primaries. The Public Affairs party used online voting to approve their positions and actions by registered members (Cirhan & Stauber, 2018). The Czech legal system does not exclude the possibility of conducting personnel elections remotely using online tools. Under the Act on Association in Political Parties and Political Movements (Czech Republic, 2024), it is necessary to comply with Section 4, which requires democratic statutes and democratically constituted bodies. Each political party and other entities can adapt their statutes and bylaws to make use of remote electronic voting. The Act (Czech Republic, 1995) regulates elections to the Chamber of Deputies and other public authorities, which exclude the use of remote electronic voting. Within primaries, the primary regulation is the political party's electoral code.

This article aims to analyze the i-voting system of the Czech Pirate Party through the lens of democratic and technical norms using mixed methods. The article is structured as follows: after the introduction, we present a literature review on i-voting systems in political parties, followed by a review on the security analysis of i-voting systems. Subsequent sections outline the research objectives, data, and methods. The results and analysis are then discussed, leading to the discussion and conclusion. This article seeks to enhance the debate on the use of i-voting systems within political parties.

Our primary objective is to evaluate the Helios Voting system in combination with other party systems through analysis and primary research, addressing its benefits, risks, and security issues in the context of Internet voting systems used by the Czech Pirate Party, not only for its personal elections. We aim to evaluate the complex system according to a defined framework and verify the parameters and the entire i-voting system based on user experience. This paper contributes to the ongoing debate on voting systems in political digital parties (Deseriis & Vittori, 2019; Gerbaudo, 2019; Vittori, 2019).

The specific objectives of this study include describing the use of electronic voting systems by Czech parliamentary parties, with a detailed description of the system used by the Czech Pirate Party; evaluating voters' perceptions of remote electronic voting and its impact on intra-party democracy within the Czech Pirate Party; and contributing to the academic and practical discussion on the advantages and disadvantages of i-voting systems.

1.1 Theoretical background on the use of voting systems in intra-party democracy of political parties around the world

The first use of Internet voting in a primary election is considered to be the 2000 US Democratic Party presidential primary in Arizona (Solop, 2001). In Spain, at least 12 political groups, including Citizens, Comuns, CUP, Democrates, TEAM, ERC, ICV, JxCAT, Podemos, PSOE/PSC, SI and UPyD, have used the internet for their staff elections. Spain's intra-party democracy is regulated only very generally, with no minimum requirements for electronic voting systems. Article 6 of the Constitution recalls that political parties 'express political pluralism, participate in the formation and expression of the will of the people and are an essential instrument of political participation'. As a counterpart to such activities, the

Constitution emphasizes that "its internal structure and functioning must be democratic" (Barrat i Esteve, 2022).

The parties Podemos (Mikola, 2017) and Compromís used the nVotes voting system, as did the Norwegian political party Sosialistisk Venstreparti (Agora Voting, 2023). France makes a strong distinction between state-organized voting (referendums and elections) using only paper and other types of voting-related to internal representation in private companies, trade unions, political parties, or institutions, which can also take place remotely electronically. As of 2017, at least 245 companies and institutions have used the Neovote system in France for internal elections. In the primary party election of the French presidential candidate, 3 of the 5 main political parties used the Neovote system. Those are the primary for Les Républicains, the Primaire de l'Ecologie, and the Primaire Populaire (Blanchard et al., 2022). In France, Neovote clients also include the Mouvement démocrate, En Marche! and the Parti radical valoisien (Neovote, 2024).

The implementation of i-voting systems within political parties can be categorized into two groups. The first group consists of parties that have adopted i-voting systems in response to a crisis, typically poor electoral outcomes. These are generally traditional social democratic and socialist parties (Musella, 2023; Raniolo & Tarditi, 2020). The second group consists of so-called digital parties, which have utilized i-voting systems since their inception (Gerbaudo, 2019). Digital parties are characterized by replacing traditional organizational structures with online participatory platforms and communication. They aim to replace traditional local branches with online meetings, simplify party membership through online registration, and enable all registered members to vote on internal party matters. The digital infrastructure aims to reduce the costs of party organization and attract new members. Examples of these parties include the aforementioned Podemos and the Movimento 5 Stelle.

However, current research shows that although Podemos initially presented itself as an inclusive protest party, the ability of members to propose any initiatives for intra-party voting was severely limited due to the high threshold (support from 10% of the membership base) (Deseriis & Vittori, 2019). In Italy, the Movimento 5 Stelle (Von Nostitz & Sandri, 2021) is a political party known for its use of online voting, but it has faced criticism due to its lack of transparency and the complex architecture of the system that precludes horizontal interaction between users (Mosca, 2020). Furthermore, the platform is managed by an external company, and the party has no control over it (Deseriis, 2017).

1.2 Theoretical background on the use of voting systems in the intra-party democracy of Czech political parties

In the Czech Republic, the Czech Pirate Party has been using the PhpBB forum since its inception, which since 2016 has gradually been replaced by the Helios Voting system linked to other party information systems (Martínek & Forýtek, 2022). The Greens used the Belenios system (Jebavá & Masare, 2020), thus building on the European Green Party standard (Lanzone & Rombi, 2018). Mayors and Independents for the 2021 primary election used the electronic voting system Polls built on NextCloud, which would hardly meet the basic requirements for vote secrecy because it stores votes in an unencrypted form in the database.

Historically, among the parliamentary parties, we can also mention Věci veřejné, which used a system managed by NetServis for Internet voting (Kopecký, 2010). In the context of the personal election of the party chairman, approximately 800 supporters out of approximately 6,000 voted in 2012 (Husarová & Hromádka, 2012). In 2011, the TOP 09 party allowed delegates to vote for the party chairmanship via an electronic system with a tablet-based voting system (TOP 09, 2024) in order to eliminate errors when filling out the ballot (TOP 09, 2011).

During the COVID-19 pandemic, the Green Party used an official installation of the Belenios system for the staff elections, using members' e-mail addresses to prepare the voter list (Jebavá & Masare, 2020). Belenios (Cortier et al, 2019), which is based on the Helios Voting source code, also has some shortcomings (Baloglu et al., 2021a), which the active development and academic community is trying to address (Baloglu et al., 2021b).

1.3 Theoretical background on security analysis of i-voting system

Although the COVID-19 pandemic necessitated much greater use of remote communications, the development of remote electronic voting has taken place in lower-profile elections rather than in nationwide, politically binding elections. Currently, secret remote electronic voting is being used in elections for academic institutions, associations, commercial companies, cooperatives or political parties. Electronic voting is constantly addressing various cryptographic challenges (U.S. Vote Foundation, 2015), security threats (Beurdouche et al., 2017), or balancing conflicting demands such as the requirement for election integrity while ensuring voter privacy. Verifiability schemes for i-voting systems are examined in terms of usability and user experience by Marky et al. (2021). The procedural components of i-voting systems in Estonia, with an emphasis on controls related to procedural security mechanisms and measures to ensure system transparency, are examined in Nurse et al. (2017). The importance of transparency of i-voting systems is examined in a study by Agbesi et al. (2023).

In the context of secret electronic voting over the Internet, there are many parts of the entire voting system that need to be trusted and secured - from the voter's device, to the network infrastructure, to the voting system itself, including the actors involved. If a breach of integrity through an attack on the system is not discovered until after the results have been announced, it is very difficult to remedy the situation. Remote voting takes place in an uncontrolled environment where voter influence can more easily occur. Historical experience with attempts to influence the results of traditional (Transparency International, 2014) and electronic elections (Wolchok, 2012) is a constant reminder of the importance of the need to continuously improve security measures throughout the system (Bernhard et al., 2012), where a breach of integrity could have significant impacts on the whole society.

In order to increase voter confidence, it is important to evaluate the voting systems themselves and the procedures by which the election is conducted. Even so, only a few papers have addressed the evaluation of voting systems. In 2015, the IEEE did reactivate the 1622 Committee on Voting System Standards (Wack, 2014), but the result was only a set of recommendations. The Council of Europe produced Recommendation CM/Rec(2017)5 on e-voting standards (Council of Europe, 2017), which is non-binding for members, including the Czech Republic. To date, the Council of Europe e-voting standards remain the most important intergovernmental resource in this area. While these recommendations are not binding, several Council of Europe member states, such as Norway and Switzerland, have voluntarily adopted them. In Estonia, these standards have been referred to by the Supreme Court, while in Belgium they have been used as a benchmark in the evaluation of e-voting. The Committee of Ministers of the Council of Europe adopted the updated standards on 14 June 2017 under CM/Rec(2017)5 (Rodríguez-Pérez, 2022).

The Helios Voting system (Adida, 2008), which is also used by the Czech Pirate Party, has been evaluated from a cryptographic point of view by academics (Marcos del Blanco & Gascó, 2019; Panizo Alonso et al., 2018), who, however, focused only on a general evaluation of the software without evaluating the specific deployment of the system, which may be additionally modified for individual implementations.

In addition to the cybersecurity of the software itself, i-voting systems should be evaluated comprehensively in terms of ensuring the integrity of the entire election as stated by Garnett & James (2020) who define three basic principles for evaluating electoral integrity: opportunities for deliberation, equality of participation, robust electoral management quality. This paper focuses on a comprehensive evaluation of the actual implementation of the system including technical standards, regulations, and

fulfillment of democratic norms, which greatly expands the evaluation of the software alone to include an evaluation of electoral integrity not only from a technological perspective. The evaluation of a specific use case involving the whole selection process is described by von Nostitz and Sandri (2021).

2 Data and Methodology

The paper uses both qualitative and quantitative approaches for its analysis. Within the qualitative approach, the Helios application in the version used by the Czech Pirate Party will be analysed on the basis of materials from developers, professional articles, party statutes, internal party regulations, testing the system by organising its own voting and examining the source code of the application. The quantitative analysis will be based on data from a questionnaire survey conducted on a sample of 213 members and data from 207 intra-party votes.

The paper will use the analytical framework of von Nostitz and Sandri (2021) for its analysis. In their analysis of Podemos and the Movement of 5 Stars, they divide the analysis of voting platforms into two parts: democratic norms and technical standards. Democratic norms contains 5 indicators that, according to the authors, allow understanding the limits and possibilities of participation in the decision-making process. These are specifically participation, representation, competitiveness, transparency and responsiveness. Technical standards contain 4 indicators, namely: security, verification process and secrecy, data ownership and control. For each indicator, the results of both quantitative and qualitative analysis will be used. Using this methodology, it will be possible to comprehensively understand the digital democratic affordance of the i-voting system (Deseriis 2023).

2.1 Case description

The Czech Pirate Party, founded in 2009, has established itself as a notable political entity in the Czech Republic, emphasizing transparency, direct democracy, and digital rights. The party employs digital tools and online voting systems to enhance internal democracy and member participation.

Research highlights the party's strategic adjustments following its entry into the Chamber of Deputies in 2017. These adjustments involved refining their digital participatory practices to better engage voters and streamline internal decision-making processes (Šárovec, 2019). The party's use of online platforms for congresses and internal deliberation is noted for broadening participation, although it presents challenges in maintaining effective deliberative processes (Šárovec, 2022).

An analysis of the party's deliberative practices during the coalition formation in Brno in 2018 reveals both strengths and limitations. The study indicates that while the Czech Pirate Party promotes inclusive dialogue and collective decision-making, it faces challenges in ensuring all voices are effectively heard within its digital framework (Vodová & Voda, 2020).

Additionally, the party's rise in popularity and its impact on Czech politics can be attributed to its innovative practices and commitment to transparency. This commitment includes enabling broader member participation in decision-making through digital tools, which has helped maintain a tech-savvy and engaged electorate (Mortkowitz, 2019). In 2019, the party entered the European Parliament (Pink & Folvarčný, 2020). Currently, the party is represented in the government, Senate, House of Commons, European Parliament, as well as at the regional and municipal level.

Overall, the Czech Pirate Party represents a significant case of integrating digital tools into political processes, enhancing internal democracy, and engaging with a digitally-oriented voter base, making it an important subject of study in the context of political science and digital democracy (Šárovec, 2019; Vodová & Voda, 2020; Mortkowitz, 2019).

2.2 Data collection

A quantitative approach was used in this study across several datasets. In order to evaluate the impact of the digitization of decision-making processes on intra-party perceptions, an anonymous questionnaire survey was conducted among members of the Czech Pirate Party with the approval of the Bureau of the Czech Pirate Party. The draft questionnaire was tested with a group of respondents before it was finalized and, based on the findings, was modified into its final form. For the survey, the *ankety.pirati.cz* platform was used, based on the LimeSurvey application, where only Pirate Party members had access to the survey via a unique URL sent in an e-mail invitation that allowed members to fill out the questionnaire once. Responses to the survey were voluntary and anonymous, as stated on the survey homepage and in the email invitation. The poll ran from 22 February to 14 March 2024. 213 members out of a total of 1,179 party members completed the 19-question poll in full, a response rate of 18.6%. 16 research questions were Yes or No answers, 3 questions were socio-demographic questions focusing on gender, age and educational attainment.

Table 1. Data on respondents.

Data	Category	Number	Percentage
Gender	Women (F)	47	22,07 %
	Man (M)	146	68,54 %
	No answer	20	9,39 %
Age group	18-30 years old	27	12,68 %
	31-50 years old	93	43,68 %
	41-50 years old	56	26,29 %
	51-60 years old	24	11,27 %
	61-70 years old	11	5,16 %
	71 years and over	2	0,94 %
Highest completed education	High School	60	28,17 %
	Bachelor's	27	12,68 %
	Master's	97	45,54 %
	Doctoral	13	6,1 %
	Other	6	2,82 %
	No answer	10	4,69 %

All members of the Czech Pirate Party were invited to participate in the questionnaire; given the low number of members, the representativeness of respondents to the entire population is not addressed. Detailed survey results by question are in Appendix A. For further findings, the aggregated groups of answers for the given questions were analysed in relation to the answers to other questions. The research

method of descriptive statistics with numbers is used for the results. The data are aggregated and then interpreted verbally. Survey results are presented as percentages rounded to one decimal place.

In order to identify specific concerns and complaints about the system, on 2 June 2024 Pirates were asked to fill out an anonymous questionnaire on the *ankety.pirati.cz* platform with 4 open-ended questions on the Pirate Forum and in the Pirate communication application Zulip. Specifically, it was to elaborate on the reasons for questions 12, 15, 16 from Appendix A and one question to freely define possible concerns. By 12 June 2024, 22 critical responses were submitted, the main findings of which are paraphrased in the overall evaluation subsection.

Furthermore, an analysis of the voting history of the national Pirate Forum via the Helios system in the years 2017-2023, since the Czech Pirate Party entered the Chamber of Deputies, is used. The analysis follows both types of voting, i.e. personal elections and referendums. Personal elections include elections for party bodies, expert unions and candidates for elections. Referendums then include areas such as changes to the statutes, programmatic positions or joining a coalition. The analysis focuses on turnout in intra-party voting. Due to the large number of votes ($n = 207$), the data will be averaged for each year. The aim is to see if the quality of the vote (Deseriis, 2021) is sufficient to keep the average turnout stable over time.

2.3 Methodology for evaluating election turnout

Turnout (T) for each voting event is calculated using the following formula:

$$T = \left(\frac{V}{M} \right) \times 100 \quad (1)$$

Where:

- T is the turnout in percentage,
- V is the number of voting members,
- M is the total number of eligible voters (members).

To calculate the average turnout (T_{avg}) for the entire year:

$$T_{avg} = \frac{\sum_{i=1}^n T_i}{n} \quad (2)$$

Where:

- T_i is the turnout for the i -th voting event in the given year.
- n is the total number of voting events in the given year.

Turnout is calculated as the percentage of voting members out of the total number of eligible voters for each individual voting event. For each year, turnout is averaged separately for personal (denoted in Figure 1 primary) elections and referendums (denoted in Figure 1 consultations). Average turnout is a key indicator of party members' participation in voting. Higher turnout may indicate higher member engagement and higher adoption of the electronic voting system. Conversely, low turnout may indicate the need for adjustments in the system or in the approach to member mobilization.

The trend in turnout determines whether the participation of Czech Pirate Party members in intra-party voting shows an increasing, decreasing or stable tendency during the analysed period. A linear regression (Montgomery & Runger, 2010) is used to calculate the turnout trend, where the independent variable (x) is the years and the dependent variable (y) is the average turnout (T_{avg}) for each year. The linear regression equation has the form:

$$y = a + bx \quad (3)$$

Where:

- y is the average turnout,
- x is the year,
- a there's an intercept,
- b is the slope, which represents the change of the tour per unit time (year).

The regression coefficients a and b are calculated by the following formulae:

$$b = \frac{n\sum_{i=1}^n (x_i y_i) - \sum_{i=1}^n x_i \sum_{i=1}^n y_i}{n\sum_{i=1}^n x_i^2 - (\sum_{i=1}^n x_i)^2} \quad (4)$$

Where b tells whether turnout is increasing or decreasing on average each year and a :

$$a = \frac{\sum y_i - b \sum x_i}{n} \quad (5)$$

Where:

- n is the number of years,
- x_i is the i -th year,
- y_i is the average turnout in the i -th year.

2.4 Methodology for assessing the correlation between questions

Correlation analysis (Lee Rodgers & Nicewander, 1988) was used to analyse the dependencies between the questions in the dataset (Martínek & Malý, 2024). Yes responses were converted to a value of 1 and No responses to a value of 0. The correlation matrix was calculated using Pearson's correlation coefficient (Pearson, 1895). This coefficient measures the strength of the linear relationship between two variables. The resulting coefficient can take values from -1 to 1, where:

- 1 means perfectly positive linear dependence,
- 0 means no linear dependence,
- -1 means perfectly negative linear dependence.

The formula for the Pearson correlation coefficient r is:

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}} \quad (6)$$

Where:

- n is the number of pairs of values,
- x and y are the individual values of the two variables.

To interpret the results, a heatmap of the correlation matrix for the 16 research questions from the dataset is used to provide an overview of the interdependencies between the responses, which are numbered in order from Appendix A. The Pandas 1.4.0 library for the Python programming language was used for data analysis, and the heatmap was generated using the Python library Matplotlib 3.4.3 using the Seaborn 0.11.2 library.

3 Results and Analysis

3.1 Evaluation of the election process by the Helios Voting system of the Czech Pirate Party

Prior to the implementation of the Helios Voting system, the Czech Pirate Party used a polling system integrated into the phpBB discussion system, where the votes cast are not encrypted in any way and anyone with access to the database could see how each member voted. Currently, this polling system is only used to get nomination support and other less important votes. All major votes involving the election of the Bureau and members of other party organs, primary elections to fill nomination lists, recalls from Pirate Party elected positions, or referenda to change the constitution and the like are already conducted on the Helios Voting system, which uses homomorphic encryption to ensure the secrecy of the vote (Adida et al., 2009). The National Forum elects its candidates for the Euro elections, candidates for the post of Euro Commissioner, President or for the Pirate Party International organs in the primaries. Regional forums elect candidates for regional elections, parliamentary elections, senate, or nominees for national party bodies, or they can use Helios for local association primaries.

3.1.1 Regulations

Most party regulations, from the statutes to the election rules, are written without regard to the method of election, whereby an online election must be accommodated in the same way as a traditional paper-based election. The bylaws only briefly mention that voting shall be done electronically, by correspondence if possible, and with an extended voting period. The Rules of Procedure issued by the Republic Committee mention the basic requirements for Internet voting. The regulation that specifically establishes Helios as the system for secret ballot elections is the Decree on the Proceedings of the National Forum issued by the Party's Administrative Department. The Helios system is set out in the Principles for Secret Ballot Voting, including other basic requirements for the voting procedure. These are not detailed security requirements, as the policy originally regulated only unencrypted voting through a poll at the forum. All party regulations are available on the Pirate Wiki (Martínek & Forýtek, 2022).

3.1.2 Democratic norms for i-voting

Participation: The largest number of voters participated in the second round of the 2021 Helios election for party chairman in the personnel elections, with 948 members voting out of 1,232 voters and a 76.9% turnout. The largest number of voters in any election was in the 2021 Cabinet approval process, where 1,082 voters out of 1,193 participated with a 90.7% turnout.

Between 2017 and 2023 (since the Czech Pirate Party entered Parliament), 207 national votes have been launched. Of these, 118 were referendum-type votes and 89 were personnel-type votes. The overall average turnout was 34.22%, 30.66% in referendum-type votes and 38.95% in personal elections. Average turnout in both types of votes has been increasing over time. Thus, participation is stable or not declining over time, which was a problem for Podemos and Movement of 5 Stars, which experienced an initial boom and then participation declined (Deseriis and Vittori, 2019).

Party members are admitted by local associations after a public vote of the respective Bureau. The identity of party members is verified by regional coordinators and other authorized persons during physical meetings by checking ID cards or other identification. In view of the establishment of both the eDocuments digital ID card and the NIA (National Identification Authority) in the Czech Republic, there are demands among members to digitise the identity verification process.

Helios is compliant with Web Content Accessibility Guidelines 2.0 A (Marcos del Blanco & Gascó, 2019), which should allow visually impaired voters to vote independently. However, Recommendation CM/Rec(2017)5 (Council of Europe, 2017) requires WCAG 2.0 AA level of usability (W3C Web

Accessibility Initiative, 2023), which could be improved by modifying the design of the actual installation. In the questionnaire survey, 86.9% of members found the Helios voting system intuitive. The Pirates provide additional documentation to members on the website, including voting instructions, and the Pirate Party's system is translated into the official - Czech language. In terms of election typology, Helios only allows for elections based on vote counting, which excludes some alternative voting methods, as offered by the Belenios system.

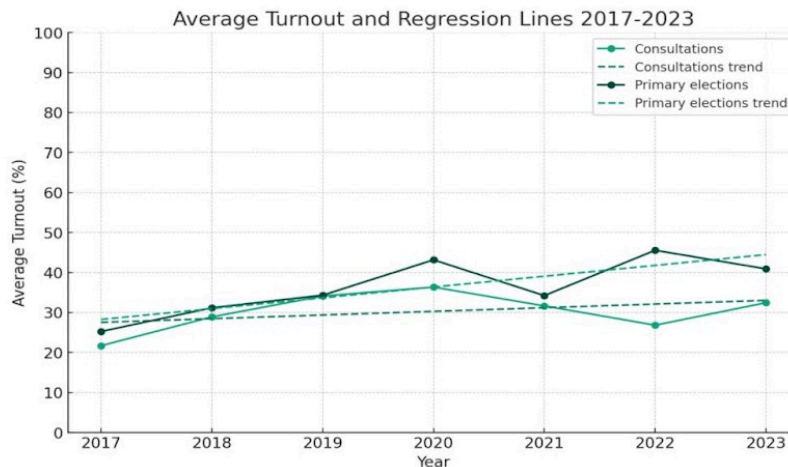


Figure 1. Average voting participation of Czech Pirate Party members by year and type.

Representation: All party members have the right to vote in national votes. Direct democracy thus allows the opinion of every member to be recorded, regardless of socio-demographic data. Any member can stand for election, just as any member can nominate a non-member for the primary. Although the party is male-dominated, with over 68.5% of men participating in the questionnaire survey, four women were elected in the most recent election of the five-member presidency, indicating that the electoral process does not impose barriers on the underrepresented gender. In the 2021 parliamentary elections, the average age of the candidates of the Czech Pirate Party was the lowest of all parliamentary political parties, remaining below 40 years, which was more than 9 years lower than the overall average of all parliamentary political parties and movements (Boček et al., 2021). The low average age of party members is also demonstrated by the questionnaire survey, where 56.3% of respondents are in the under 40 age category. The Czech Pirate Party does not use a quota system in voting. The average age of the survey participants is also mainly among the young and middle generation. University graduates are also over-represented among Pirate Party members compared to the average Czech population, with over 64.3% of respondents having completed a university degree. Visually impaired or otherwise disabled voters should be able to vote independently in online voting. In order to receive a nomination, candidates must by default receive the support of a group of members, the size of which is calculated according to the following formula:

$$a = 2 * \sqrt{x} \quad (7)$$

Where:

- a represents a required number of the group of members who supports the proposal,
- x represents a total number of members of the district (Martínek & Forýtek, 2022).

Competitiveness: Each candidate must supply a publicly available candidate speech along with the acceptance of the nomination, as well as have basic information about themselves completed. No funds are provided to candidates in intra-party primaries. Candidates may present themselves at public candidate introductions or on their own. During the election, a list of all candidates is displayed on the Helios home page with links to their candidate speech and a personal medallion including a photo. The list of candidates in the election part of Helios is sorted randomly for each voter.

In order to mitigate the risk of pressure and corruption, the Pirates allow the ballot to be cast repeatedly until the election is over. Only the last vote cast is counted in the final results. However, according to the evaluation with recommendation CM/Rec(2017)5 (Council of Europe, 2017), the system is not resistant to coercion. As of February 2024, Pirates has deployed its own modification of the Helios system, which, while still displaying the voter list during voting, only displays the voting hash for the registered voter during the ongoing voting. As a result, information about the participation of individual members is not displayed until after the voting has ended, which is intended to reduce pressure on non-voting members.

In the questionnaire survey, 63.9% of Pirates consider it appropriate in terms of credibility that a list of voters with information about their participation be publicly available. 91.1% of respondents said they were aware of the possibility of re-voting, 81.2% of respondents used re-voting. 24.4% of respondents voted in the presence of a third person who could see the selected choice, only 2.4% of respondents voted according to the preference of the third person in their presence. 21.6% of respondents allowed themselves to be influenced by a third person when voting.

Transparency (and accountability): The foundation of open-source Helios systems is verifiability, where secrecy is ensured by homomorphic encryption. Currently, there is no formal, universal definition for E2Ev: End-to-End Verifiability because the associative and commutative operators are inaccessible to symbolic analysis tools, which for example makes it impossible to analyze the following homomorphic property as stated in (Cortier, 2015):

$$enc(pk;v_1) * enc(pk;v_2) = enc(pk;v_1+v_2) \quad (8)$$

where $*$ and $+$ are associative and commutative operators. Thanks to them it is possible to sum the contents of votes (v_1 and v_2) encrypted (enc) with public key (pk) without further decrypting them individually.

Voting on the Helios platform normally runs from 10:00 am on Friday to 8:00 pm on Monday, except during the physical meetings of the national forum, when voting normally runs for an hour. Election administrators may cancel and re-announce the poll based on a discovered error or other concerns before the polls close. In the questionnaire survey, 61.5% of respondents said that the transparency of the electoral system, including access to the source code, was important to them in terms of trust.

Responsiveness: The Pirates practice direct democracy, the results are accepted by the party leadership and valid. The party's administrative department is responsible for the implementation of the results and verifies that the elections are carried out in accordance with the regulations. The standard option is the process of objecting to the presiding officer's procedure, whereby the immediate objection is decided by consensus or by a counted vote. If the objection is rejected, or if, on the other hand, the inaction of the responsible authorities appears arbitrary to some, they can appeal to the party's arbitration committee to rule on the validity of the legal act. If someone suspects manipulation of the voting system or other electoral fraud, he or she may take the complaint to the Party's Audit Committee, which should gather evidence and refer the matter to the Party's Arbitration Committee for a decision. In the context of a primary election, one can also approach the party's Republican Committee, which is in charge of electoral supervision and can make a political decision to modify the candidate list. All decisions are then subject to possible extraordinary review by the national forum. In addition to the primary elections, the Pirates also allow other votes, including the possibility of recalling elected candidates or voting on the invalidity of an election.

3.1.3 Technical standards for i-voting

Security: The servers where the *helios.pirati.cz* installation runs are under the control of the party, the TLS certificate from Let's Encrypt is used for encrypted connections, the source code of the system is transparently published on the pirate Gitlab (Martínek & Forýtek, 2022). For higher credibility, the voter list is publicly accessible - after the election is over and with information about the voter turnout, which is contrary to the recommendation CM/Rec(2017)5 (Council of Europe, 2017). The system is vulnerable to attacks on the voter client, network infrastructure and phishing etc. (Bernhard et al., 2012). On the other hand, it is a low-volume and lower-impact voting system; voting can also be postponed, which, for example, in the framework of the CNIL recommendation (La Commission nationale de l'informatique et des libertés, 2019), sets a medium level 2 risk level and thus less minimum security requirements for an Internet voting system. The academic origin of Helios has subjected the system to independent audits by the public and academic experts (Marcos del Blanco & Gascó, 2019).

According to the author of the system (Adida, 2008), Helios Voting is applicable for elections with low risk of corruption or other manipulation and low number of voters, specifically, a limit of around 1000 voters is given, although after adding additional resources the Helios system managed to process over 4000 votes during the 2009 University of Leuven elections (Panizo Alonso et al, 2018). The Czech Pirate Party has almost 1 200 members with the right to vote, and only one vote exceeded 1 000 voters, specifically the party's system managed to process the results for 1 082 votes cast to approve participation in the government. As part of the design of the election process, there is the possibility of dividing voters into smaller groups, for example by region, thus allowing more voters to vote according to designated districts, where the results can then be published simultaneously so that the groups are not influenced by each other.

Helios does not allow you to submit a wrongly filled in ticket. On the other hand, the Pirates retain the option to cast a blank ballot, which is considered a legitimate expression of the voter's will. In the questionnaire survey, 53.1% of respondents said they understand the way votes are encrypted and privacy is ensured in the Helios system, with only 13.2% concerned about breaking the secrecy of the vote. Interestingly, 47.4% of voters would not mind if someone revealed how they voted.

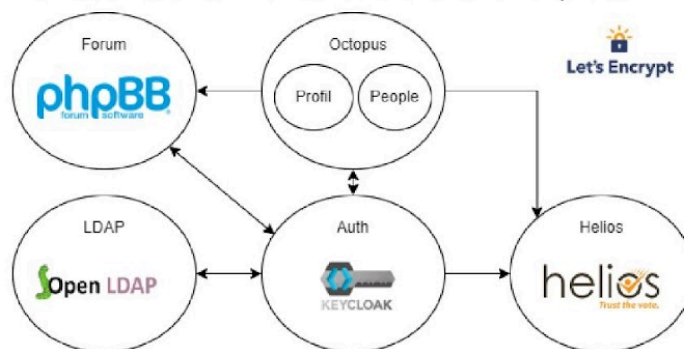


Figure 2. Simplified scheme of the i-voting system of the Czech Pirate Party. Source: (Martínek & Forýtek, 2022).

Verification process and secrecy: As part of eligibility, the Czech Pirate Party allows members to vote on the Helios system, which it uploads to the voter lists via an API connection from its own Octopus system, where an up-to-date register of members - eligible voters - is maintained. For authentication, members log in via the Single-Sign On system Keycloak (Martínek & Forýtek, 2022), where they can also enable two-factor authentication. Voting information is sent to the party email alias *name@pirati.cz*, which forwards the mail to the member's private email.

Helios has a cast-or-audit approach for casting as intended, i.e., the voter can check his vote as many times as he wants until he is convinced that Helios is trustworthy. For being recorded as cast, the voter receives a hash of his encrypted vote, which he can later check in the electronic ballot box. The party uses the current version of Helios version 3 with custom modifications (Bernhard et al., 2011). Since Helios version 2 (Adida et al., 2009), exponential El Gamal with homomorphic property is used for encryption. Finally, for the recorded state, ElGamal along with the Sako-Kilian mixnet (Sako & Kilian, 1995) are implemented Zero Knowledge Proof (ZKP). As a result, Adida concludes that Helios is E2Ev (Adida, 2008) if the ballot box and the voting authorities are honest. Otherwise, either party could irregularly add votes (Marcos del Blanco & Gascó, 2019).

An example of a website with published election results is shown in Figure B1 of Appendix B. In the survey, only 31% of party members actually verify the presence of the displayed tracking code in the publicly accessible electronic ballot box.

Data ownership: the Helios system is provided free of charge without any guarantees based on the Apache 2.0 license, so the party has only the costs of implementation, operation and maintenance of the system on its servers. The party manages the personal data of its members through a self-developed Octopus application. The party states that it handles personal data in accordance with the GDPR, with the head of the administrative department (Pirates, 2022) as the proxy. After decryption, the aggregated election results are displayed to all voters.

Control: Votes are encrypted by default with the Helios Voting system, which then uses ElGamal homomorphic encryption (Pereira, 2016) to keep the vote secret, allowing the overall result to be calculated without having to decrypt individual votes.

As part of the shared responsibility, the Pirates always use at least 3 party members as trustees for the national vote, who together with the election server generate their own keys needed for the final decryption and verification of the overall result. For county forum elections, the multiple trustees rule is not always followed, which increases the risk of privacy breaches as well as reducing credibility.

The system runs on a server controlled by the party, which is located in the Czech Republic. Access to the server is restricted to system administrators who have been authorised by the head of the Party's technical department. The server is backed up. In the questionnaire survey, 89.2% of members are satisfied that the Helios system is managed directly by the party.

3.2 Overall evaluation of the Czech Pirate Party's i-voting system

Overall, the Pirates rate the Helios system for their online voting positively, specifically 96.2% of respondents believe that the Pirates should continue to allow electronic voting through the Helios system. 93% of respondents believe that their participation would decrease if online voting were replaced with traditional paper voting during national or regional forum meetings. 98.6% of respondents believe that remote electronic voting facilitates their intra-party functioning.

Other interesting findings include that 71.4% of respondents who are concerned about breaking the secrecy of the vote do not understand the way the vote is encrypted in Helios. On the other hand, only 44.2% of those who are not worried about breaking secrecy do not understand the vote encryption system. This indicates the importance of the need for sufficient awareness of the operation of the system. Furthermore, respondents (3.8%) who do not want to continue using the Helios system from 87.5% do not find the system intuitive and do not understand the way of vote encryption in the Helios system. Thus, in addition to sufficient awareness, the User Interface of the system could also be improved.

The Helios system is based on all actors taking the maximum possible steps to verify their actions to ensure the integrity of the election. The fact that only 31% of the members performed at least one verification of the presence of a tracking hash in the ballot box may increase the risk of vote manipulation.

The open-ended responses also repeatedly request that alternative voting methods be made available, which, unlike the newer Belenios system, Helios does not offer. In terms of intuitiveness, respondents criticise that voters are often unaware of the option to cast a blank ballot, which is essentially a vote against all options. Elections with only one voting option often end successfully for that option. Respondents are also concerned about breaking so-called perpetual privacy (Haines et al., 2023), as the system displays a permanent tracking hash next to the voter's real name in the publicly accessible ballot box. With the increasing power of quantum computers, the asymmetric cipher could be broken in the future (Bavdekar et al., 2022), which would allow the ballots in the electronic ballot box to be declassified. Critical respondents of Internet voting are also concerned about possible vote manipulation. Respondents also condition the operation of the voting system aside from sufficient transparency.

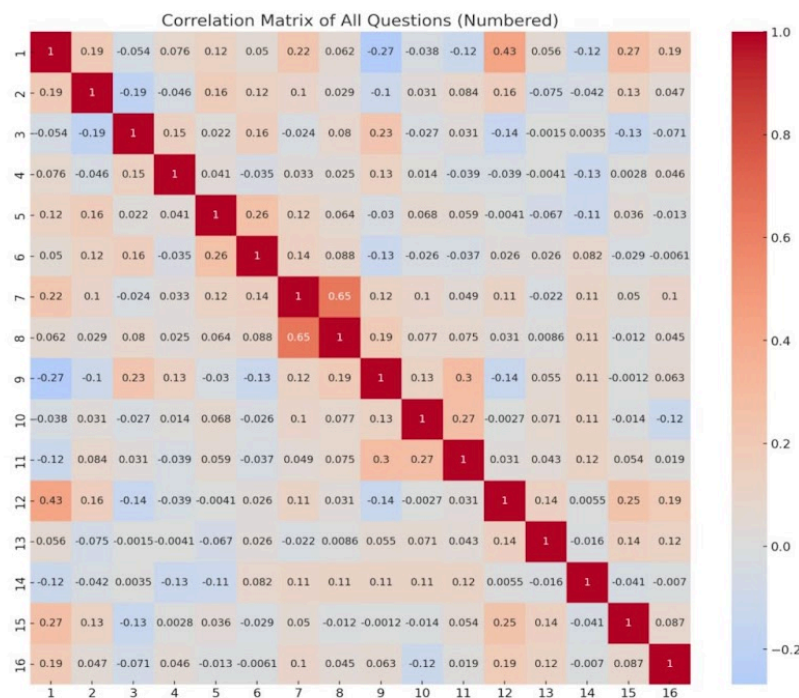


Figure 3. Correlation matrix of questions numbered in order from Appendix A.

In the correlation analysis, there is a strong positive correlation of 0.65 between awareness of the possibility to vote repeatedly and the actual use of this possibility. Respondents who find the system intuitive often support the continuation of e-voting, as reflected by a correlation of 0.43. There is a correlation of 0.3 between questions focusing on choice in the presence of a third person and choice according to the third person's wishes. A recommendation might be to add a disclaimer at the beginning of the choice that the choice of options must be made independently without the presence of a third person. The perceived importance of the transparency of the voting system is moderately correlated (0.26) with the verification of the tracking code after the vote is cast.

To assess the integrity of the entire electoral system of the Czech Pirate Party, the Garnett & James (2020) framework can be used, which assesses three main principles. Within the Deliberative Opportunities principle, it can be said that each candidate in the primary elections has the opportunity to promote

himself or herself in the candidate and nomination speeches, where direct communication with voters is possible through the Forum. The Pirates do not put barriers to candidacy, every member has the right to nominate anyone and anyone who gets enough support gets the opportunity to run.

Under the principle of Equality of Participation, the election can be said to be direct, which ensures the right to participate for every member of the Forum. The announced election through the Helios Voting systems within the digital party, taking place at predetermined times, ensures that the election is accessible to all voters with access to the Internet. With i-voting, similar to other voting systems, potential security risks are present, including concerns about vote tampering, etc.

Under the third principle of Electoral Management Delivery, it can be stated that the method of election seeks to be as transparent as possible. Even to the extent that displaying real names in the public ballot box may compromise privacy. On the one hand, the system makes it impossible to cast an invalid ballot by mistake; on the other hand, cases have been reported with the Helios system (Acemyan et al., 2014) where the ballot is not completed even though the voter believes that he or she has cast the ballot. Universal verifiability should provide a mathematical proof to guarantee the correct counting of the votes cast (Adida et al., 2009). The system used entails low implementation and operation costs only within the party's own technical department staff and the hardware used.

In general, the answers to the three basic questions of adoption, ownership and contingency planning defined by Garnett & James (2020) can also be stated, where the Helios Voting technology is known to be combined with other party systems, where the party is the operator of the technology and the owner of the resulting data, and where any voter has the ability to contest an election in the event of a technology failure or malfunction, just as the party's administrative department can call a rerun election.

4 Discussion

In the Czech Republic, political parties that emphasize direct democracy and greater member participation are trying to make intra-party elections accessible through online voting. Parties such as ODS, Freedom and Direct Democracy, ANO 2011 and others continue to let national staff elections be decided indirectly by delegates through traditional paper ballots or by appointment based on leadership decisions. Also because the Czech Pirate Party does not use a quota system in voting, nor does it create any inclusive space for minorities (Lupato and Meloni, 2023), it is a relatively more inclusive system compared to Podemos or the Movement of 5 Stars, which allows members to be more actively involved in intra-party affairs (Deseriis and Vittori, 2019).

Due to the open source nature of the Helios system, it has been subjected to several security analyses (Adida et al., 2009; Bernhard et al., 2012; Acemyan et al., 2014; Marcos del Blanco, Gascó, 2019), and although the system has its shortcomings (Baloglu et al., 2021), it performs well for smaller elections with fewer voters (Panizo Alonso et al., 2018). The downside remains that the Helios system is no longer under active development and academics have focused on developing other open source voting systems such as Belenios or have moved on to developing commercial voting tools.

Voting systems for intra-party democracy of political parties and movements are regulated in a very limited way. One exception is France, where internet voting systems are subject to minimum requirements from the CNIL (La Commission nationale de l'informatique et des libertés, 2019). Countries such as Switzerland and Estonia have adopted regulations for internet voting, but these primarily apply to national politically binding elections (Von Nostitz et al., 2021). In contrast, laws in Germany do not allow for internet primary elections of political parties without traditional paper confirmation, as the requirements from national politically binding elections are transferred to intra-party democracy (Fitzpatrick & Jöst, 2022). Furthermore, Recommendation CM/Rec(2017)5 on standards for e-voting applies to members of the Council of Europe (Council of Europe, 2017). The importance of adhering to the

standards is compounded by the fact that, as in some municipalities in Canada, online voting is the only possible channel of election for Pirates (Essex & Goodman, 2020).

The lack of legislation regarding compliance with mandatory minimum standards for political parties' online voting systems increases the risk of vote manipulation and the number of security threats, as election organizers are not forced to transparently publish the source code to verify the correct functionality of the system, ensure monitoring, auditing, or other security analyses. Basic security analyses are only possible when using open source systems such as Helios Voting (Panizo Alonso et al., 2018) or Belenios (Cortier et al., 2020), or when developers actively collaborate, as in the case of Scytll's iVote (Marcos del Blanco, Gascó, 2019) or nVotes (Marcos del Blanco et al., 2020), or based on election observation data such as Neovote (Blanchard et al., 2022), where it can be inferred from the observation itself that the Neovote system does not meet the CNIL requirements (La Commission nationale de l'informatique et des libertés, 2019). Based on recommendation CM/Rec(2017)5 (Council of Europe, 2017), a baseline assessment of the entire electoral process can be made, although it is difficult for the evaluator to answer whether all requirements are met (Brunet & Essex, 2023).

Collaboration with academics and other cryptography experts is essential to verify that the system works as intended and that the results match the reality of the vote. Even if it is only an intra-party primary, the consequences of a breach of voting integrity can be similar to those of a political national binding election. For example, if a major political party were to select a presidential candidate through an intra-party vote, a person who does not actually have the support of his or her own political party could become president in the event of an electoral victory.

5 Conclusion

This study evaluated the i-voting system of the Czech Pirate Party based on the software Helios, focusing on its democratic and technical attributes. Our findings demonstrate that the Helios system successfully enhances member participation and transparency, similar to other digital parties. While Podemos and Movimento 5 Stelle have encountered issues with limited member initiative and transparency (Deseriis & Vittori, 2019; Von Nostitz & Sandri, 2021), the Czech Pirate Party's use of Helios provides a more transparent and participatory model.

Key insights from our research include the high satisfaction rate among party members with the Helios system, the stable voter turnout over time, and the system's compliance with basic security standards. The transparency of the system is considered important with respect to credibility. On the other hand, the display of real names in the ballot box is seen as a potential privacy threat in the future, so the possibility of replacing real names with aliases is offered.

Our study's limitations include its focus on a single case, which restricts the generalizability of the findings. The Czech Pirate Party represents a unique context with a specific set of values and technological literacy among its members, which may not be applicable to other political parties or cultural contexts. Additionally, the sample size and the specific demographic characteristics of the Czech Pirate Party members limit the extent to which these findings can be generalized to other political organizations.

Future research should explore multiple case studies across different political and cultural settings to better understand the broader applicability of i-voting systems. Comparative studies with other digital parties, particularly those using different voting platforms, can provide deeper insights into best practices and potential pitfalls in the implementation of i-voting systems. Further investigation into the long-term security and privacy implications of i-voting, particularly in light of emerging technologies, is essential. The experience with the Czech Pirate Party's system could help to develop a national recommendation, along the lines of the French CNIL (La Commission nationale de l'informatique et des libertés, 2019), which could define basic requirements for other secret online elections held in parties, institutions, organisations

and other departments. Moreover, research on how different demographic groups within political parties interact with i-voting systems could provide valuable insights into improving accessibility and inclusivity. Exploring alternative voting methods and their integration into existing platforms like Helios could also enhance voter confidence and participation.

In summary, the Czech Pirate Party's implementation of the Helios i-voting system represents a significant advancement in integrating digital tools into political processes. The system has proven effective in fostering internal democracy and engaging a digitally-oriented voter base. However, continuous evaluation and adaptation are necessary to address emerging challenges and ensure the integrity and inclusivity of the democratic process. The experiences of the Czech Pirate Party can serve as a valuable model for other political organizations seeking to adopt digital voting systems, but they must consider the specific needs and contexts of their own memberships.

This work contributes to the current discussion of decision-making voting platforms in political parties. Compared to Podemos and Movimento 5 Stelle, Helios offers more transparent conditions for its users (Deseriis & Vittori, 2019). A crucial difference is the scale of participation: the Helios platform was created for an effective scale of only a few thousand users, whereas Participa (Podemos) and Rousseau (Movimento 5 Stelle) platforms are designed for hundreds of thousands of members. Unlike the German Pirate Party, which used LiquidFeedback, Helios does not allow for vote delegation and tries to maintain an egalitarian approach to voting (Deseriis, 2021). The overall ease of voting for members is relatively high, and the platform can be described as user-friendly (Deseriis, 2023).

Additional Information and Declarations

Acknowledgments: Thanks to all participants of the anonymous survey who helped to create a unique dataset through their participation.

Funding: The first author (T.M.) prepared this article within the project "Smart environments – modelling and simulation of complex decision-making problems in intelligent systems" (2022B0010) funded through the IGA foundation of the Faculty of Economics and Management, Czech University of Life Sciences in Prague.

Conflict of Interests: Tomáš Martínek is a member of the Czech Pirate Party. The second author, Michal Malý, who critically analysed the findings, is not a member. The authors approached the analysis with a critical eye to ensure that a trustworthy and secure online voting system would enable the preservation of a functional intra-party democracy.

Author Contributions: T.M.: Conceptualization, Data Curation, Investigation, Funding acquisition, Project administration, Supervision, Validation, Visualization, Software, Resources, Writing – Original draft preparation. M.M.: Methodology, Formal Analysis, Writing – Reviewing and Editing.

Institutional Review Board Statement: Ethical review and approval were waived for this study due to prior approval from political party leadership.

Informed Consent Statement: The anonymous questionnaire survey was conducted on the basis of the consent of the Bureau of the Czech Pirate Party. Each participant of the anonymous survey was informed about the anonymous nature of the survey, including other documents and consent, in an invitation e-mail.

Data Availability: The data that support the findings of this study are openly available in Zenodo at <https://doi.org/10.5281/zenodo.10829926>.

Appendix A

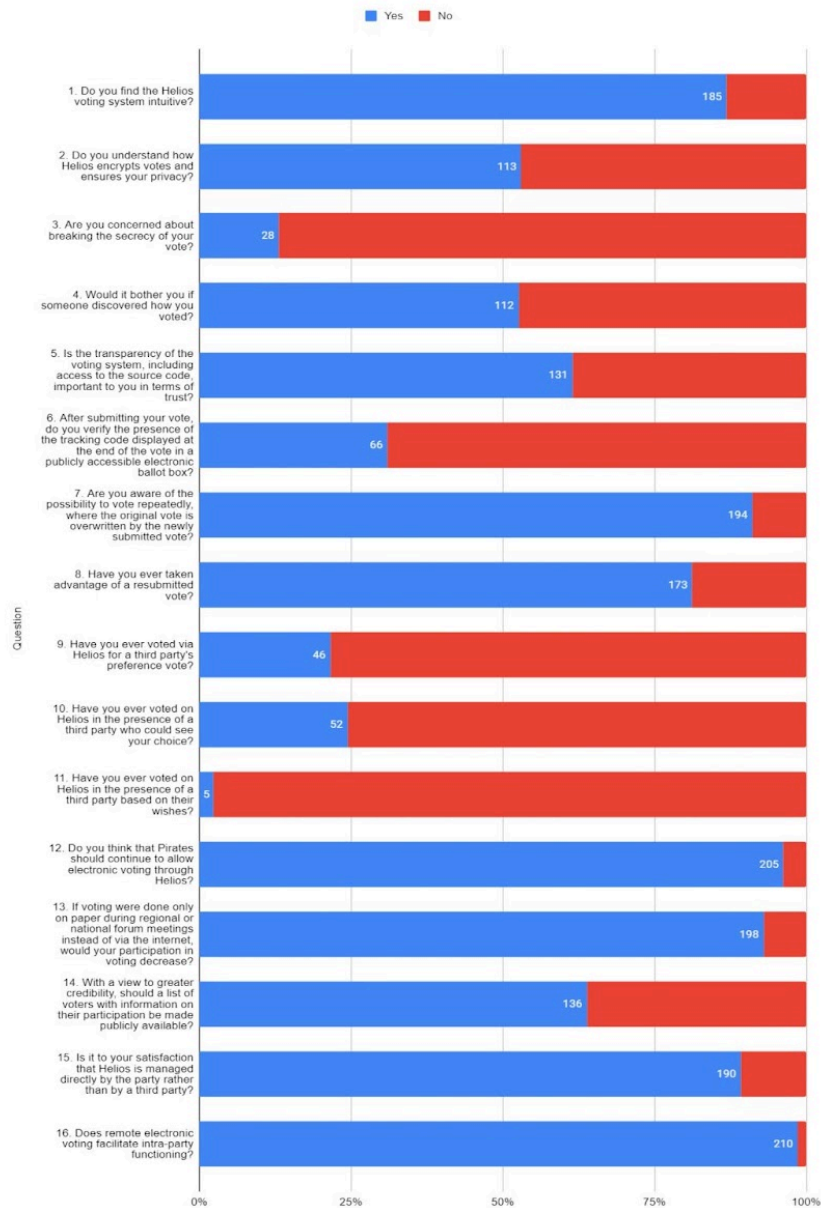


Figure A1. Results of the Helios survey among Pirates members, N=213. Source: (Martínek & Malý, 2024).

Appendix B


Hlasovací systém Helios | Česká pirátská strana

[Help](#)

[O Heliosu](#)

CF 15/2023 (1) Volba lídra v primárních volbách do EP 2. kolo

veřejné election vytvořeno uživatelem [Tereza Vovesová](#)

Vážené Celostátní fórum,

zahajují hlasování ve věci CF 15/2023 (3) Volba lídra v primárních volbách do EP 2. kolo.

Rozprava proběhla [zde](#).

Volební kalkulačku můžete využít [zde](#).

Navržení kandidátů a kandidátky:

- Marcel Kolaja - videomedailonek - kandidátská řeč - závěrečné slovo
- Markéta Gregorová - videomedailonek - kandidátská řeč - závěrečné slovo
- Mikuláš Peksa - videomedailonek - kandidátská řeč - závěrečné slovo

V druhém kole hlasujeme o preferenci. Volíme tedy toho, koho nejvíce preferujeme jako lídra kandidátky. Každý hlasující může hlasovat pro jednoho kandidáta. Pokud chce volit proti všem kandidátům, může vhodit prázdný hlas. V případě rovnosti hlasů rozhoduje pořadí z 1. kola volby.

Hlasování začíná: 16. září 2023 11:25
Hlasování končí: 16. září 2023 12:25

[otázky \(1\)](#) | [voliči a hlasovací lístky](#) | [trustees \(5\)](#)

Toto hlasování bylo ukončeno. Výsledek byl zveřejněn 16. září 2023 12:38. Celkem hlasovalo 543 voličů.

Výsledek hlasování

Otázka #1
Jako lídra kandidátky do EP preferuji

Marcel Kolaja	299
Markéta Gregorová	102
Mikuláš Peksa	81

Audit Info

URL hlasování:
<https://helios.pirati.cz/helios/e/cf-15-2023-1-volba-lidra-2-kolo>

Otisk hlasování:
yeb1pY538AHZVKRzf1SMfopIgl17NZ1mtrhqqZQods8

Váš kód pro sledování hlasovacího lístku:
RqBqnz5XZZ98L1NMfM3AC15TjDVCfHzLoLg6PHpBg7s

[Ballot Tracking Center](#) | [Audited Ballots](#)

ověřit [výsledek hlasování](#). [review the voting booth](#).

Figure B1. The web page of the Helios.pirati.cz system with the published results of the second round of the election of the leader for the Euro elections. The final results page contains at the top the name of the election, below the name of the election administrator, below the information about the voting methods and candidates displayed to all voters even before the election, including links to the candidates' speeches and other information about the candidates, below the start and end dates of the voting, below links to the questions, the list of voters and the list of trustees, below voting information including the total number of voters, below the results for each candidate, and in the expanded yellow box, the supporting documentation for individual audit verification including the vote imprint and ballot tracking code.

Figure B2. The page for adding voters to the election. In addition to the basic Helios options, Pirates allows election administrators to select a third option where voters who are in the selected group are selected to vote. A group can be a national forum that includes all party members, or a regional membership group such as a regional or local forum, or a regional or local association that includes registered supporters. Uploading voters is done when the blue bulk add voters button is pressed. The source of the actual data is the linked Octopus application.

Jméno	Kód pro sledování lístku
Tomáš Martinek	P4q3x291UwGXnhIE75z2fwVKxZW126iQL18s+qRB8Xk
Václav Dvořák	3A9XU0P3JALAVPTL7E751FAL8E7A7L0R0V

Figure B3. Publicly accessible electronic ballot box page. Pirates in the ballot box display the real names of voters next to the ballot tracking code, which may compromise privacy in the future. In this case, it is an electronic ballot box from a county primary election to cast a write-in ballot for a county election. The name of the election is displayed at the top, with who can vote defined below, a search, and then a public list of voters.

References

- Acemyan, C. Z., Kortum, P., Byrne, M. D., & Wallach, D. S. (2014). From Error to Error: Why Voters Could not Cast a Ballot and Verify Their Vote With Helios, Prêt à Voter, and Scantegrity II. *USENIX Journal of Election Technology and Systems*, 2(3), 26–56. <https://www.usenix.org/jets/issues/0302/acemyan>
- Adida, B. (2008). Helios: Web-based Open-Audit Voting. *USENIX security symposium*, 17, 335–348. https://www.usenix.org/legacy/event/sec08/tech/full_papers/adida/adida.pdf
- Adida, B., de Marneffe, O., Pereira, O., & Quisquater, J.-J. (2009). Electing a University President using Open-Audit Voting: Analysis of real-world use of Helios. In *Proceedings of the 2009 Conference on Electronic Voting Technology/Workshop on Trustworthy Elections*. https://www.usenix.org/legacy/event/evt09/tech/full_papers/adida-helios.pdf
- Agbesi, S., Budurushi, J., Dalela, A., & Kulyk, O. (2023). Investigating transparency dimensions for internet voting. In *Electronic Voting* (pp. 1–17). Springer. https://doi.org/10.1007/978-3-031-43756-4_1

- Agora Voting.** (2023). NVotes. Democracy Technologies. <https://democracy-technologies.org/product/nvotes/>
- Baloglu, S., Bursuc, S., Mauw, S., & Pang, J.** (2021a). Election Verifiability Revisited: Automated Security Proofs and Attacks on Helios and Belenios. In *2021 IEEE 34th Computer Security Foundations Symposium (CSF)*, (pp. 1–5). IEEE. <https://doi.org/10.1109/CSF51468.2021.00019>
- Baloglu, S., Bursuc, S., Mauw, S., & Pang, J.** (2021b). Provably Improving Election Verifiability in Belenios. In R. Krimmer, M. Volkamer, D. Duenas-Cid, O. Kulyk, P. Rønne, M. Solvak, & M. Germann (Eds.), *Electronic Voting* (pp. 1–16). Springer. https://doi.org/10.1007/978-3-030-86942-7_1
- Barrat i Esteve, J.** (2022). The Use of Electronic Vote Within the Political Parties. Ideas for democracy. <https://www.minsait.com/ideasfordemocracy/en/use-electronic-vote-within-political-parties-full-length-article>
- Bavdekar, R., Chopde, E. J., Bhatia, A., Tiwari, K., Daniel, S. J., & Atul.** (2022). Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research. *Arxiv.org*. <https://doi.org/10.48550/arXiv.2202.02826>
- Bernhard, D., Cortier, V., Pereira, O., Smyth, B., & Warinschi, B.** (2011). Adapting Helios for Provable Ballot Privacy. In V. Atluri & C. Diaz (Eds.), *Computer Security – ESORICS 2011*, (pp. 335–354). Springer. https://doi.org/10.1007/978-3-642-23822-2_19
- Bernhard, D., Pereira, O., & Warinschi, B.** (2012). How Not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios. In *Advances in Cryptology – ASIACRYPT 2012* (pp. 626–643). Springer. https://doi.org/10.1007/978-3-642-34961-4_38
- Beurdouche, B., Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Kohlweiss, M., Pironti, A., Strub, P. -Y., & Zinzindohoue, J. K.** (2017). A messy state of the union. *Communications of the ACM*, 60(2), 99–107. <https://doi.org/10.1145/3023357>
- Blanchard, E., Gallais, A., Leblond, E., Sidhoum-Rahal, D., & Walter, J.** (2022). An Analysis of the Security and Privacy Issues of the Neovote Online Voting System. In R. Krimmer, M. Volkamer, D. Duenas-Cid, P. Rønne, & M. Germann (Eds.), *Electronic Voting* (pp. 1–18). Springer. https://doi.org/10.1007/978-3-031-15911-4_1
- Boček, J., Kočí, P., Krawiecová, N., & Zákopčanová, K.** (2021). Kandidáti do sněmovny zestárlí. 'Transformace stranického systému skončila,' říká politolog. IROZHLAS. https://www.irozhlas.cz/volby/snemovni-volby-2021-interaktivni-kandidatky_2109140634_jab
- Brunet, J., & Essex, A.** (2023). Online Voting in Ontario Municipalities: A Standards-Based Review. In *E-Vote-ID 2023: Electronic Voting* (pp. 52–68). Springer. https://doi.org/10.1007/978-3-031-43756-4_4
- Cirhan, T., & Stauber, J.** (2018). Online supporter and registered sympathiser as alternatives to a regular party member. *East European Politics*, 34(4), 458–482. <https://doi.org/10.1080/21599165.2018.1532410>
- Cortier, V.** (2015). Formal verification of e-voting: solutions and challenges. *ACM SIGLOG News*, 2(1), 25–34. <https://doi.org/10.1145/2728816.2728823>
- Cortier, V., Gaudry, P., & Glondou, S.** (2019). Belenios: A Simple Private and Verifiable Electronic Voting System. In J. D. Guttman, C. E. Landwehr, J. Meseguer, & D. Pavlovic (Eds.), *Foundations of Security, Protocols, and Equational Reasoning, Lecture Notes in Computer Science* (pp. 214–238). Springer. https://doi.org/10.1007/978-3-030-19052-1_14
- Cortier, V., Gaudry, P., & Glondou, S.** (2020). Analyse de sécurité de la plateforme de vote Belenios Conformité avec les recommandations 2019 de la CNIL. <https://www.belenios.org/analyse-secu.pdf>
- Council of Europe.** (2017). Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting: (Adopted by the Committee of Ministers on 14 June 2017 at the 1289th meeting of the Ministers' Deputies). https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f
- Czech Republic.** (2024). Zákon č. 424/1991 Sb.: Zákon o sdružování v politických stranách a v politických hnutích. <https://www.e-sbirka.cz/sb/1991/424?zalozka=text>
- Czech Republic.** (1995). Zákon č. 247/1995 Sb.: Zákon o volbách do Parlamentu České republiky a o změně a doplnění některých dalších zákonů. <https://www.e-sbirka.cz/sb/1995/247/2021-07-01>
- Deseriis, M.** (2017). Direct Parliamentarianism: an analysis of the political values embedded in Rousseau, the 'Operating system' of the Five star movement. *eJournal of eDemocracy and Open Government*, 9(2), 47–67. <https://doi.org/10.29379/jedem.v9i2.471>
- Deseriis, M.** (2023). Reducing the Burden of Decision in Digital Democracy Applications: A Comparative Analysis of Six Decision-making Software. *Science, Technology, & Human Values*, 48(2), 401–427. <https://doi.org/https://doi.org/10.1177/01622439211054081>
- Deseriis, M.** (2021). Rethinking the digital democratic affordance and its impact on political representation: Toward a new framework. *New Media & Society*, 23(8), 2452–2473. <https://doi.org/https://doi.org/10.1177/1461444820929678>
- Deseriis, M., & Vittori, D.** (2019). The Impact of Online Participation Platforms on the Internal Democracy of Two Southern European Parties: Podemos and the Five Star Movement. *International Journal of Communication*, 13(1), 5695–5714.
- Essex, A., & Goodman, N.** (2020). Protecting electoral integrity in the digital age: Developing E-Voting regulations in Canada. *Election Law Journal Rules Politics and Policy*, 19(2), 162–179. <https://doi.org/10.1089/elj.2019.0568>
- Fitzpatrick, J., & Jöst, P.** (2022). "The High Mass of Democracy" —Why Germany remains aloof to the idea of electronic voting. *Frontiers in Political Science*, 4, 876476. <https://doi.org/10.3389/fpos.2022.876476>
- Garnett, H. A., & James, T. S.** (2020). Cyber Elections in the Digital Age: Threats and Opportunities of technology for electoral integrity. *Election Law Journal*, 19(2), 111–126. <https://doi.org/10.1089/elj.2020.0633>

- Gerbaudo, P. (2019). *The Digital Party Political Organisation and Online Democracy*. Pluto Press.
- Haines, T., Mosaheb, R., Müller, J., & Pryvalov, I. (2023). SoK: Secure E-Voting with Everlasting Privacy. *Proceedings on Privacy Enhancing Technologies*, 2023(1), 279–293. <https://doi.org/10.56553/popets-2023-0017>
- Husarová, L., & Hromádka, M. (2012). John obhájil v internetovém hlasování pozici předsedy Věcí veřejných. *IROZHLAS*. https://www.irozhlas.cz/zpravy-domov/john-obhajil-v-internetovem-hlasovani-pozici-predsedy-veci-verejnych_201206202001_mhromadka
- Jebavá, J., & Masare, V. (2020). Pražské Zelené nově povede Jana Jebavá a Vít Masare. *Zelení*. <https://praha.zeleni.cz/prazske-zelene-nove-povede-jana-jebava-a-vit-masare/>
- Kopecký, J. (2010). Hlasování věčkařů o vládě musela strana zastavit. Ukazovalo se jen ANO. *IDNES.cz*. https://www.idnes.cz/zpravy/domaci/hlasovani-veckaru-o-vlade-musela-strana-zastavit-ukazovalo-se-jen-ano_A100709_123617_domaci_kop
- La Commission nationale de l'informatique et des libertés. (2019). Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet: NOR: CNIL1917529X. Légifrance. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038661239>
- Lanzone, M. E., & Rombi, S. (2018). Selecting Candidates Online in Europe: A Comparison Among the Cases of M5S, Podemos and European Green Party. In G. Cordero & X. Coller (Eds.), *Democratizing Candidate Selection*, (pp. 99–121). Springer. https://doi.org/10.1007/978-3-319-76550-1_5
- Lee Rodgers, J., & Nicewander, W. A. (1988). Thirteen ways to look at the correlation coefficient. *The American Statistician*, 42(1), 59–66. <https://doi.org/10.1080/00031305.1988.10475524>
- Lupato, F. G., & Meloni, M. (2023). Digital Intra-Party Democracy: An Exploratory Analysis of Podemos and the Labour Party. *Parliamentary Affairs*, 76(1), 22–42. <https://doi.org/10.1093/pa/gsab015>
- Marcos del Blanco, D. Y., Duenas-Cid, D., & Aláiz Moretón, H. (2020). E-Voting System Evaluation Based on the Council of Europe Recommendations: nVotes. In R. Krimmer, M. Volkamer, B. Beckert, R. Küsters, O. Kulyk, D. Duenas-Cid, & M. Solvak (Eds.), *Electronic Voting* (pp. 147–166). Springer. https://doi.org/10.1007/978-3-030-60347-2_10
- Marcos del Blanco, D. Y., & Gascó, M. (2019). A Protocolized, Comparative Study of Helios Voting and Scytl/iVote. In *2019 Sixth International Conference on eDemocracy & eGovernment (ICEDEG)*, (pp. 31–38). IEEE. <https://doi.org/10.1109/ICEDEG.2019.8734351>
- Marky, K., Zollinger, M., Roenne, P., Ryan, P. Y. A., Grube, T., & Kunze, K. (2021). Investigating usability and user experience of individually verifiable internet voting schemes. *ACM Transactions on Computer-Human Interaction*, 28(5), 1–36. <https://doi.org/10.1145/3459604>
- Martínek, T., & Forýtek, L. (2022). The highly secure anonymous e-voting system of the Czech Pirate Party. In R. Krimmer, M. Volkamer, D. Duenas-Cid, M. Germann, S. Glondy, T. Hofer, I. Krivosova, B. Martin-Rozumilowicz, P. Rønne, & M. -L. Zollinger (Eds.), *E-Vote-ID 2022: Seventh Joint International Conference on Electronic Voting*, (pp. 165–168). University of Tartu Press. <https://doi.org/10.1515/diss/036>
- Martínek, T., & Malý, M. (2024). Questionnaire survey among members of the Czech Pirate Party regarding the use of the online voting system Helios. *Zenodo*. <https://doi.org/10.5281/zenodo.10829926>
- Mikola, B. (2017). Online primaries and intra-party democracy: Candidate selection processes in Podemos and the Five Star Movement: Candidate selection processes in Podemos and the Five Star Movement. *Revista de Internet, Derecho y Política*, (24), 37–49. <https://www.redalyc.org/pdf/788/78850913004.pdf>
- Montgomery, D. C., & Runger, G. C. (2010). *Applied statistics and probability for engineers*. John Wiley.
- Mortkowitz, S. (2019). Czech Pirates, ahoy!. *Politico*. <https://www.politico.eu/article/czech-pirate-party-anti-establishment-ivan-bartos-ahoy/>
- Mosca, L. (2020). Democratic vision and online participatory spaces in the Italian Movimento 5 Stelle. *Acta Politica*, 55(1), 1–18. <https://doi.org/10.1057/s41269-018-0096-y>
- Musella, F. (2023). How a left-wing political party fails to keep up with the times. *Journal of Modern Italian Studies*, 28(5), 585–601. <https://doi.org/10.1080/1354571x.2023.2255060>
- Neovote. (2024). Elections politiques. *Neovote*. https://www.neovote.com/scrutins_specifiques/scrutins-politiques
- Nurse, J. R. C., Agrafiotis, I., Erola, A., Bada, M., Roberts, T., Williams, M., Goldsmith, M., & Creese, S. (2017). An Assessment of the Security and Transparency Procedural Components of the Estonian Internet Voting System. In *Human Aspects of Information Security, Privacy and Trust* (pp. 366–383). Springer. https://doi.org/10.1007/978-3-319-58460-7_26
- Panizo Alonso, L., Gascó, M., Marcos del Blanco, D. Y., Alonso, J. Á. H., Barrat, J., & Moreton, H. A. (2018). E-Voting System Evaluation Based on The Council of Europe Recommendations: Helios Voting. *IEEE Transactions on Emerging Topics in Computing*, 9(1), 161–173. <https://doi.org/10.1109/TETC.2018.2881891>
- Pearson, K. (1895). VII. Note on regression and inheritance in the case of two parents. *Proceedings of the Royal Society of London*, 58, 240–242. <https://doi.org/10.1098/rspl.1895.0041>
- Pereira, O. (2016). Internet voting with Helios. In *Real-World Electronic Voting: Design, Analysis and Deployment*. CRC Press.
- Pink, M., & Folvarčňý, A. (2020). The Czech Pirate Party: A New Alternative, Not Only for the Young. *Intersections*, 6(4), 176–196. <https://doi.org/10.17356/ieejsp.v6i4.610>
- Pirates. (2022). Ochrana osobních údajů. *Pirati.cz*. <https://www.pirati.cz/ochrana-osobnich-udaju/>

- Raniolo, F., & Tarditi, V. (2020). Digital revolution and party innovations: An analysis of the Spanish case. *Italian Political Science Review*, 50, 235–253. <https://doi.org/10.1017/ipo.2019.27>
- Rodríguez-Pérez, A. (2022). The Council of Europe's CM/Rec(2017)5 on e-voting and Secret Suffrage: Time for yet Another Update? In R. Krimmer, M. Volkamer, D. Duenas-Cid, P. Renne, & M. Germann (Eds.), *Electronic Voting* (pp. 90–105). Springer. https://doi.org/10.1007/978-3-031-15911-4_6
- Sako, K., & Kilian, J. (1995). Receipt-Free Mix-Type Voting Scheme. In *Advances in Cryptology — EUROCRYPT '95* (pp. 393–403). Springer. https://doi.org/10.1007/3-540-49264-X_32
- Solop, F. I. (2001). Digital democracy comes of age: internet voting and the 2000 Arizona Democratic Primary election. *Political Science & Politics*, 34(02), 289–293. <https://doi.org/10.1017/s104909650100052x>
- Šárovec, D. (2022). Digitalization of the Digitalized Ones: The Czech Pirate Party and its Online Congresses. *European Consortium for Political Research*. <https://ecpr.eu/Events/Event/PaperDetails/64060>
- Šárovec, D. (2019). Assured Newcomers on a Squally Sea? The Czech Pirate Party before and after the 2017 Elections. *Acta Fakulty filozofické Západočeské univerzity v Plzni*, 11(2), 1–21. <https://doi.org/10.24132/actaff.2019.11.2.1>
- TOP 09. (2024). Tajné elektronické volby. https://www.top09.cz/files/soubory/tajne-elektronicke-volby-navod_980.pdf
- TOP 09. (2011). Delegáti sněmu TOP 09 si budou volit vedení elektronicky, ve stanu. TOP 09. <https://www.top09.cz/co-delame/medialni-vystupy/delegati-snemu-top-09-si-budou-volit-vedeni-elektronicky-ve-stanu-7369.html>
- Transparency International. (2014). Masová manipulace u voleb potvrzena. *Transparency.cz*. <https://www.transparency.cz/masova-manipulace-u-voleb-potvrzena/>
- U.S. Vote Foundation. (2015). E2E-VIV Project: The Future of Voting: End-to-End Verifiable Internet Voting - Specification and Feasibility Study. *U.S. Vote Foundation*. <https://www.usvotefoundation.org/E2E-VIV>
- Vittori, D. (2019). Membership and members' participation in new digital parties: Bring back the people? *Comparative European Politics*, 18(12), 609–629. <https://doi.org/https://doi.org/10.1057/s41295-019-00201-5>
- Vodová, P., & Voda, P. (2020). The effects of deliberation in Czech Pirate Party: The case of coalition formation in Brno (2018). *European Political Science*, 19(2), 181–189. <https://doi.org/10.1057/s41304-019-00233-1>
- von Nostitz, F., & Sandri, G. (2021). I-Voting Regulation Within Digital Parties: The Case of Podemos and Five Stars Movement. In O. Barberà, G. Sandri, P. Correa, & J. Rodríguez-Teruel (Eds.), *Digital Parties* (pp. 85–107). Springer. https://doi.org/10.1007/978-3-030-78668-7_5
- von Nostitz, F., Sandri, G., & Esteve, J. B. (2021). Regulating i-Voting Within Countries and Parties. In O. Barberà, G. Sandri, P. Correa, & J. Rodríguez-Teruel (Eds.), *Digital Parties* (pp. 43–66). Springer. https://doi.org/10.1007/978-3-030-78668-7_3
- Wack, J. (2014). IEEE VSSC/1622: Voting System Standards. National Institute of Standards and Technology. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=916378
- Wolchok, S., Wustrow, E., Isabel, D., & Halderman, J. A. (2012). Attacking the Washington, D.C. Internet Voting System. In *16th Conference on Financial Cryptography & Data Security* (pp. 114–128). Springer. https://doi.org/10.1007/978-3-642-32946-3_10
- W3C Web Accessibility Initiative. (2023). Zásady přístupnosti. *Web Accessibility Initiative (WAI)*. <https://www.w3.org/WAI/fundamentals/accessibility-principles/cs>

Editorial record: The article has been peer-reviewed. First submission received on 21 March 2024. Revision received on 13 June 2024. Accepted for publication on 20 July 2024. The editor in charge of coordinating the peer-review of this manuscript and approving it for publication was Zdenek Smutný .

Acta Informatica Pragensia is published by Prague University of Economics and Business, Czech Republic.

ISSN: 1805-4951

Příloha I: Článek Implementace tajné a ověřitelné personální elektronické volby na dálku agrární organizace dle doporučení Rady Evropy

MARTÍNEK, Tomáš, Martin PELIKÁN, Jan TYRYCHTR a Jakub KONOPÁSEK, 2024. Implementation of a Secret and Verifiable Personal Remote Electronic Election of an Agrarian Organization per the Recommendation of the Council of Europe. *AGRIS on-line Papers in Economics and Informatics* [online]. 16(3), 59-73 [cit. 2024-09-30]. ISSN 1804-1930. Dostupné z: doi:[10.7160/aol.2024.160305](https://doi.org/10.7160/aol.2024.160305)

Implementation of a Secret and Verifiable Personal Remote Electronic Election of an Agrarian Organization per the Recommendation of the Council of Europe

Tomáš Martínek , Martin Pelikán , Jan Tyrychtr , Jakub Konopásek 

Department of Information Engineering, Faculty of Economics and Management, Czech University of Life Sciences Prague, Czech Republic

Abstract

Lockdowns and social progress have increased hours of work from home, often requiring remote methods of communication. Agricultural organizations from associations to cooperatives to joint stock companies must prepare to carry out more activities online. This article proposes a procedure for the possible implementation of a remote electronic election in personnel matters of the organization using the Belenios system, based on an evaluation of expectations from a questionnaire survey of agricultural college students and graduates. The proposed procedure is subsequently verified based on an evaluation of compliance with the Council of Europe recommendation on standards for electronic voting.

Keywords

Internet voting, E-voting, E-democracy, Open-Source, Belenios, E-elections.

Martínek, T., Pelikán, M., Tyrychtr, J. and Konopásek, J. (2024) "Implementation of a Secret and Verifiable Personal Remote Electronic Election of an Agrarian Organization per the Recommendation of the Council of Europe", *AGRIS on-line Papers in Economics and Informatics*, Vol. 16, No. 3, pp. 59-73. ISSN 1804-1930. DOI 10.7160/aol.2024.160305.

Introduction

Online voting is becoming an increasingly prevalent method of casting a ballot. In Estonia, 51% of participating voters cast a ballot online in the 2023 Parliamentary elections (Valimised.ee, 2023). While the COVID-19 pandemic has promoted the use of ICT tools for remote communication, i-voting has not developed as much in national politically binding elections (Driza Maurer et al., 2023). Remote electronic dialing is one of the possibilities of using ICT. So that the members of the institution do not have to all meet in one place for the elections, but elections can be instead conducted remotely.

If it is a public election without the secrecy of individual ballots, such an election can be carried out in many ways. The problem arises if the principle of secrecy of elections is to be observed, i.e. the secrecy of ballots so that even the administrator of the election system cannot find out the form of individual ballots. I-voting is developing in its use in the primary elections of political parties (Blanchard et al., 2022) and their other intra-party decision-making (Martínek and Malý, 2024), in academic elections

(Adida et al., 2009) and in other institutions. In our paper, we focus on secret personnel ballots in agricultural enterprises, which can be agricultural or food production cooperatives, or limited liability companies or joint stock companies with a focus on agriculture and food production. The proposed methodological procedure may also be suitable for agricultural unions and associations.

Food cooperatives began to be established in the Czech Republic in the first half of the 19th century, and agricultural cooperatives were also established in the second half. Among the basic principles of cooperatives is democratic control, requiring also voting by cooperative members (Kofínková et al., 2017). After 1989, other types of agricultural enterprises using voting within the ownership structure began to emerge in the Czech Republic in the form of limited liability companies or joint stock companies. The Act on Companies and Cooperatives (Czech Republic, 2012) allows voting using technical means. The voting conditions must ensure that the identity of the voting person is verified and that the shares or stocks associated with the voting right are identified. These conditions are determined by the articles of association or the articles

of association and are set out in the invitation to the general meeting or in the draft resolution. In the case of a cooperative, each member has 1 vote in the voting and secret ballots are generally permitted. In the case of limited liability companies, a secret ballot is excluded in certain cases, for example when the law requires the voting members to be named in the notarial deed. A secret ballot is required for the election and removal of employee members of the supervisory board.

In the Czech Republic, agrarian enterprises already use a number of digital services, which include e-mail, electronic signature, the Ministry of Agriculture's eAgri portal, data box, public administration portal, tax portal, electronic procurement, e-customs and others (Rysová et al., 2013). Agricultural enterprises are also gradually starting to use social networks (Kánská et al., 2013). Secret ballot via the Internet is not among the commonly used systems. With the use of information and communication technologies (ICTs), farms can enjoy benefits that may include better accessibility of elections, greater voter interaction, voter time savings, and others. At the same time, however, potential threats and risks must be addressed where the security of the constitutional principles of personal elections, which commonly include universal, equal, free and secret suffrage, may be compromised. Legislative documents that should be considered when i-voting in the Czech Republic include the recommendations of the Council of Europe, of which the Czech Republic is a member (Driza Maurer et al., 2023).

Council of Europe Recommendation on standards for e-voting

The Council of Europe's core legislative document for i-voting is Recommendation CM/Rec(2017) 5 of the committee of ministers to member states on standards for e-voting (Council of Europe, 2017). While the Recommendation is not binding on members, compliance with it is expected. Norway and Sweden have voluntarily adopted the Recommendation, the Supreme Court in Estonia has referred to the Recommendation, and in Belgium the Recommendation has been used as a benchmark in the evaluation of e-voting (Rodríguez-Pérez, 2022).

Based on the results of a questionnaire survey among students and graduates of agricultural colleges, this paper aims to propose a sufficiently transparent and verifiable methodological procedure using the open source Belenios

system for conducting a secret remote electronic election in an agricultural enterprise or union. The methodological procedure should be subsequently validated using the requirements of the Council of Europe (2017) recommendations.

Materials and methods

In this article, a methodical procedure for the implementation of a secret remote electronic election using the Belenios test system was proposed. To achieve the goal of the article, a survey of professional literature was conducted from the scientific databases Web of Science and Scopus. To process the literature search, the article further focuses on professional texts, legislation and other sources related to agricultural enterprises.

Questionnaire survey on the characteristics of remote electronic voting

In order to find out the opinions on the features of remote electronic voting, a questionnaire survey was conducted among students and graduates of Czech universities with agricultural specialization. We assume that these are people with higher technical literacy who may be potential users of i-voting systems on farms in the near future. The Agbesi et al. (2023) framework with identical questions was used to construct the questions, which explored dimensions of Internet voting transparency, supplemented with a few specific questions. Agbesi et al. (2023) identify five core dimensions, namely Information Availability, Understandability, Monitoring and verifiability, Remedial Measures, Testing, these dimensions affect the perception of transparency which in turn affects the trustworthiness in the whole system. The anonymous questionnaire survey was conducted online via the Dotaznik.czu.cz platform operated by the Czech University of Life Sciences Prague. The invitation to participate in the survey was extended primarily to Czech students and graduates of agricultural universities. The survey was conducted from 24 October 2023 to 12 May 2024. Participants were shown all information including consent to data processing on the survey homepage.

Respondents answered questions on a seven-point Likert scale ranging from Strongly Disagree (0) to Strongly Agree (6) on five defined dimensions. A total of 177 people were recorded as completing the questionnaire. A total of 108 questionnaires were completed in full. Of these, 8 more questionnaires

were removed because the control question "This question is not part of the survey and just helps us to detect bots and automated scripts. To confirm that you are a human, please choose 'Strongly agree' here" was answered differently than Strongly agree. Out of the 100 responses, 64 were male, 35 were female and 1 respondent did not indicate their gender. 72 respondents are aged 18-30, 18 aged 31-40, 5 aged 41-50, 2 aged 51-60 and 3 aged 61-70. 72 respondents have completed secondary education, 10 have a Bachelor's degree, 12 have a Master's degree and 6 have a PhD.

The questionnaire survey is evaluated in aggregate according to the defined dimensions and transparency, which consist of individual questions. The rating describes the average frequency of responses on a Likert scale and the degree of expectation of fulfilling a given dimension on a scale from 0 (not at all expected) to 1 (fully expected), where from 0.5 upwards a given characteristic is expected. The level of expectation for a given attribute is the ratio of the average rating to the maximum possible rating within the aggregate of the whole dimension. The value is rounded to 2 decimal places.

The Statistica 14 software was used to do the descriptive statistics. We calculated fundamental information such as the mean, minimum, and maximum values, various measures of variation, and data regarding the shape of the variable's distribution (including the standard deviation and the standard error). An important aspect of the description of a variable was the shape of its distribution, which indicates the frequency of values within different ranges of the variables. More precise information was obtained by performing normality tests to determine the probability that the sample originated from a normally distributed population of observations, specifically using the Shapiro-Wilk test. These statistics were included in the dataset (Martínek and Tyrychtr, 2024).

Methodology for the testing the software used

Our methodology was developed to be used with the Belenios system, which, according to Cortier et al. (2019), offers a compromise between simplicity and security. Belenios is based on the Helios system (Adida et al., 2009). For the testing purposes of this article, the Belenios system installation at <https://volba.odvolit.cz> is used, which also verifies the correct functionality of the open-source code of the official system installation at <https://vote.belenios.org>. To specify

the new methodological procedure, the general characteristics of the organization's information systems and their requirements were considered. The proposed methodological procedure combines the instructions of the Belenios voting system (Belenios team, 2023) embedded in the practical paper voting common in Czech organizations.

Methodology for the design of the election procedure

The methodological procedure is designed to meet the expectations identified in the questionnaire survey. The methodological procedure is tested by experimental voting in the form of a secret personnel election of a model organization. In our case, the model organization is a medium-sized agricultural cooperative, which has its information system for members and which uses the procedure for the election of the board. The cooperative thus uses an ERP system that enables the display of personalized information for individual members of the cooperative as well as communication through encrypted messages.

Methodology for verification of the proposed methodological procedure

Subsequently, the proposed methodological procedure of the election was verified by checking against the fulfillment of Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for electronic voting of the Council of Europe (Council of Europe, 2017) through answers created based on the methodological evaluation of the Helios electronic system (Panizo Alonso et al., 2018), professional literature, security analysis (Cortier et al., 2020) created by the authors of the Belenios system, by testing the system. Considering the limitation of the length of the paper, the basic 49 standards (Brunet and Essex, 2023) are evaluated descriptively. Each requirement is also evaluated in brackets as fulfilled (○), not fulfilled (×), or fulfilled under certain conditions - partial according (Δ) to the symbols in the framework of Panizo Alonso et al. (2018).

Results and discussion

Based on the evaluation of the questionnaire survey, it can be determined that students and graduates of agricultural colleges expect the i-voting system to meet all 5 defined dimensions and transparency, so in the proposal of the methodological procedure of e-voting of agricultural organizations, we will try to meet the expectations (Table 1).

Dimensions (number of questions within a dimension)	Average frequency of responses							Level of expectation
	0	1	2	3	4	5	6	
Information Availability (4)	1.25	1.75	3.25	9	15	25.5	44.25	0.81
Understandability (5)	0	0.2	0.8	3.4	17	33	45.6	0.86
Monitoring and verifiability (5)	0.4	0.4	1.8	8	17.2	30	42.2	0.83
Remedial Measures (5)	0.6	1.6	4	9.6	15	30.8	38.4	0.80
Testing (4)	0.75	0.75	1.75	8	16.5	27.25	45	0.83
Transparency (4)	1.5	0.75	2.25	12.5	19.25	29	34.75	0.79

Source: Authors (Martinek and Tyrychtr, 2024)

Table 1: Evaluation of a questionnaire survey of expected characteristics of i-voting systems among students and graduates of agricultural colleges.

Methodical procedure for remote secret electronic election

The basis for the possibility of conducting an electronic election is to use a trusted electoral system under an administration that voters trust. For the purposes of this article, we use the open-source system Belenios, the functionality of which was verified by our installation. The following method of conducting an election is designed to be conducted, for example, during a remote meeting via an online conference of the membership to participate in the election.

Voters should be informed in advance of the plan to conduct electronic elections, for example in an invitation to a meeting. In accordance with the GDPR, voters should be informed about the way personal data is protected within the organization's information system. The organization should prepare or refer to detailed instructions for using the voting system. In the first phase, it is necessary to designate an election administrator who, as a member of the election commission, will ensure the technical setup and administration of the election. This can be the secretary of the membership body, in the case of ensuring greater credibility, it can be, for example, the independent IT administrator of the given organization.

The administrator can create a new option after logging in. Access codes and authentication are important in the system, which can be via email and password or a trusted third-party system (CAS). In the basic mode, access codes and passwords are sent by the election server; to increase security, access codes should be sent to voters in a different way than by e-mail sent by the election server. This activity can be ensured by an authorized authority, which could distribute the access codes to invited voters in a paper invitation to the meeting, or send them, for example, via the organization's

internal communication system. If access codes or passwords are transmitted in a way other than those sent by the election server to the voter's e-mail, there is less chance of discrediting the election, as the potential risk of "eavesdropping" on encrypted e-mail communication or breaking access to the voter's e-mail box is reduced. The administrator thus enters the name of the authorized authority and gives it a link for generating access codes. In the case of a test election, the individual personal access codes are imported by an authorized authority, which can be the election administrator, into the organization's internal system, which then displays the specific access code after logging in to the given voter with a link to the specific election. The authorized authority has at its disposal a list of voters, which it can also provide to other members of the electoral commission. After the end of the elections and their successful audit verification, this information is removed from the internal system in order to increase the long-term security of the secrecy of the vote.

After setting the voter authentication methods, the administrator further enters a clear name and description of the election, sets questions and answers for the first round of the election, and adds his name and contact, which should be on the authorized identity in case of obtaining a lost access code. It also sets the language of choice, in the Czech Republic the default is Czech (cs), or for people who do not know Czech, they can add other languages of choice, including English (en).

The administrator further populates the voter register by adding a voter email list with one email per line. The system allows you to enter the login of each user in case of using a more sophisticated method of authentication connected to the central authentication service (CAS). The number of whole votes of a given voter can be added to the third place

of the line, separated by a comma, in the case of, for example, different ownership shares of the voters. The same vote weight is used in the experiment. Members of the electoral commission should also have access to the list of voters, including information about their participation in the vote, before the start and after the end of the vote.

As in the case of paper elections, it is necessary to choose persons who will take care of the security of the election in the given institution. In the case of using Belenios, at least two other members of the electoral commission can be elected by public election, who will also be guarantors of the election. The guarantors should not have a personal interest in the outcome of the election so they have no motivation to influence the election after the agreement. Alternatively, the guarantors could be appointed by each of the candidates so that each candidate has one trustworthy person in the electoral commission without whose participation the election results cannot be influenced. After selecting the guarantors, the administrator enters their names and e-mails into the selection settings of the Belenios system. Subsequently, the administrator gives the guarantors, for example, using a confidential secure communication system, their links for generating keys.

When preparing for the election, it is necessary to fill in the voting questions and answers by the administrator. Although the Belenios system allows for various alternative voting methods, including ranking and scoring, for testing purposes, traditional two-round voting, which is often used in organizations as well, will be used. Thus, all nominated candidates participate in the first round. The method of nomination is determined by each organization itself, just as it is already done in paper elections. If any of the candidates receives more than half of the votes, they will be elected in the first round. Otherwise, the two candidates with the highest number of votes advance to the second decisive round. In order to reduce the risk of a tie election in the second round, it is possible to define a condition in the approved voting procedure that in case of equality of votes in the second round, the number of votes in the first round is taken into account.

Before starting the election, the guarantors carry out its encryption, when they save and enter a private key and a unique fingerprint. Immediately after the election is started by the administrator after it has been encrypted, the guarantors will

verify the identity of their unique fingerprint with the publicly displayed fingerprint on the front page of the given election next to their name.

The Electoral Commission shall determine in advance the beginning and end of the voting, which shall be clearly announced to the voters, and the administrator shall set the given times. If an event occurs that may limit voters' access to casting their vote in the electronic ballot box, the electoral commission may agree to extend the deadline for voting.

The voter accesses the election at the URL sent by email with the password or displayed together with the access code. First, he enters the access code, then he fills in the ballot when it should be possible to submit an empty ballot. After it has been encrypted, the voter should save a printout of the ballot for verification and then insert it into the electronic ballot box by logging in using the password sent. At any time after that, he can verify the presence of the ballot in the ballot box using the stored fingerprint.

After the end of the election, the administrator has the encrypted result calculated and then waits for the decryption of the result by all the guarantors. The administrator will provide the guarantors with a URL to enter their private keys to decrypt the election. Admin can also postpone the publication of the result to the exact time. After the evaluation of the elections, the administrator should hand over to the members of the electoral commission the list of voters, including information on participation in the vote. The members of the electoral commission should subsequently audit the voting results (Belenios team, 2023), and anyone else can also do this.

After the audit, both the administrator and the members of the election commission should delete all stored keys and voter lists from their PCs and the organization's internal systems. The choice itself is subsequently archived and deleted after a longer period of time. If all verifications are carried out, the choice can be immediately deleted to ensure the greater long-term security and secrecy of votes.

In the event of an incident or violation of the procedure, in any part for which the members of the election commission are responsible, they immediately inform their superiors - the presiding organization, so that correction can take place. Similarly, voters or auditors should immediately inform the electoral commission of any suspicious event.

Verification of the electoral methodological procedure with the Recommendation CM/Rec(2017)5 of the Committee of Ministers of Member States on standards for electronic voting of the Council of Europe (2017)

1. *The voter interface of an e-voting system shall be easy to understand and use by all voters. (○)*

The Belenios system has already been used in many elections and thousands of different users have managed the election (Cortier et al., 2019). The election process is intuitive and is supplemented with instructions that help less technically literate election participants.

2. *The e-voting system shall be designed, as far as is practicable, to enable persons with disabilities and special needs to vote independently. (Δ)*

The Belenios system achieves a rating of 72 % in the accessibility test (Accessibility Checker, 2023), but at the same time, it is open source, which, if necessary, allows modifications for greater accessibility to electronic voting.

3. *Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting. (○)*

The proposed method takes into account the availability of the voting system online via the Internet. A classic paper election is not excluded for users who do not want to vote online.

4. *Before casting a vote using a remote e-voting system, voters' attention shall be explicitly drawn to the fact that the e-election in which they are submitting their decision by electronic means is a real election or referendum. (○)*

In the proposed procedure, information regarding the meaning of the election is passed on to the voters within the given meeting and the organization's internal information system, which is related to the election.

5. *All official voting information shall be presented in an equal way, within and across voting channels. (○)*

In the proposed procedure, all voters receive the same information using the organization's internal information system or e-mail communication. Basic information

about the election is displayed on the initial page of the vote and in the public data for the election.

6. *Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the result. (○)*

The proposed procedure allows for electronic voting. If it is necessary to hold a non-electronic election, a classic paper election could be held for voters who do not participate in an electronic election. To ensure that voters are not influenced, the publication of electronic results must be set only after the end of the paper election. Subsequently, the results of the electronic and non-electronic election commissions would have to be merged. Since the Electoral Commission has information about the participation of individual voters, it can allow paper voting for those who did not participate in the electronic election, in which case it is assumed that the non-electronic election will take place only after the end of the electronic election.

7. *Unique identification of voters in a way that they can unmistakably be distinguished from other persons shall be ensured. (○)*

The list of voters is compiled based on the identification of voters using a defined e-mail address. Each email address will receive its authentication information. Members of the electoral commission, including the administrator, have access to the list of voters' e-mails, including information about the voter's turnout. Belenios provides authorization verifiability, where anyone can check that votes come from eligible voters (Cortier et al. 2019). According to Baloglu et al. (2021a), it has been shown to satisfy formal requirements for the verifiability of elections, both in the symbolic model for a particular variant (Cortier et al., 2019) and in the computational model (Cortier et al., 2018). Still, there are issues regarding possible attacks on verifiability in case of registrar corruption. Even if the registrar and server are not compromised, individual verifiability can be compromised (Baloglu et al., 2021a).

8. *The e-voting system shall only grant a user access after authenticating her/him as a person with the right to vote. (○)*

The voter is authenticated using two elements, the login name and password on the one hand and the voting code on the other. These two elements

are transmitted separately, one by the voting server, and the other by the voting code generator. In case of loss or theft, the voter can request a new password. In this case, the old password is invalid. The voting code can also be sent back to the voter by the voting code generator (without change) - possibly by the authorized authority. If in the meantime the voting documents were used by a usurper, the voter can vote again with his new identifiers and the old vote will be canceled. In addition, identity theft voting generates an automatic receipt sent to the legitimate voter, greatly increasing the likelihood of detection of potential fraud (Cortier et al., 2020).

9. *The e-voting system shall ensure that only the appropriate number of votes per voter is cast, stored in the electronic ballot box, and included in the election result. (○)*

The ballot containing the choice confirmed by the voter and signed with his valid code is completely prepared on the client side, including encryption. Registration to the ballot box is performed by the server on the condition that the ballot is valid (cryptographically) and that the voter's authentication has been successful. In this case, and only in this case, the attendance register is updated, the voter is sent a confirmation email with a tracking number that serves as a receipt, and the public ballot box also provides a way for the voter to check that their vote has been counted (Cortier et al., 2020).

10. *The voter's intention shall not be affected by the voting system, or by any undue influence. (○)*

The Electoral Commission should ensure that questions are asked impartially and correctly. The voting system itself is then displayed to all voters in the same way.

11. *It shall be ensured that the e-voting system presents an authentic ballot and authentic information to the voter. (○)*

The voter will receive the voting URL of the election in e-mail and in the organization's internal information system. The voter can always verify that he is voting at the correct URL, and that the tracking code of his ticket is inserted in the correct ballot box, which is at the same URL of the sent election extended by "/ballots". The voter can check the submitted form of the ballot after authentication in publicly accessible election data.

12. *The way in which voters are guided through the e-voting process shall not lead them to vote precipitately or without confirmation. (○)*

The voting process has several steps that can always be repeated. It is even possible to submit a completely new ballot before the end of voting, which invalidates the originally submitted one.

13. *The e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options. (○)*

After the voter's identity is verified, he is redirected to the blank ballot. A voter can also hand in a blank ballot. The neutral form of the ballot is ensured by the electoral commission through settings by the administrator. The resulting form can be verified using publicly available election data. Alternatively, the form of the ballot can be challenged and the electoral commission can be forced to correct it, including repeating the election in a correct form. The system does not allow you to set a benefit in the form of a pre-selection of one of the options.

14. *The e-voting system shall advise the voter if he or she casts an invalid e-vote. (○)*

After casting a valid vote in the ballot box, this information is displayed to the voter on the last page of the election and an information e-mail is sent. The system does not allow an invalid vote to be inserted into the ballot box. It is possible to allow the submission of a blank ballot, which is not inherently a validity error, but an opportunity to express the voter's will.

15. *The voter shall be able to verify that his or her intention is accurately represented in the vote and that the sealed vote has entered the electronic ballot box without being altered. Any undue influence that has modified the vote shall be detectable. (○)*

The confidentiality of the ballot during its processing and storage in the ballot box is ensured by the encryption used. Its integrity is ensured by double protection. On the one hand, the signature associated with the slip becomes invalid if the slip is modified (Cortier et al., 2020).

After the ballot is encrypted, a unique tracking code is displayed, which is also sent to the voter's e-mail after it is inserted into the ballot box. The ballot box publicly displays a list of tracking codes, according

to which the voter can verify the counting of his vote in the original encrypted form.

16. *The voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed. (○)*

Information about the successful submission of the ballot is displayed on the last page of the voting process, information about the submission of the vote is also sent to the voter's e-mail address.

17. *The e-voting system shall provide sound evidence that each authentic vote is accurately included in the respective election results. The evidence should be verifiable by means that are independent from the e-voting system. (○)*

Voters can check the presence of their ballot in the ballot box, and external audits ensure that the ballot box only grows. By auditing, anyone can verify, based on public data, that the cryptographic data is consistent (for example, consistency between the public keys of decryption authorities and the public key of elections). After counting, it is possible to make sure that the result corresponds to the encrypted ballots of the ballot box, thanks to the cryptographic evidence provided by the decryption authorities (Cortier et al., 2020). In the Belenios system, no single party needs to be fully trusted, as verifiability is ensured as long as neither the election server nor the registrar is compromised. The registrar generates public credentials, posts them on a bulletin board, and distributes the associated private credentials to voters. The public login serves as the authentication key of the newly created signature key pair, while the private login is the corresponding signature key. The votes are signed and the election authorities can verify on the bulletin board that all votes have been cast by the expected eligible parties (Baloglu et al., 2020).

18. *The system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system. (○)*

The voting server does not have a signing key, so it cannot create a valid signature. In theory, only unauthorized vote deletion could occur. But this would be revealed because voters can check

the presence of their ballot in the ballot box and external audits ensure that the ballot box is only growing. The ballot box (that is, the list of encrypted ballots), the public election key, the list of questions, and the list of public parts of the election codes can be viewed publicly by anyone who knows the election URL. Automatic programs, apart from the voting server, regularly monitor this data (external auditors can also perform this monitoring). Modification of election data (deletion of the ballot paper, change of the list of public voting codes, etc.) would therefore be detected immediately (Cortier et al., 2020).

19. *E-voting shall be organized in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure. (○)*

The ballot is encrypted and sent to the server via an HTTPS channel, which adds a second layer of encryption and ensures integrity. On the other hand, the ballot is authenticated thanks to the signature derived from the voting code, it is not possible to modify the ballot while maintaining a valid signature. Finally, the integrity of the ballot is again ensured by the fact that the voter can verify the presence of his own ballot in the ballot box with his tracking number (Cortier et al., 2020). The open-source election system Belenios allows the use of homomorphic programming (Glondou, 2023) to carry out an election by keeping individual ballots secret, enabling their verification and simultaneously displaying the overall election results.

Currently, there is no formal, universal definition for End-to-End Verifiability (E2Ev) because the associative and commutative operators are inaccessible to symbolic analysis tools, which for example makes it impossible to analyze the following homomorphic property as stated in (Cortier, 2015):

$$enc(pk; v_1) * enc(pk; v_2) = enc(pk; v_1 + v_2) \quad (1)$$

where $*$ and $+$ are associative and commutative operators. Thanks to them it is possible to sum the contents of votes (v_1 and v_2) encrypted (enc) with the public key (pk) without further decrypting them individually.

After the election results have been evaluated and confirmed, voter lists including access codes as well as decryption keys should be deleted. The choice itself is archived and subsequently deleted.

20. *The e-voting system shall process and store, as long as necessary, only the personal data needed for the conduct of the e-election. (○)*

Voter lists are separate from the ballot box. After the election is over and the results are confirmed, the entire election, including voter lists containing email addresses, can be deleted.

21. *The e-voting system and any authorised party shall protect authentication data so that unauthorised parties cannot misuse, intercept, modify, or otherwise gain knowledge of this data. (○)*

Authentication data is encrypted on the election server, or on a third-party server in the case of using CAS. The voter will receive the password by e-mail, in case of losing the password, they can have a new password generated by the administrator.

22. *Voters' registers stored in or communicated by the e-voting system shall be accessible only to authorised parties. (○)*

The voter register is not public. It is updated by the server and made available to election administrators. In case of doubts about its integrity, the compliance of the voter registers with the ballot box can be checked by the voting code generator (authorized authority), which knows the link between the codes used to sign the ballot boxes and the voters. The voter list is accessible to the administrator and authorized authority, who should make it available to the electoral commission for review.

23. *An e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties. (Δ)*

The system does not allow you to find out the content of the submitted vote. The voter can only verify that the vote in the ballot box is the same as the one he cast.

The system is not resistant to coercive voting, when the voter would be influenced by the participation of a third person to make the election, if he voluntarily gave the third person a public imprint of the ballot submitted in front of him to verify the counting of the given vote in the ballot box (Cortier et al., 2019).

24. *The e-voting system shall not allow the disclosure to anyone of the number of votes cast for any voting option until after the closure of the electronic ballot*

box. This information shall not be disclosed to the public until after the end of the voting period. (○)

The counting option can only be activated after the voting is closed. Each decryption authority then performs the calculation on its own computer using its private key. After reaching the contribution threshold, the result is announced. Partial counting cannot be done during the election, because the counting operation can only be activated once and requires the active participation of the decryption guarantors.

25. *E-voting shall ensure that the secrecy of previous choices recorded and erased by the voter before issuing his or her final vote is respected. (○)*

The content of the voter's previously submitted ballot is always overwritten by the newly submitted ballot. The results of earlier elections are not archived for a long time.

26. *The e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous. (○)*

Tightness between the voter's identity and the expression of his vote is ensured by two means. The keys needed for decryption are generated and stored on separate, independent machines, managed by different persons or entities, as it is on the one hand the server and on the other hand the decryption authorities chosen by the electoral commission. It is even unlikely that they all have the same operating system, for example. Thus, while a link is established between the voter and his encrypted ballot, it is not possible to establish a link between the voter and the cast of the vote. During analysis, the keys necessary for decryption remain on separate, independent computers managed by different people or entities. Voters' encrypted ballots are never deciphered. Belenios uses two decryption solutions depending on the voting method used: homomorphic counting or verifiable mixnets. In both cases, no link can be established between the expression of the vote and the voter (Cortier et al., 2020).

27. *Member States that introduce e-voting shall do so in a gradual and progressive manner. (Δ)*

In the Czech Republic, it is not possible to vote electronically in major political national elections, on the other hand, it is not prohibited to vote electronically in elections of private or public organizations. As electronic voting is only possible in minor elections, the rollout can be considered gradual and progressive.

28. *Before introducing e-voting, member States shall introduce the required changes to the relevant legislation. (A)*

Electronic voting in national elections has not yet been introduced in the Czech Republic. Electronic voting within organizations should be governed by statutes and other legal regulations.

29. *The relevant legislation shall regulate the responsibilities for the functioning of e-voting systems and ensure that the electoral management body has control over them. (O)*

Within the organization, responsibility can be defined by its own statutes, regulations or resolutions, including the designation of the election commission. In the event of a possible future introduction to national elections, a significant change in the country's laws will be needed.

30. *Any observer shall be able to observe the count of the votes. The electoral management body shall be responsible for the counting process. (A)*

The decryption of the tallied results is carried out by guarantors who are part of the electoral commission. Anyone with access to the election URL can verify the data used in the census based on publicly available data.

31. *Member States shall be transparent in all aspects of e-voting. (A)*

In the event of the eventual introduction of nationwide electronic voting, the state must be transparent, similar to the proposed procedure for electronic voting in organizations.

32. *The public, in particular voters, shall be informed, well in advance of the start of voting, in clear and simple language, about: any steps a voter may have to take in order to participate and vote; the correct use and functioning of an e-voting system; the e-voting timetable, including all stages. (O)*

The organization informs voters of the plan for conducting electronic elections in the invitation

to the meeting, the voter obtains information using the internal information system and e-mail. Detailed instructions should also always be available.

33. *The components of the e-voting system shall be disclosed for verification and certification purposes. (O)*

Belenios is open source, which is free to download and verify the code. Likewise, certain election data required for certification is publicly available.

34. *Any observer, to the extent permitted by law, shall be enabled to observe and comment on the e-elections, including the compilation of the results. (A)*

Anyone who knows the election URL can view the ballot box and public data. After the election result is decrypted, anyone can perform verification based on public data and third-party tools.

35. *Open standards shall be used to enable various technical components or services, possibly derived from a variety of sources, to interoperate. (A)*

Belenios is open source, and it also offers a tool for calculating a unique fingerprint as open source. The system allows the development of other third-party control systems.

36. *Member States shall develop technical, evaluation and certification requirements and shall ascertain that they fully reflect the relevant legal and democratic principles. Member States shall keep the requirements up to date. (A)*

State assessment and certification requirements should be developed for possible national elections in the future.

37. *Before an e-voting system is introduced and at appropriate intervals thereafter, and in particular after any significant changes are made to the system, an independent and competent body shall evaluate the compliance of the e-voting system and of any information and communication technology (ICT) component with the technical requirements. This may take the form of formal certification or other appropriate control. (O)*

We checked the functionality of the Belenios system by testing our own installation. A security analysis (Cortier et al., 2020) compares the fulfillment of the technical requirements

of the CNIL (La Commission nationale de l'informatique et des libertés, 2019). The Belenios voting platform meets levels 1 and 2 defined by the CNIL as well as level 3 depending on the chosen implementation (Cortier et al., 2020).

38. *The certificate, or any other appropriate document issued, shall clearly identify the subject of evaluation and shall include safeguards to prevent its being secretly or inadvertently modified. (X)*

Belenios allows anyone who knows the election URL to audit voting results. The standards for issuing the certificate have not yet been defined.

39. *The e-voting system shall be auditable. The audit system shall be open and comprehensive, and actively report on potential issues and threats. (Δ)*

The auditor regularly downloads the contents of the ballot box and checks its consistency. These tests ensure that no votes have disappeared and that only legitimate (properly signed) votes have been added. This audit is performed at least by an automatic program set up by the Belenios team, but it can also be performed by third parties. Software tools enabling these tests are available in the open-source Belenios code. On the other hand, the detailed specification of Belenios also allows to reprogram all the tests. In addition, voters can check at any time whether their ballot is in the ballot box. This last point means that security does not rely as much on attendance as with a traditional system. However, verification that this is consistent with the ballot box can be permanently done by the voting code generator (Cortier et al., 2020).

Belenios has an active academic community working on updates as well as third-party solutions for greater control and auditing of the elections made. Belenios publishes public data that allows for an audit. The Belenios system, compiled in the object-oriented programming language OCaml, is open source, including the auditing part. The academic community also informs about potential problems and threats in professional publications (Baloglu et al., 2021b).

40. *The electoral management body shall be responsible for the respect for and compliance with all requirements even in the case of failures and attacks. The electoral management body shall be responsible for the availability, reliability, usability and security of the e-voting system. (○)*

The electoral commission is responsible for the correctness of the election, which may also have tools for correction, including the possibility of extending the vote or repeating it.

41. *Only persons authorised by the electoral management body shall have access to the central infrastructure, the servers and the election data. Appointments of persons authorised to deal with e-voting shall be clearly regulated. (Δ)*

In the case of using the official Belenios installation, the server of the Belenios platform is hosted by the LORIA high-security laboratory. It thus benefits from associated services: controlled physical access, activity monitoring, and logical separation with other hosted services. The system is a stable version, with a limited number of services and regular updates. The list of people with physical and logical access to the server is limited and controlled (Cortier et al., 2020).

Only members of the elected electoral commission have access to voter lists including e-mails, the connection with the access code is handled by the authorized authority.

42. *Before any e-election takes place, the electoral management body shall satisfy itself that the e-voting system is genuine and operates correctly. (Δ)*

We verified the correct functionality of the system by installing it ourselves. Before the start of the election, the functionality of the system is verified by the administrator and other members of the election commission.

43. *A procedure shall be established for regularly installing updated versions and corrections of all relevant software. (X)*

In the case of using the official Belenios installation, the system developers themselves ensure that the system is kept up-to-date.

44. *If stored or communicated outside controlled environments, the votes shall be encrypted. (○)*

All ballots are encrypted.

45. *Votes and voter information shall be kept sealed until the counting process commences. (○)*

Only members of the election commission have access to personal information in the form of e-mail. Votes are encrypted, the electoral commission

only obtains information about the participation of individual voters in the vote.

46. *The electoral management body shall handle all cryptographic material securely.* (○)

Guarantors whose private keys are needed to decrypt the election results are advised to store the decryption keys securely. The authorized authority is informed of the need to handle voters' access codes with care.

47. *Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the electoral management body.* (Δ)

Voters and auditors immediately inform the electoral commission of suspicious events, in case of a suspicious event with a member of the electoral commission, the superior/chairman of the given organization should be informed immediately.

48. *The authenticity, availability, and integrity of the voters' registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be respected.* (○)

The list of voters is entered into the systems by the administrator based on e-mails delivered, for example, from the organization's internal systems. The list of voters does not change throughout the election and, including personal data in the form of e-mail, is available exclusively to members of the electoral commission. Voters should be familiarized with the protection of personal data under the GDPR, the organization can extend its personal data protection conditions beyond the requirements of the Belenios system itself, for example within the registration conditions for the organization's internal information system.

49. *The e-voting system shall identify votes that are affected by an irregularity.* (○)

As part of the audit carried out by the electoral commission, which can be carried out by anyone who has access to the URL of the given election, possible irregularities should be identified.

Discussion

Even though the recommendation of the Council of Europe is important for the member states, the verification of the internet voting system or the proposed method of the voting procedure

following the Recommendation of the Council of Europe is not a common part of the documentation. Even the documentation (Cortier et al., 2020) of the investigated French Belenios system evaluates its security only in accordance with the national requirements for electronic voting. The methodological procedures for evaluating electronic elections focus more on the system itself (Panizo Alonso et al., 2018) and only exceptionally evaluate the entire methodological procedure of real elections.

As evidenced by the assessment, elections in Ontario would not meet the requirements of the Council of Europe recommendations (Brunet and Essex, 2023). Token and envelope protocols are evaluated in more detail by academic staff often not directly connected to the development of the given system, while for example evaluating their strengths and weaknesses in relation to the recommendations of the Council of Europe CM/Rec(2017)5. The findings show that envelope protocols do not meet the requirements of the recommendation, while token protocols can meet the requirements if certain technical provisions are met (Bagnato, 2022).

The independent evaluation of voting procedures using the electronic voting system by a trusted authority is fundamental in terms of its application use by the general public, therefore it is advisable to strive for greater standardization of the evaluation and the way it is made available to all users of the system. The transparency of the i-voting system is important in terms of the Council of Europe (2017) recommendations and for building credibility. Similarly, research on the Swiss electoral system (Driza Maurer, 2019) calls for an emphasis on the transparency of the system. The requirement for public source code is also highlighted by Buckland et al. (2012) who conclude that the lack of transparency in the Australian e-voting system may negatively affect voter attitudes towards e-voting. Volkamer et al. (2011) also rate the transparency of an electoral system as crucial with respect to credibility. Few countries have developed adequate legislation or standards for online voting systems (Brunet et al., 2022).

Conclusion

From the described analysis, it follows that the proposed method of conducting a remote electronic secret election can to a certain extent meet most of the requirements

of the Council of Europe (2017) recommendation in the case of a less important election within the agricultural organization. The proposed procedure methodology does not provide for the certification required by Requirements 38 and 43. The proposed methodological procedure does not meet requirement 23, which requires the prevention of the possibility of transferring information about the choice to a third party. On the other hand, this requirement is better addressed by the possibility of repeated voting than in the postal elections that operate in many EU countries, and is less essential for elections in private institutions, since the verification of the voter's choice in this case can be legitimate. For example, in the case when a cooperative member/shareholder delegates a representative to express his will when electing the board. BeleniosRF should bring an improvement

in resistance to coercion (Chaidos, 2016). Points 27, 28, 29, 31, and 36, which deal primarily with requirements for the state, are obviously relevant to national elections to the Parliament, etc., even so, they are fulfilled to a certain extent for electronic voting in the organization. A greater level of security could be provided by the use of a third-party authentication system (CAS), which will simultaneously require two-factor authentication.

Acknowledgments

This work was conducted within the project "Smart environments - modeling and simulation of complex decision-making problems in intelligent systems" (2022B0010) funded through the IGA foundation of the Faculty of Economics and Management, Czech University of Life Sciences in Prague.

Corresponding author:

Ing. Tomáš Martinek

Department of Information Engineering, Faculty of Economics and Management

Czech University of Life Sciences Prague, Kamýcká 129, 165 00, Prague, Czech Republic

E-mail: martinek@pef.czu.cz

References

- [1] Accessibility Checker (2023) "Audit", Accessibility Checker. [Online]. Available: <https://www.accessibilitychecker.org/audit/> [Accessed: Feb 20, 2024].
- [2] Adida, B., de Marneffe, O., Pereira, O. and Quisquater, J. -J. (2009) "Electing a University President using Open-Audit Voting: Analysis of real-world use of Helios", *Proceedings of the 2009 Conference on Electronic Voting Technology/Workshop on Trustworthy Elections, EVT/WOTE*. [Online]. Available: https://www.usenix.org/legacy/event/evtvote09/tech/full_papers/adida-helios.pdf [Accessed: Feb 20, 2024].
- [3] Agbesi, S., Budurushi, J., Dalela, A. and Kulyk, O. (2023) "Investigating Transparency Dimensions for Internet Voting", In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Rønne, P., Germann, M. (eds) *Electronic Voting, E-Vote-ID 2023, Lecture Notes in Computer Science, Conference paper, Vol. 14230*. Springer, Cham, pp. 1-17. ISBN 978-3-031-43756-4. DOI 10.1007/978-3-031-43756-4_1.
- [4] Bagnato, D. (2022) "Recommendation CM/REC(2017)5 of the Council of Europe and an Analysis of eVoting Protocols", *Proceedings of the Central and Eastern European eDem and eGov Days*, pp. 169-178. ISBN 9781450397667. DOI 10.1145/3551504.3551519.
- [5] Baloglu, S., Bursuc, S., Mauw, S. and Pang, J. (2021a) "Election Verifiability Revisited: Automated Security Proofs and Attacks on Helios and Belenios", *2021 IEEE 34th Computer Security Foundations Symposium (CSF)*, pp. 1-15. ISBN 978-3-030-86941-0. DOI 10.1109/CSF51468.2021.00019.
- [6] Baloglu, S., Bursuc, S., Mauw, S. and Pang, J. (2021b) "Provably Improving Election Verifiability in Belenios", In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Rønne, P., Germann, M. (eds) *Electronic Voting, E-Vote-ID 2021, Lecture Notes in Computer Science, Conference paper, Vol. 12900*, Springer, Cham. DOI 10.1007/978-3-030-86942-7_1.
- [7] Belenios team (2023) "Who does what during a Belenios election?", Belenios. [Online]. Available: <https://www.belenios.org/instructions.html> [Accessed: Feb 20, 2024].

- [8] Blanchard, E., Gallais, A., Leblond, E., Sidhoum-Rahal, D. and Walter, J. (2022) "An Analysis of the Security and Privacy Issues of the Neovote Online Voting System", In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Ronne, P., Germann, M. (eds) *Electronic Voting*, E-Vote-ID 2022, Lecture Notes in Computer Science, Conference paper, Vol. 13553, Springer, Cham, pp. 1-18. ISBN 978-3-031-15910-7. DOI 10.1007/978-3-031-15911-4_1.
- [9] Brunet, J. and Essex, A. (2023) "Online Voting in Ontario Municipalities: A Standards-Based Review", In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Ronne, P., Germann, M. (eds) *Electronic Voting*, E-Vote-ID 2023, Lecture Notes in Computer Science, Springer, Cham, Conference paper, Vol. 14230, pp. 52-68. ISBN 978-3-031-43756-4. DOI 10.1007/978-3-031-43756-4_4.
- [10] Brunet, J., Pananos, A. D. and Essex, A. (2022) "Review Your Choices: When Confirmation Pages Break Ballot Secrecy in Online Elections", In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Ronne, P., Germann, M. (eds) *Electronic Voting*, E-Vote-ID 2022, Lecture Notes in Computer Science, Springer, Cham, Conference paper, Vol. 13553, pp. 36-52. ISBN 978-3-031-15910-7. DOI 10.1007/978-3-031-15911-4_3.
- [11] Buckland, R., Teague, V. and Wen, R. (2012) "Towards Best Practice for E-election Systems", In: Kiayias, A., Lipmaa, H. (eds) *E-Voting and Identity*, E-Vote-ID 2011, Lecture Notes in Computer Science, Vol. 7187, Springer, Berlin, Heidelberg pp. 224-241. ISBN 978-3-642-32746-9. DOI 10.1007/978-3-642-32747-6_14.
- [12] Cortier, V. (2015) "Formal verification of e-voting: solutions and challenges", *ACM SIGLOG News*, Vol. 2, No. 1, pp. 25-34. ISSN 2372-3491. DOI 10.1145/2728816.2728823.
- [13] Cortier, V., Dragan, C. C., Dupressoir, F. and Warinschi, B. (2018) "Machine-Checked Proofs for Electronic Voting: Privacy and Verifiability for Belenios", *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, Oxford, UK, pp. 298-312. ISSN 2374-8303. DOI 10.1109/CSF.2018.00029.
- [14] Cortier, V., Gaudry, P. and Glondy, S. (2019) "Belenios: A Simple Private and Verifiable Electronic Voting System", In: Guttman, J., Landwehr, C., Meseguer, J., Pavlovic, D. (eds) *Foundations of Security, Protocols, and Equational Reasoning*, Lecture Notes in Computer Science, Springer, Cham, Vol. 11565, pp. 214-238. ISBN 978-3-030-19052-1. DOI 10.1007/978-3-030-19052-1_14.
- [15] Cortier, V., Gaudry, P. and Glondy, S. (2020) "Analyse de sécurité de la plateforme de vote Belenios Conformité avec les recommandations 2019 de la CNIL", Belenios. [Online]. Available: <https://www.belenios.org/analyse-secu.pdf> [Accessed: Feb 20, 2024].
- [16] Council of Europe (2017) "Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting". [Online]. Available: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f [Accessed: Feb 20, 2024].
- [17] Czech Republic (2012) "Zákon č. 90/2012 Sb. - Zákon o obchodních společnostech a družstvech (zákon o obchodních korporacích)", Sbirka zákonů. [Online]. Available: <https://www.e-sbirka.cz/sb/2012/90/2023-07-01> [Accessed: Feb 20, 2024]. (In Czech).
- [18] Driza Maurer, A. (2019) "The Swiss Post/Scytal Transparency Exercise and Its Possible Impact on Internet Voting Regulation", In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Ronne, P., Germann, M. (eds) *Electronic Voting*, E-Vote-ID 2019, Lecture Notes in Computer Science, Vol. 11759, pp. 83-99. ISBN 978-3-030-30625-0. DOI 10.1007/978-3-030-30625-0_6.
- [19] Driza Maurer, A., Volkamer, M. and Krimmer, R. (2023) "Council of Europe Guidelines on the Use of ICT in Electoral Processes", In: Katsikas, S., et al. *Computer Security. ESORICS 2022 International Workshops*, Lecture Notes in Computer Science, Springer, Cham, Vol. 13785, pp. 585-599. ISBN 978-3-031-25459-8. DOI 10.1007/978-3-031-25460-4_34.
- [20] Glondy, S. (2023) "Belenios specification: Version 2.1". [Online]. Available: <https://www.belenios.org/specification.pdf> [Accessed: Feb 20, 2024].

- [21] Chaidos, P., Cortier, V., Fuchsbauer, G. and Galindo, D. (2016) "BeleniosRF: A Non-interactive Receipt-Free Electronic Voting Scheme", *CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, pp. 1614-1625. ISBN 978-1-4503-4139-4. DOI 10.1145/2976749.2978337.
- [22] Kánská, E., Jarolínek, J., Hlavsa, T., Šimek, P., Vaněk, J. and Vogeltanzová, T. (2012) "Using social networks as an integration tool in rural areas of the Czech Republic - agricultural enterprises", *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, Vol. 60, No. 4, pp. 173-180. ISSN 1211-8516. DOI 10.11118/actaun201260040173.
- [23] Kořínková, J., Čížková, Z. and Němčík, L. (2017) "*I 70 COOP*". ISBN 978-80-87118-11-5.
- [24] La Commission nationale de l'informatique et des libertés (2019) "*Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet: NOR: CNIL1917529X*", Légifrance. [Online]. Available: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038661239> [Accessed: Feb 20, 2024]. (In French).
- [25] Martínek, T. and Malý, M. (2024) "Evaluation of the I-Voting System for Remote Primary Elections of the Czech Pirate Party", *Acta Informatica Pragensia*, Vol. 13, No. 3, pp. 395-417. ISSN 1805-4951. DOI 10.18267/j.aip.249.
- [26] Martínek, T. and Tyrychtr, J. (2024) "A questionnaire survey of expected characteristics of i-voting systems among students and graduates of agricultural colleges [Data set]", Zenodo. [Online]. Available: <https://zenodo.org/records/11234690> [Accessed: May 21, 2024].
- [27] Panizo Alonso, L., Gascó, M., Marcos del Blanco, D. Y., Alonso, J. Á. H., Barrat, J. and Moreton, H. A. (2018) "E-Voting System Evaluation Based on The Council of Europe Recommendations: Helios Voting", *IEEE Transactions on Emerging Topics in Computing*, Vol. 9, No. 1, pp. 161-173. ISSN 2168-6750. DOI 10.1109/TETC.2018.2881891.
- [28] Rodríguez-Pérez, A. (2022) "The Council of Europe's CM/Rec(2017)5 on e-voting and Secret Suffrage: Time for yet Another Update?", In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Ronne, P., Germann, M. (eds) *Electronic Voting, E-Vote-ID 2022, Lecture Notes in Computer Science*, Conference paper, Vol. 13553. Springer, Cham, pp. 90-105. ISBN 978-3-031-15910-7. DOI 10.1007/978-3-031-15911-4_6.
- [29] Rysová, H., Kubata, K., Tyrychtr, J., Ulman, M., Šmejkalová, M. and Vostrovský, V. (2013) "Evaluation of electronic public services in agriculture in the Czech Republic", *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, Vol. 61, pp. 473-479. ISSN 1211-8516. DOI 10.11118/actaun201361020473.
- [30] Valimised.ee (2023) "*Statistics about Internet voting in Estonia*", Valimised.ee. [Online]. Available: <https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia> [Accessed: Feb 20, 2024].
- [31] Volkamer, M., Spycher, O. and Dubuis, E. (2011) "Measures to establish trust in internet voting", *ICEGOV '11: Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance*, Tallinn, Estonia, pp. 1-10. ISBN 978-1-4503-0746-8. DOI 10.1145/2072069.2072071.

Příloha J: Článek Digitální nástroje, demokratické affordance a participace v síťové straně: Česká pirátská strana

MARTÍNEK, Tomáš a Michal MALÝ, 2024. Digital Tools, Democratic Affordances and Participation in Networked Party: the Czech Pirate Party. *Acta Politologica* [online]. ISSN 1803-8220.

/PŘIJAT K UVEŘEJNĚNÍ - 14. října 2024 bylo zasláno potvrzení o přijetí článku redakcí Acta Politologica zastoupené šéfredaktorem doc. PhDr. Milošem Brunclíkem, Ph.D. k uveřejnění ve speciálním vydání Digitalization of Political Parties: Challenges and Solutions, kde hostujícími editory jsou Oscar Barberà (University of Valencia) a Jasmin Fitzpatrick (Johannes Gutenberg-Universität Mainz)/

Digital Tools, Democratic Affordances and Participation in Networked Parties: The Czech Pirate Party

Tomáš Martínek, Michal Malý¹

Abstract

The article explores the Czech Pirate Party, identified as a networked party that utilizes digital participatory tools. The study analyzes how software design and usage norms influence the quality and extent of member participation. The Czech Pirate Party serves as a relevant case study due to its early adoption of digital tools for internal deliberation and voting, as well as its transition from a parliamentary party in 2017 to a governing party in 2021. The research findings indicate that, despite the inclusive nature of the party's participatory processes, voter turnout remains stable but relatively low. This suggests that inclusivity alone may not be sufficient to increase participation rates. The study also highlights that exclusive membership, involving a more selective process for admitting new members, may contribute to stable participation, though it can also limit the expansion of the party's membership base. The findings provide insights that may be valuable for further research on digital parties and their internal democratic processes, illustrating how digital platforms can influence member engagement in decision-making.

Key words: Pirate Party, Networked Parties, Digital Party, Intra-party Voting, Deliberation, Digital Democratic Affordance, Participation Platforms

Introduction

The development of ICT has led to the emergence of parties whose internal processes and communication are based on digital participatory tools that draw from the logic of corporate entities (Gerbaudo 2019). These parties have been described in various ways as cyber-parties (Margetts 2006), anti-elitist cyber-parties (Hartleb 2013), connective parties (Bennett et al. 2018), and digital parties (Gerbaudo 2019, 2021). Deseriis (2020a) in his essay differentiates digital parties into platform and networked, with platforms characterized as centralized and networked as decentralized. Liou et al. (2019) discuss open and closed platforms, offering a parallel to Deseriis' later distinction between networked and platform parties. While open platforms mirror networked parties in their decentralized, participatory nature, closed

¹ Tomáš Martínek, Ph.D. Student, Department of Information Engineering, Faculty of Economics and Management, Czech University of Life Sciences Prague, Czech Republic, martinekt@pef.czu.cz, ResearcherID: GYU-6458-2022, ORCID: 0000-0002-4295-0886.

Michal Malý, Ph.D. Student, Institute of Political Studies, Faculty of Social Sciences, Charles University, Czech Republic, michal.maly@fsv.cuni.cz. ResearcherID: GXF-9941-2022, ORCID: 0000-0002-4782-2672.

Tomáš Martínek prepared this article within the project "Smart environments - modelling and simulation of complex decision-making problems in intelligent systems" (2022B0010) funded through the IGA foundation of the Faculty of Economics and Management, Czech University of Life Sciences in Prague.

platforms resemble platform parties, where decision-making is centralized. Current research has primarily focused on platform parties, specifically the Movement of 5 Stars and Podemos, which are characterized as centralized, using participatory platforms for plebiscitary legitimization of party leadership, without allowing the membership base to actively propose initiatives for voting (Deseriis, Vittori 2019; Gerbaudo 2021; de Nadal 2021; Vittori 2020). Research on networked parties is not yet extensive (exceptions include Deseriis 2022 and 2023b; Voda, Vodová 2020). This article examines the Czech Pirate Party, identified by Deseriis (2020a) as a networked party. As an early adopter of digital participatory tools for deliberation and voting, the Czech Pirate Party serves as a compelling case for studying digital parties. Its evolution from a parliamentary party in 2017 to a governing party in 2021 further underscores its significance for research. A detailed case study of the Czech Pirate Party provides valuable insights into the operation of participatory and voting platforms, offering broader implications for the study of networked parties.

This paper builds on Deseriis' framework of digital democratic affordances by examining how software design and usage norms impact the quality and scale of participation over time. It goes beyond Deseriis' focus on agenda setting to analyze the dynamic evolution of participation and deliberation, assessing how these factors influence stable and active member engagement (Deseriis 2023a; Vittori 2019). By focusing on the Czech Pirate Party, the article explores the role of its internal participatory platforms in either facilitating or hindering democratic engagement, thereby contributing to the broader debate on digital democratic participation. Therefore, we pose the following research question: To what extent software design and norms of use on digital democratic platforms influence participation in the Czech Pirate Party?

The article will be organized as follows: After the introduction, we will first discuss the current state of research on digital parties, followed by a literature review on networked parties. This will be followed by a section on case selection and description, methodology, and data used. In the empirical section, we will analyze software design, norms of use, and participation, which will be followed by a discussion of the findings. The article will conclude with a comparison of our results with existing research on digital parties.

Theoretical Framework

Political Parties, Digital Platforms and Internal Participation

Since the 2000s, with the expansion of the internet, there has been a growing body of research examining its impact on political parties, particularly in terms of communication and organization (Castells 2001). In recent years, this literature has increasingly focused on the influence of digital technologies on organizational processes, leading to the identification of a potential new type of political party: the digital party (for an overview, see Barberà et al., 2021). The first mention of the term "digital party" is found in Norris's study (2001), which, however, focused more on global parties and their websites, without addressing deeper organizational elements.

Margetts (2006) expanded this discussion by introducing the concept of the "cyber party," which she described as a potential future type of political party. Cyber parties use web-based technologies to engage voters, offering more flexible and direct interactions compared to traditional parties. While this digital shift enabled innovative campaign strategies and cost-effective engagement, it also brought challenges such as social exclusion (due to unequal access to technology) and the risk of superficial involvement.

With the emergence of new parties such as the Pirate Parties and the Five Star Movement (FSM), the need for new conceptualizations of cyber parties became evident. Hartleb (2013) categorized these into two main types: strictly authoritarian and participatory cyber parties. Strictly authoritarian cyber parties are marked by centralized control, where leadership tightly manages decision-making processes and limits broader member involvement. On the other hand, participatory cyber parties, like the Pirate Party, emphasize member engagement through digital platforms, promoting transparency and decentralized decision-making, as seen in the "liquid democracy" model.

Building on these ideas, Bennett and his colleagues (2018) introduced the concept of "connected parties," which rely heavily on digital technologies to create a network of supporters and replace traditional party structures and functions. Their study included cases such as the Danish Alternativet, Icelandic Píratar, and Spanish Podemos, highlighting how these parties integrate technology into their core operations.

Klimowicz (2018) further contributed to this discourse by developing the concept of "network parties." These parties are characterized by horizontal, decentralized structures and the use of open-source software for communication, decision-making, and public engagement. Network parties emphasize transparency, ethical behavior, and participatory democracy, often employing digital tools for crowdsourced decision-making and policy development. Examples like Spain's Podemos, Barcelona en Comú, Poland's Partia Razem, and Iceland's Píratar illustrate how these parties challenge traditional political models and promote citizen involvement in governance.

In more recent research, digital parties have been empirically tested, particularly regarding participation within digital party platforms. Gerbaudo (2018) offered a nuanced conceptualization of the digital party, focusing not just on the implementation of digital technologies, but on their role in promoting internal party democratization. He argued that digital technologies should help transcend the crisis of representative politics by offering citizens more active participation in public affairs. However, Gerbaudo's analysis of FSM and Podemos showed that despite their participatory platforms, party leadership often maintains control, limiting member engagement. The participation process in these cases is often plebiscitary, with members only responding to proposals put forward by the leadership.

Deseriis and Vittori (2019) also examined participatory processes within the platforms of FSM and Podemos, criticizing the static measurements often used in the analysis of intra-party democracy (IPD). Their study, focusing on the technical design of platforms, norms of use, and actual participation over time, confirmed Gerbaudo's findings. They observed that both FSM and Podemos struggle with maintaining stable turnout and active discussions, and

neither party has shown significant interest in redesigning their platforms to encourage greater and more stable participation.

Further studies (Deseriis, 2020a, 2021; Mosca, 2020; Vittori 2019), highlight the need to include the technical setup of platforms and the rules governing their use in analyses. These works emphasize that the democratic vision of digital parties and its fulfillment depend significantly on the design and functioning of these platforms over time.

Networked Parties and Internal Participation

Although it might seem that digital parties have failed in their goal to re-engage people with politics and participation, current studies only cover one side of the coin. Building on Hartleb's earlier work, Deseriis (2020b) postulated the existence of two ideal-type digital party models: the platform party and the networked party. The platform party represents a centralized organization led by a charismatic hyper-leader. This type of party corresponds to the previous analysis results of FSM and Podemos, indicating that platforms are controlled by the party's central office and that their participatory outcomes are plebiscitary in nature (De Blasio, Sorice 2020; Gerbaudo 2018 and 2021; Deseriis, Vittori 2019). In contrast, the networked party represents the cyber-optimistic version of a digitally decentralized party. Deseriis (2020b) characterizes the networked party using seven features, which he contrasts with the platform party: non-exclusive membership, decentralization, leadership function, bottom-up division of labor, collective agenda setting, hybrid participation, and scalable deliberation.

First, non-exclusive membership allows members to belong to other parties or civil society organizations, fostering broader collaboration. Second, decentralization ensures that decision-making is not centralized in the party headquarters but occurs at various organizational levels, often locally or regionally. Third, the leadership function is distributed among individuals based on their expertise and contributions, reducing dependence on a single charismatic leader. Fourth, tasks and responsibilities are divided from the bottom up, with members deciding who takes on certain roles based on their skills and input. Fifth, collective agenda-setting involves members actively participating in shaping the party's program through discussions and voting at different organizational levels. Sixth, hybrid participation combines online and offline methods, allowing members to engage in discussions and decision-making both in physical meetings and through online platforms, ensuring broader member involvement. Finally, scalable deliberation is designed to facilitate effective decision-making even with a large number of members, utilizing sophisticated online platforms for voting and discussion (Deseriis 2020b). Deseriis provides several examples of networked parties. These include the Pirate Parties in countries such as Sweden, Germany, Iceland, and the Czech Republic. Additionally, he mentions Barcelona en Comú and the X Party in Spain. De Blasio and Viviani identify the fundamental difference between platform and networked parties as the functioning and role of participation within these parties. Specifically, they highlight the distinction between plebiscitarian participation in platform parties and collective agenda setting in network parties (De Blasio, Viviani 2020).

This difference in participation models is further illuminated by Deseriis' (2023a) theoretical framework for digital democratic affordances (DDA), which analyzes how the design and functionality of participatory platforms can either enable or constrain democratic engagement within political parties. These platforms are categorized into two types: instrumental and emergent. While instrumental platforms are integrated into existing governance systems and operate within traditional modes of governance, emergent platforms seek to transcend these established structures and develop new forms of democratic participation, as seen in the case of digital parties. Deseriis' concept responds to existing taxonomies, which have inadequately considered the influence of software design on the quality and democratic nature of participation (Dahlberg 2011).

Deseriis identifies four key dimensions of DDA: software design, usage norms, scale of participation, and quality of participation. Software design refers to the architectural configuration of the decision-making software and platforms, which include specific features and their relation to democratic processes. For instance, the integration of online voting into deliberative platforms can affect how democratic processes are perceived and regulated (Deseriis 2023a: 16). Usage norms determine how technologies are practically employed and how they impact the effectiveness and legitimacy of DDA. For example the decline in the use of the LiquidFeedback platform following the German Pirate Party's decision that approved proposals would not be binding illustrates how usage norms can influence the political impact of these tools (Deseriis 2023a: 17). Scale of participation is understood as the ability of DDAs to facilitate large-scale citizen engagement, which plays a crucial role in legitimizing representative institutions. Such participation helps to reinforce representative claims and extend political mobilization beyond traditional electoral mechanisms. However, this scale can also introduce a plebiscitarian character, potentially lacking the depth needed for meaningful democratic engagement (Deseriis 2023a: 17). As for quality of participation, lowering participation barriers through digital tools does not automatically lead to more substantive democratic processes. Quality hinges on fostering deliberation, ensuring diversity of viewpoints, and achieving practical inclusivity to avoid reinforcing existing inequalities (Deseriis 2023a: 17).

While Deseriis provides a useful framework for analyzing DDA, it is essential to expand this framework with a dynamic approach to the dimensions of participation quality and scale. Participation quality should not be regarded as static; rather, it varies depending on the context in which the platform is used and the interactions among participants. Higher participation quality can be achieved if the platform supports deliberation and inclusive discussions, extending beyond mere voting. Similarly, the scale of participation is subject to changes over time, influenced by factors such as political campaigns, organizational changes, or specific events. This perspective aligns with Vittori's analyses (2019), which demonstrate that the quality and scale of participation on digital platforms—exemplified by parties like Podemos and the Five Star Movement—are not constant but instead shaped by various organizational and political factors. Vittori's work reveals that while these platforms may initially attract a significant number of participants, sustaining political mobilization and

relevance is crucial for maintaining long-term engagement. By considering how participation quality and scale evolves over time, as both Deseriis' framework and Vittori's insights suggest, we can better understand the functionalities and limitations of DDAs and, eventually and explore how digital platforms can be designed to effectively contribute to democratic processes.

Based on Vittori's work (2019), we expect that in networked parties (CPP), bottom-up agenda setting and decentralization will empower members to not only vote on existing proposals but also to initiate their own consultations and proposals, engage in discussions, provide feedback on others' ideas, and contribute alternative perspectives, which, unlike platform parties, will foster more stable and sustained participation and deliberation within intra-party consultations, ensuring that member activity remains consistent over time.

Methodology

Case Selection and Description

We investigate the Czech Pirate Party (CPP), a small networked party that is considered part of the original family of digital parties (Jääsaari, Šárovec 2021), making it a particularly relevant case study for providing one of the first analyses of networked parties, which have so far been absent in research, limiting a more comprehensive understanding of how digital parties function. The CPP was selected for this study because it has utilized a digital structure as the foundation of its operations since its inception, particularly in the areas of internal discussions and party voting processes. This makes the CPP an exemplary case for expanding the existing body of research on digital parties, which, to date, remains relatively limited in terms of the number of cases studied. Moreover, the inclusion of this case provides valuable insights from Eastern Europe, a region that has been underexplored in the current scholarship on digital parties. Previous research has primarily focused on the Swedish and German Pirate Parties, particularly regarding intra-party democracy (Bolleyer et al. 2015), organizational frameworks (Cammaerts 2015), programmatic agendas (Jääsaari, Hildén 2015), and descriptions of electoral results (Otjes 2019). There are also accounts of the participation platform LQFB in the German Pirate Party (Deseriis 2020b; 2022).

The Czech Pirate Party was established in 2009 through an online petition initiated by programmer Jiří Kadeřávek and quickly garnered the necessary 1000 signatures. Advocating for internet freedom, copyright reform, and open access to information, the party first gained political traction by winning a Senate seat in 2012, marking a significant milestone as the world's first pirate party with national legislative representation. Further successes followed in the 2014 municipal elections, particularly in Prague. The 2017 parliamentary elections were a landmark, with the party winning 10.79% of the vote. Success continued with securing three seats in the 2019 European Parliament elections and acquiring three ministerial roles in the government formed in 2021, despite a significant reduced share of parliamentary seats.

Research on the Czech Pirate Party has so far focused on analyzing its entry into the parliament (Maškarinec 2020), an overview of its digital platforms (Jääsaari, Šárovec 2021),

analyses of anti-corruption communication through a lens of populism (Naxera 2023), intra-party democracy dynamics (Malý 2024), evaluation of i-voting platform (Martínek, Malý 2024), hybridization of digital structures (Folvarčný, Kopeček 2024) and deliberative communications in entering municipal coalitions (Voda, Vodová 2020).

Data and Methods

In this article, we employed a mixed-methods approach. For the sections on Software Design and Norms of Use, we conducted a qualitative analysis using party documents and the party's websites to examine the functioning of participatory platforms, Helios and Pirate Party Forum, and their integration into the party's operations. We analyzed party statutes to assess the platforms' alignment with statutory norms, and we utilized the party's internal Wikipedia, which provides detailed information on each platform used within the party. Additionally, we used the collection of internal regulations that describe the procedures for online voting and discussions. Furthermore, we conducted email correspondence with the head of the Administrative Department of the CPP to obtain supplementary information on the development of individual consultations, particularly on aspects not covered by the aforementioned public sources.

To analyze participation (e.g., its quality and scale), we gathered data from the Pirate Party Forum, focusing specifically on consultation threads that occurred between 2017 and 2023 (Malý, Martínek 2024). The objective of this data collection was to provide a quantitative assessment of various aspects of these consultations. In total, 103 consultations² from the original dataset *Participation in the Czech Pirate Party*³ were analyzed. The analysis distinguishes between two main aspects of participation: scale and quality. To assess the scale of participation, we utilized several metrics. First, voter turnout was measured as the number of members participating in the voting process for each consultation. We also recorded the number of eligible voters, defined as the total number of party members with voting rights, to understand the potential scale of participation. Additionally, we examined the number of votes received by the winning options, which provides insights into the level of support for the final decision and indicates whether the results exhibit a plebiscitary character. Another key metric was the number of days voting was open for each consultation, offering a temporal dimension to participation. For each of these metrics, we calculated annual averages to identify trends and changes over time. On the other hand, to gauge the quality of participation, we focused on the number of comments within the consultation threads. This metric serves as an indicator of member engagement and the extent of discussions, providing a deeper understanding of the deliberative aspect of each consultation topic.

² In addition to consultations, the CPP also conducts primaries. However, while primaries are becoming an increasingly common tool in political parties (see Scarrow et al. 2022), consultations remain less prevalent. For this reason, we chose to focus our analysis exclusively on consultations, which have not been thoroughly examined in the existing literature.

³ The dataset is available upon request on the Zenodo platform: <https://zenodo.org/records/13629499>.

Analysis

The CPP Digital and Participatory Tools

The Czech Pirate Party operates a comprehensive internal system composed of various interconnected tools, primarily based on open-source platforms. Table 1 outlines the party's main systems, detailing their functions, development processes and user access methods.

Table 1: Information systems of the Czech Pirate Party

Function	Tool	Development	Users	URL
I-voting	Helios Voting	Open Source with modifications	Members	helios.pirati.cz
Discussion, Nomination	phpBB forum	Open Source	Everyone	forum.pirati.cz
Surveys (non-binding)	LimeSurvey	Open Source	Members	ankety.pirati.cz
Membership Management	Octopus	Self developed	Administrators, Leadership	chobotnice.pirati.cz
Authentication SSO (Pirate Identity)	KeyCloak	Open Source	Members, Registered supporters	auth.pirati.cz
Voice meetings	Jitsi	Open Source	Everyone	jitsi.pirati.cz
Informal discussion	Zulip	Open Source	Members, Registered supporters	zulip.pirati.cz
Wiki	DokuWiki	Open Source	Everyone	wiki.pirati.cz
Project management	Redmine	Open Source	Members, Everyone	redmine.pirati.cz
Contact records	OpenLobby	Self developed	Everyone	evidence.pirati.cz
Learning	Moodle	Open Source	Members, Registered supporters	moodle.pirati.cz
Registration new user	Onboarding	Self developed	Everyone	nalodeni.pirati.cz
Register of contracts	Contracts	Self developed	Everyone	smlouvy.pirati.cz
Reimbursement	PiroPlaceni	Self developed	Administrators, Everyone	piroplaceni.pirati.cz
Donations	Donations Jekyll	Open Source with modifications	Everyone	dary.pirati.cz

Source: own elaboration based on (Pirates 2022a).

One of the central components of this system is the Octopus platform, developed by the party to manage its membership registry. This platform handles personal data, public profiles, identity verification requests, and membership fee payments, all in compliance with GDPR regulations. For new supporters, the party utilizes the Onboarding system, which provides access credentials to registered supporters. All party applications, managed by the technical department, are integrated into a Single-Sign On (SSO) system through Keycloak, an open-source identity and access management tool that enhances security with two-factor authentication (Chatterjee, Prinz 2022).

The party's key participation tools include a discussion Forum PhpBB (Patel et al. 2020) and the i-voting system Helios (Martínek, Malý 2024). The Surveys system is employed to

gather opinions from party members and external individuals. For informal discussions, the Zulip platform is used, while live meetings of party bodies are conducted via the video conferencing tool Jitsi. The Pirate Wiki is utilized for managing the party's regulations and other documents. Project management, including departmental requests, is facilitated through the Redmine system. Educational courses are made available to members and registered supporters via Moodle. Additionally, the party's Contracts system publicly discloses all party contracts, while the Reimbursement system provides public access to the party's financial management. The OpenLobby application records lobbying contacts publicly, and the Donations system is used for fundraising.

Software Design

Among the primary participatory tools of the Czech Pirate Party (CPP) are the internet forum (Pirates 2020a) and the Helios voting platform (Pirates 2020b). The forum is largely accessible to the public; however, there are sections restricted to members, registered supporters, or users with regional limitations (Pirates 2020c). Visually, the forum appears outdated, reminiscent of the design of online forums from the early 2000s (Malý 2024). This outdated appearance is due to the fact that the forum was established concurrently with the party's founding in 2009 and has not undergone significant visual changes since then.

The main purpose of the forum is to facilitate communication, which can be either binding (e.g., related to voting) or non-binding, encompassing various topics related to politics and internal party life. The forum also serves as a platform for the organization and communication of regional and local associations (Jääsaari, Šárovec 2021). Although the Helios voting system is separate from the forum, discussions concerning specific votes take place there, and proposals that meet all necessary conditions are subsequently submitted for voting on Helios.

Non-binding discussions also occur outside the forum, such as on the internal platform Zulip (Pirates 2024c) or offline, but only on the forum can amendments to votes be proposed or procedural actions challenged. Discussions on the forum occur in the form of posts, which can be appreciated with so-called "thanks," serving as an indicator of popularity but without influencing the course of the discussion⁴. Posts are arranged chronologically, and this order cannot be changed (Pirates 2023a). Voting in the form of polls on the forum serves either as non-binding surveys or as a tool for gaining support for member consultation (see more in the Norms of Use section).

However, the forum polls had their issues, especially due to the possibility for administrators to determine how each individual voted, leading to concerns about the party's democratic principles, particularly with the growing number of members (Martínek, Malý 2024). For this reason, it was decided in 2016 to move voting to the Helios platform.

Since 2016, the main electronic voting system of the Czech Pirate Party has been the open-source platform Helios Voting. This system uses homomorphic encryption to ensure the

⁴ "Thanks" can in some cases serve as preferences in the candidate selection process. This process happens most often in the case of nominations at regional level.

secrecy of individual votes while providing complete verifiability of the voting process (Adida et al. 2009). The Helios version 3 (Helios 2009) allows voters to verify that their vote was correctly cast and displays all submitted votes in encrypted form, enabling public verification of their correct counting.

The specific configuration of Helios used by the Czech Pirate Party, which displays the names of voters alongside the hash codes of their ballots, is resistant to Clash Attacks (Kusters et al. 2012). However, this method reveals information about voters who did not participate, which contradicts the Recommendation CM/Rec(2017)5 (Council of Europe 2017). In 2024, the Czech Pirate Party therefore modified the Helios system to display the hash codes of other voters in the ballot box only after the voting has closed (Martínek, Malý 2024). This step eliminated the public availability of information about who had already voted during the ongoing election. However, election administrators still have access to this information, giving them an advantage over ordinary voters.

To ensure the credibility of the results, the hash codes of all voters' ballots are published after the voting ends, allowing verification that no one voted on behalf of someone else. Although the public availability of these hash codes in connection with specific voters is useful for transparency, it may pose a future risk if the public key used in the election were compromised, potentially revealing the contents of individual votes (Cortier et al. 2014; Martínek, Malý 2024).

Voting in the Helios system is managed by administrators, usually representatives of the party's administrative department. The list of voters for a specific vote on the forum is imported using an API created by the party's technical department from the member register maintained in the Octopus system. As mentioned earlier, the forum is the first step before the actual voting, where discussions on the proposal take place, and where a link to the Helios system is provided once the vote is created. Voters are informed via email, SMS, and other party communication channels (Martínek, Malý 2024).

On the voting homepage, voters have access to basic information about the election, including a description of the voting options, links to more detailed information on the forum, the election date, information about the administrator and election trustees, a list of voters, and access to the public ballot box. After selecting voting options in the voting booth, the ballot is encrypted (Martínek, Malý 2024).

The voter then must authenticate through the Pirate Identity (Single-Sign On Key) and submit their vote (Pirates 2022b; Pirates 2023c). This identity also serves as a login credential for the rest of the Pirate systems, including the forum. It is essentially a similar tool to, for example, a bank identity. The CPP requires that the member or registered supporter use their legal name in the format *Name.Surname* within the identity to allow identification in discussions.

After submitting the vote, the voter is informed of the successful delivery of the ballot, including a tracking hash⁵, which allows them to verify the delivery of the ballot to the ballot box. The same information is also sent to their email (Martínek, Malý 2024).

To reduce the risk of coercion, the voter can submit the ballot multiple times, with only the last one being valid. After the voting closes, the trustees decrypt the overall result, which is then published. Voters can then verify the presence of their tracking hash in the publicly accessible ballot box and audit the entire voting process. The result is also recorded on the forum, where the administrative department subsequently ensures the implementation of the voting results (Martínek, Malý 2024).

Norms of Use

Members gain voting rights immediately upon acceptance by the regional branch forum thread on the Pirate Party's platform, after which the process is finalized within the information system by the administrative department. Registered supporters generally do not have voting rights but are allowed to participate in discussions, among other activities (Pirates 2024b). Contributions from anonymous visitors are added only after approval by an administrator (Respondent 1). The administrative department also oversees the moderation of discussions on both the Forum and Zulip, ensuring that they adhere to the Rules of Online Communication (Pirates 2023a), which, for example, prohibit racism.

To initiate a group of members proposal, the required threshold is set at twice the square root of the number of members present (Pirates 2024e); however, it must not be less than one percent nor more than twenty percent of those present. For instance, with a total membership of 1,238, thirty-six votes are necessary, representing 2.9% of the membership (Malý 2024). Support for a proposal is gathered through public endorsements or forum polls. For a proposal to be eligible for voting, it must secure sufficient support within 24 hours, while ensuring that the opposition does not exceed the support. To include the proposal on the national forum agenda and subject it to a full vote, it must secure twice the square root of the total membership, which would be seventy-two votes, or 5.8% of the membership (Malý 2024). Subsequently, a forum discussion is initiated, which can be chaired by the chairman, vice-chairman, a member of the administrative department, or another designated member or registered supporter (Pirates 2024d). During the forum discussion, counterproposals can also be submitted, which must similarly garner the support of a group of members to proceed (Pirates 2023b).

The specific form of the resolution to be voted on is determined by the chair of the meeting. Members may also submit a motion against the chair for consultation on the wording of a question if its title is misleading (Respondent 1). For a proposal to be adopted, it must be approved by a majority of those voting, or by two-thirds of those voting if it is a fundamental proposal (Pirates, 2023b). The standard vote consists of two rounds. The first round is a vote on acceptability, where voters may choose from none to all options. The options selected by

⁵ The tracking hash in the Helios Voting system is a unique identifier that allows the voter to verify that their vote has been correctly recorded without compromising their anonymity.

the required majority will proceed to the second round. In the second round, only those options that received votes in the first round are voted on. In the event of a tie, the result of the first round is considered. If the result is the same in the first round, the outcome is decided by drawing lots (Pirates, 2023b).

The administrative department is responsible for implementing the results, addressing objections, and overseeing the election process to ensure compliance with the party's regulations. The party's control commission serves as the supervisory body, and any disputes are resolved according to the Arbitration Rules before the party's Arbitration Commission. Any decision may be subject to further review by the National Forum of the party (Pirates, 2023b; Pirates 2024a; Respondent 1). All party consultations are binding.

Participation

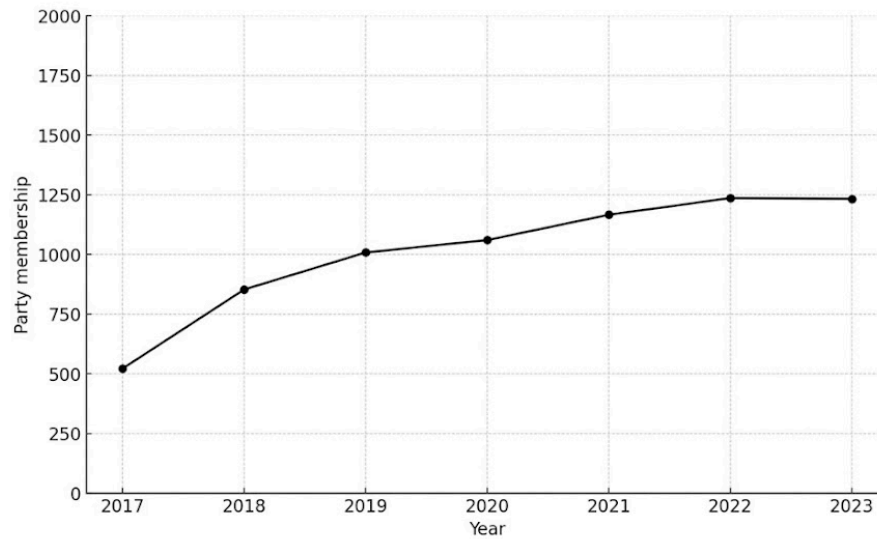
Unlike parties like Podemos or the Five Star Movement, the CPP does not permit non-exclusive membership through a simple registration and verification process (Deseriis, Vittori 2019; Gerbaudo 2019; Vittori 2020). To become a member of CPP, citizens must register through the Onboarding platform, with the registration process managed by the leadership of a regional or local organization. Prospective members are required to participate in either an online or offline meeting where they introduce themselves and are typically asked about their programmatic and ideological commitments. Additionally, they are usually expected to attend one of the regional or local party events to demonstrate their interest. This admission process often takes weeks to months to complete (Malý 2024). Membership is also subject to a minimum fee of 8 euros per year. Thus, the CPP operates on a principle of exclusive membership, which is relatively uncommon among digital and especially networked parties.

Furthermore, the CPP offers a lighter form of cyber membership, known as registered supporter⁶ (Scarrows 2015). However, registered supporters are only permitted to vote in a limited number of instances, whereas full members have the right to vote in all cases and can propose consultations.

Figure 1 illustrates the evolution of CPP membership from 2017 to 2023. While the number of members is increasing, the total remains modest, with approximately 1,200 members, a figure that is significantly lower than those of other digital parties (Deseriis, Vittori 2019; Vittori 2020). The low membership numbers may be attributed to the exclusive membership process, which limits large-scale growth through simple registration.

⁶ The CPP does not archive data on the development of registered supporters, and therefore, these figures are not included in the figure 1.

Figure 1: Membership development in the CPP from 2017 to 2023



Source: Own elaboration based on consultations data from forum.pirati.cz and helios.pirati.cz (Malý, Martínek 2024)

As mentioned in the methodology section, we collected data on 103 consultations conducted between 2017 and 2023, with an average of 14.4 consultations per year. These consultations cover topics such as internal governance and organizational structure, policy and ideological decisions, financial and resource management, membership and disciplinary matters, as well as procedural and miscellaneous votes. As shown in Table 2, there are no significant fluctuations in the number of consultations, and the frequency remains relatively stable over time.

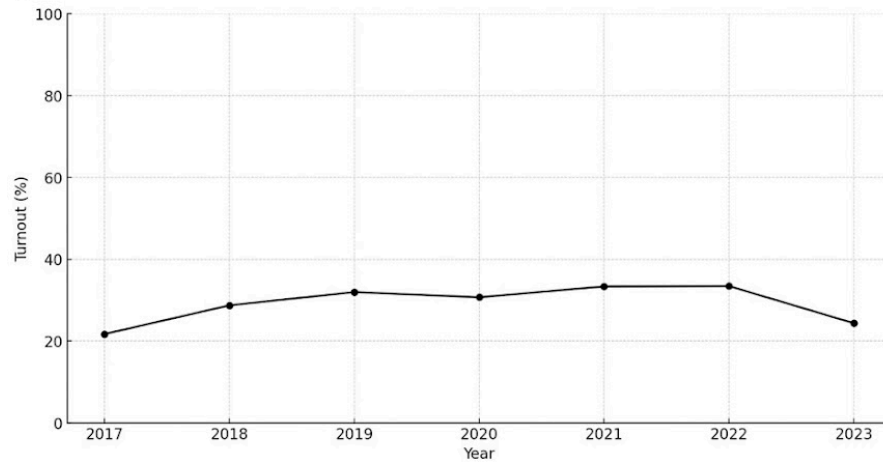
Table 2: Internal consultations per year in CPP

Year	2017	2018	2019	2020	2021	2022	2023
Number of consultations	12	11	9	13	22	17	15

Source: Own elaboration based on consultations data from forum.pirati.cz and helios.pirati.cz (Malý, Martínek 2024)

However, does an inclusive environment, where members can propose consultations, discuss, provide feedback, and even challenge their content, necessarily lead to stable turnout? To address this question, we averaged turnout data for each year to track its trend over time. As Figure 2 illustrates, the turnout rate remains relatively stable over time without significant drops or increases. Nevertheless, the overall turnout consistently hovers around 30%, which is somewhat surprising given the more inclusive conditions. This rate is comparable to the average participation levels observed in Podemos and the Five Star Movement (Deseriis, Vittori 2019). One possible explanation could be voter fatigue due to the high frequency of voting (Kostelka, Blais 2021), as in addition to consultations, the party also conducts internal primaries (see Martínek, Malý 2024).

Figure 2: Voter turnout in CPP consultations 2017-2023



Source: Own elaboration based on consultations data from forum.pirati.cz and helios.pirati.cz (Malý, Martínek 2024)

As Gerbaudo points out, intra-party ballots can often tend to be plebiscitary. The main reasons for this outcome, according to Gerbaudo, are the lack of opportunities for members to engage in discussions about the consultations, propose their own consultations, or influence the wording and timing of the questions, which are typically controlled by the party leadership (Gerbaudo 2019, 141-142). As a result, voting becomes a top-down tool rather than a participatory process.

As mentioned above, in the case of the CPP, members can propose their own consultations and participate in debates on the forum, where they can present alternative viewpoints and challenge the wording of the questions. Therefore, we expected that the voting outcomes in the CPP would not exhibit plebiscitary characteristics. In Table 3, we categorized the analyzed consultations according to the percentage of votes received by the winning option.

Table 3: Distribution of Consultations by Turnout Percentage Ranges

%	0-10 %	10-19 %	20-29 %	30-39 %	40-49 %	50-59 %	60-69 %	70-79 %	80-89 %	90-100 %
Count	0	1	0	0	11	21	22	19	20	9

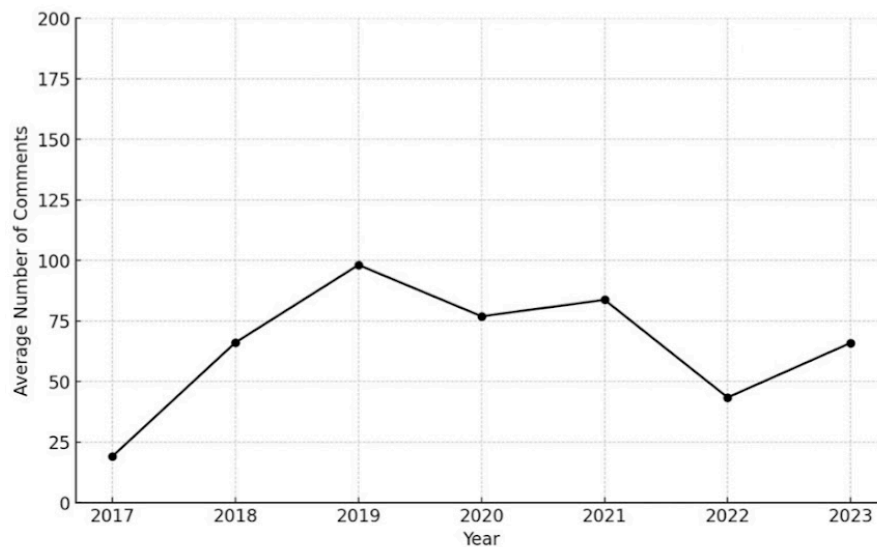
Source: Own elaboration based on consultations data from forum.pirati.cz and helios.pirati.cz (Malý, Martínek 2024)

Out of the consultations where the winning option received more than 80% of the votes, the majority were related to internal governance and organizational structure, with 10 such cases. Financial reports and audits accounted for 7 consultations, while strategic decisions, such as long-term goals and major policies, had strong support in 4 instances. Thus, it can be said that the high level of support is driven by various factors, which in only a few cases are related to the leadership's position (such as entering a coalition and joining the government). In most cases, the high support is for organizational matters. Another factor may be that 51 consultations offered more than two alternatives for members to vote on, which could contribute to the absence of plebiscitary outcomes. Additionally, the fact that voting typically

lasts for an average of three days, often spanning the weekend, may also contribute to the stability of turnout. This extended period likely allows more members the opportunity to participate in important consultations, which can also avoid plebiscitary outcomes.

To further analyze the discussions on the forum related to these consultations, Figure 3 shows that the average number of comments has remained stable over time, with a slight upward trend. The average number of comments per consultation stands at 69.5, which is relatively high given the party's size compared to other digital parties. This stability contributes positively to the quality of participation, which depends not only on lowering participation barriers but also on fostering meaningful deliberation, including a range of viewpoints, and achieving practical inclusivity to prevent existing inequalities from being perpetuated (Deseriis 2023a: 17). As Mosca (2020) demonstrated in his study, the average number of comments per law proposal in the Five Star Movement was 446 in 2014, but dropped to just 63 by 2017. The sustained level of comments in the CPP suggests continuous and active engagement, which may be attributed to the party's debate process allowing members to submit alternative proposals for voting.

Figure 3: Average number of comments in consultations from 2017 to 2023



Source: Own elaboration based on consultations data from forum.pirati.cz (Malý, Martínek 2024)

Discussion: Digital Democratic Affordance and Participation in a Networked Party

As stated in the Introduction, the objective of this paper was to assess how digital democratic affordances influence participation in the internal consultations of the CPP. The first factor

that can significantly impact participation stability is exclusive membership. A selective membership process may result in a base of members who are genuinely interested in active participation and engagement in party life. In contrast to the more accessible registration processes seen in Podemos and the Five Star Movement—where members eventually lost interest in participation (Biancalana, Vittori 2021)—exclusive membership may foster stronger connections between members and the party's processes (Gauja, 2013). However, this form of membership also limits the expansion of the party's membership base, which is why the CPP has a relatively small membership compared to other digital parties (Deseriis, Vittori, 2019; Gerbaudo, 2019; Vittori, 2020).

Another affordance is the party leadership's responsiveness to members' demands, such as modifying the voting platform to ensure genuinely secret ballots, making it impossible to determine how individuals voted. Mosca (2020) identifies the absence of a party leadership response as one of the factors contributing to decreased turnout.

In contrast to Podemos and the Five Star Movement, the CPP allows its members to submit their own consultation proposals with a relatively low quorum of 5.8%. This threshold is lower than that of Podemos (10%), although Podemos had 500,000 members at its peak (Vittori, 2020). If Podemos had the same number of members as the CPP, the number of member consultations would likely be significantly higher. Thus, while this procedure is inclusive, its effectiveness is conditioned by the exclusive nature of membership and the small number of members.

An important affordance is the ability to submit alternative positions for voting. This process helps to prevent potential plebiscitary outcomes in the voting process. Additionally, members have the opportunity to contest the wording of questions if they find them misleading, which further supports trust in the voting process. This trust is also related to the duration of the voting period, which typically lasts three days and occurs over weekends, providing members with ample time to participate. Members are also notified via email and SMS about ongoing votes, which may further contribute to higher participation rates. These features significantly differentiate the CPP from the Podemos and Five Star Movement, where absence of these tools was one of the factors of unstable participation (Deseriis, Vittori 2019; Gerbaudo 2019; Vittori 2020).

Although the participatory procedures of the CPP are relatively inclusive (excluding the aspect of exclusive membership) and offer members considerable influence over the participatory processes, overall turnout remains relatively low at 29.77%, and the CPP has struggled to increase this figure over time. This outcome suggests that an inclusive framework does not necessarily lead to a high degree of participation scale. On the other hand, the turnout rate and level of discussion have remained stable over time, confirming our expectation that inclusive software design and norms of use would lead to participatory stability.

Conclusion

This article examines the participation platforms of the Czech Pirate Party, specifically the party forum and Helios, through the lens of the digital democratic affordance framework proposed by Marco Deseriis (2023b). The framework was expanded by incorporating the quality and scale of participation through the analysis of turnout and discussion over time. The aim of the study is to explore whether the inclusive setup of software design and usage norms positively affects the stability of participation, including voter turnout and the level of discussion.

To summarize our findings, we identify 7 indicators that influence the scale and quality of participation in the networked party (CPP). These indicators include the exclusive membership process, which aims to ensure a committed member base, potentially enhancing reliability but limiting overall participation due to the party's size. The low quorum for consultation proposals (5.8%) facilitates initiating discussions, though inclusiveness is still constrained by the small membership. The voting platform's design, which guarantees secret ballots and provides notifications via email and SMS, enhances trust and encourages turnout. In terms of quality, the ability to submit alternative proposals and contest question wording supports diverse discussions and transparency. Additionally, the voting duration and timing—lasting three days over weekends—allows ample time for deliberation, fostering stable and meaningful participation.

Exclusive membership might be one of the most relevant explanatory factor for the stability of turnout and discussion within the CPP, which indeed remains stable. However, the inclusiveness of participation procedures, voter turnout averages just under 30% of the membership, a figure comparable to the average turnouts in Podemos and the Five Star Movement (Deseriis, Vittori 2019; Gerbaudo 2019; Vittori 2020). This outcome raises further questions about whether an inclusive setup necessarily leads to higher participation levels, even with exclusive membership. In the case of the CPP, it does not.

The results of this article are limited by the fact that it is a single case study, with specific characteristics such as a relatively small membership base compared to other digital parties. In contrast to previous studies on parties like Podemos and the Five Star Movement, the case of the CPP provides insights showing that intra-party participation does not necessarily decline over time and can remain stable (albeit relatively low) if the software design and norms of use are set inclusively, focusing on bottom-up agenda setting and creating a deliberative space that allows members to influence the nature of participation (Deseriis, Vittori 2019; Gerbaudo 2019; Vittori 2020). The case of the CPP expands the literature on networked parties and challenges the predominantly cyber-pessimistic conclusions about digital parties by providing a positive example of the use of digital platforms. Future research should focus on the factors influencing turnout rates and whether members are more inclined to participate in regional or local voting, which may be more relevant to them than national-level issues.

References

- ADIDA, Ben; DE MARNEFFE, Olivier, PEREIRA, Olivier; QUISQUATER, Jean-Jacques (2009). Electing a University President using Open-Audit Voting: Analysis of real-world use of Helios [accessed 2024-04-15]. *Proceedings of the 2009 Conference on Electronic Voting Technology/Workshop on Trustworthy Elections*. Available from WWW: <https://www.usenix.org/legacy/event/evtwote09/tech/full_papers/adida-helios.pdf>
- BARBERÀ, Oscar; SANDRI, Giulia; CORREA, Patricia; RODRÍGUEZ-TERUEL, Juan (2021). Digital Parties: The Challenges of Online Organisation and Participation. *Springer Nature*. <https://doi.org/10.1007/978-3-030-78668-7>.
- BENNETT, W. Lance; SEGERBERG, Alexandra; KNÜPFER, Curd B. (2018). The democratic interface: technology, political organization, and diverging patterns of electoral representation. *Information, Communication & Society*. Vol. 21, no. 11, pp. 1655-1680. <https://doi.org/10.1080/1369118x.2017.1348533>.
- BIANCALANA, Cecilia; VITTORI, Davide (2021). Cyber-Parties' Membership Between Empowerment and Pseudo-participation: The Cases of Podemos and the Five Star Movement. *Digital Parties, The Challenges of Online Organisation and Participation*. pp. 1-304. Springer Nature. https://doi.org/10.1007/978-3-030-78668-7_6.
- BIEZEN, Ingrid van; POGUNTKE, Thomas (2014). The decline of membership-based politics. *Party Politics*. Vol. 20, no. 2, pp. 205-216. <https://doi.org/10.1177/1354068813519969>.
- BLASIO, Emiliana De; VIVIANI, Lorenzo (2020). Platform Party between Digital Activism and Hyper-Leadership: The Reshaping of the Public Sphere: The Reshaping of the Public Sphere. *Media And Communication*. Vol. 8, no. 4, pp. 16-27. <https://doi.org/10.17645/mac.v8i4.3230>.
- BOLLEYER, Nicole; LITTLE, Conor; VON NOSTITZ, Felix-Christopher (2015). Implementing Democratic Equality in Political Parties: Organisational Consequences in the Swedish and the German Pirate Parties. *Scandinavian Political Studies*. Vol. 38, no. 2, pp. 158-178. <https://doi.org/10.1111/1467-9477.12044>.
- CAMMAERTS, Bart (2015). Pirates on the Liquid Shores of Liberal Democracy: Movement Frames of European Pirate Parties. *Javnost - The Public*. Vol. 22, no. 1, pp. 19-36. <https://doi.org/10.1080/13183222.2015.1017264>.
- CASTELLS, Manuel (2001). *The Internet galaxy: reflections on the Internet, business, and society*. Oxford University Press.
- CORTIER, Véronique; GALINDO, David; GLONDU, Stéphane; IZABACHÈNE, Malika (2014). Election Verifiability for Helios under Weaker Trust Assumptions. *Computer Security - ESORICS 2014*. https://doi.org/10.1007/978-3-319-11212-1_19.
- COUNCIL OF EUROPE (2017). Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting: (Adopted by the Committee of Ministers on 14 June 2017 at the 1289th meeting of the Ministers' Deputies) [accessed 2024-04-

- 15]. Available from WWW <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f>.
- DAHLBERG, Lincoln (2011). Re-constructing digital democracy: An outline of four 'positions': An outline of four 'positions'. *New Media & Society*. Vol. 13, no. 6, pp. 855-872. <https://doi.org/10.1177/1461444810389569>.
- DALTON, Russell J; WATTENBERG, Martin P (2002). Parties without partisans: political change in advanced industrial democracies. Oxford University Press, Druk.
- DE BLASIO, Emiliana; SORICE, Michele (2020). Spaces of Struggle: Socialism and Neoliberalism With a Human Face Among Digital Parties and Online Movements in Europe. Triplec: Communication, Capitalism & Critique. *Open Access Journal For A Global Sustainable Information Society*. Vol. 18, no. 1, pp. 84-100. <https://doi.org/10.31269/triplec.v18i1.1132>.
- DE NADAL, Lluís (2021). Populism and plebiscitarianism 2.0: How Podemos used digital platforms for organization and decision-making. *New Media & Society*. Vol. 25, no. 11. <https://doi.org/10.1177/14614448211038763>.
- DESERIIS, Marco (2023a). Reducing the Burden of Decision in Digital Democracy Applications: A Comparative Analysis of Six Decision-making Software. *Science, Technology, & Human Values*. Vol. 48, no. 2. <https://doi.org/10.1177/01622439211054081>.
- DESERIIS, Marco (2020a). Two Variants of the Digital Party: The Platform Party and the Networked Party. *Partecipazione E Conflitto*. Vol. 13, no. 1, pp. 896-917. <https://doi.org/10.1285/i20356609v13i1p896>.
- DESERIIS, Marco (2023b). Rethinking the digital democratic affordance and its impact on political representation: Toward a new framework. *New Media & Society*. Vol. 23, no. 8, pp. 2452-2473. <https://doi.org/10.1177/1461444820929678>.
- DESERIIS, Marco (2022). Is Liquid Democracy Compatible with Representative Democracy? Insights from the Experience of the Pirate Party Germany. *Partecipazione E Conflitto*. Vol. 15, no. 2, pp. 466-481. <https://doi.org/10.1285/i20356609v15i2p466>.
- DESERIIS, Marco (2020b). Digital movement parties: a comparative analysis of the technopolitical cultures and the participation platforms of the Movimento 5 Stelle and the Piratenpartei. *Information, Communication & Society*. Vol. 23, no. 12, pp. 1770-1786. <https://doi.org/10.1080/1369118x.2019.1631375>.
- DESERIIS, Marco; VITTORI, Davide (2019). The impact of online participation platforms on the internal democracy of two Southern European parties: Podemos and the five star movement. *International Journal Of Communication*. Vol. 13, no. 1. <https://doi.org/5696-5714>.
- GAUJA, Anika (2013). The Politics of Party Policy: From Members to Legislators. *Understanding Governance*. Springer.
- GERBAUDO, Paolo (2019). The digital party: political organisation and online democracy. London Pluto Press.

- GERBAUDO, Paolo (2021). Are digital parties more democratic than traditional parties? Evaluating Podemos and Movimento 5 Stelle's online decision-making platforms. *Party Politics*. Vol. 27, no. 4. <https://doi.org/10.1177/1354068819884878>.
- HARTLEB, Florian (2013). Anti-elitist cyber parties?. *Journal Of Public Affairs*. Vol. 13, no. 4, pp. 355-369. <https://doi.org/10.1002/pa.1480>.
- HELIOS (2009). Helios v3 Verification Specs [accessed 2024-04-15]. Available from WWW: <<https://documentation.heliosvoting.org/verification-specs/helios-v3-verification-specs>>.
- CHATTERJEE, Ayan; PRINZ, Andreas (2022). Applying Spring Security Framework with KeyCloak-Based OAuth2 to Protect Microservice Architecture APIs: A Case Study. *Sensors*. Vol. 22, no. 5. <https://doi.org/10.3390/s22051703>.
- JÄÄSAARI, Johanna; HILDEN, Jockum (2015). From File Sharing to Free Culture: The Evolving Agenda of European Pirate Parties. *International Journal Of Communication*. Vol. 9, 870-899.
- JÄÄSAARI, Johanna; ŠÁROVEC, Daniel (2021). Pirate Parties: The Original Digital Party Family. *Digital Parties: The Challenges of Online Organisation and Participation* (p. 304). Springer Nature.
- KLIMOWICZ, Katarzyna Anna (2018). Network parties – A new model to democratise and digitise party politics?. *Das Progressive Zentrum*. pp. 1-17.
- KOSTELKA, Filip; BLAIS, André (2021). The Generational and Institutional Sources of the Global Decline in Voter Turnout. *World Politics*. Vol. 73, no. 4, pp. 1-39. <https://doi.org/10.1017/s0043887121000149>.
- KUSTERS, Ralf; TRUDERUNG, Tomasz; VOGT, Andreas (2012). Clash Attacks on the Verifiability of E-Voting Systems. *2012 IEEE Symposium on Security and Privacy*. pp. 395-409. <https://doi.org/10.1109/SP.2012.32>.
- LIOY, Alberto; DEL VALLE, Marc Esteve; GOTTLIEB, Julian (2019). Platform politics: Party organisation in the digital age. *Information Polity*. Vol. 24, no. 1, pp. 41-58. <https://doi.org/10.3233/ip-180093>.
- MALÝ, Michal (2024). Who Holds the Power in Digital Parties? The Case of the Czech Pirate Party. *Studia Politica - Romanian Political Science Review*. Vol. 24, no. 1, pp. 11-38. <https://doi.org/10.62229/sprps24-1/1>.
- MALÝ, Michal; MARTÍNEK, Tomáš (2024). Participation in the Czech Pirate Party - voting turnout [Data set]. *Zenodo*. <https://doi.org/10.5281/zenodo.13629499>.
- MARGETTS, Helen (2006). Cyber Parties. *Handbook of Party Politics*. pp. 560. Sage Publications.
- MARTÍNEK, Tomáš; MALÝ, Michal (2024). Evaluation of the I-Voting System for Remote Primary Elections of the Czech Pirate Party. *Acta Informatica Pragensia*. Vol. 13, no. 3, pp. 395-417. <https://doi.org/10.18267/j.aip.249>.
- MAŠKARINEC, Pavel (2020). Crossing the left-right party divide? Understanding the electoral success of the Czech Pirate Party in the 2017 parliamentary elections. *Politics*. Vol. 40, no. 4, pp. 510-526. <https://doi.org/10.1177/0263395720920768>.

- MOSCA, Lorenzo (2020). Democratic vision and online participatory spaces in the Italian Movimento 5 Stelle. *Acta Politica*. <https://doi.org/10.1057/s41269-018-0096-y>.
- NAXERA, Vladimír (2023). 'Let us blow them down!': Corruption as the subject of (non-)populist communication of the Czech Pirate Party. *Politics*. Vol. 43, no. 4. <https://doi.org/10.1177/02633957211010984>.
- NORRIS, Pippa (2001). Digital Parties: Civic Engagement & Online Democracy: Civic Engagement & Online Democracy.
- OTJES, Simon (2019). All on the same boat? Voting for pirate parties in comparative perspective. *Politics*. Vol. 40, no. 1, pp. 38-53. <https://doi.org/10.1177/0263395719833274>.
- PATEL, Nishitkumar; WIMMER, Hayden; POWELL, Loreen Marie (2020). PHPBB3 Bulletin Board Security Testing. *Issues In Information Systems*. https://doi.org/10.48009/2_iis_2020_289-299.
- SCARROW, Susan E (2015). Beyond party members: changing approaches to partisan mobilization: changing approaches to partisan mobilization. Oxford University Press.
- VITTORI, Davide (2020). Membership and members' participation in new digital parties: Bring back the people?. *Comparative European Politics*. Vol. 18, no. 2. <https://doi.org/10.1057/s41295-019-00201-5>.
- VODOVÁ, Petra; VODA, Petr (2020). The effects of deliberation in Czech Pirate Party: the case of coalition formation in Brno. *European Political Science*. Vol. 19, no. 2, pp. 181-189. <https://doi.org/10.1057/s41304-019-00233-1>.

Appendix

List of examined documents of the Czech Pirate Party

- PIRATES (2020a). Fórum [accessed 2024-08-30]. Available from WWW: <<https://wiki.pirati.cz/to/technicke-systemy/forum>>.
- PIRATES (2020b). Helios [accessed 2024-08-30]. Available from WWW: <<https://wiki.pirati.cz/to/technicke-systemy/helios>>.
- PIRATES (2020c). Nastavení internetového fóra [accessed 2024-04-15]. Available from WWW: <<https://wiki.pirati.cz/ao/opravneni>>.
- PIRATES (2022a). Přehled technických systémů [accessed 2024-08-30]. Available from WWW: <<https://wiki.pirati.cz/to/technicke-systemy>>.
- PIRATES (2022b). Keycloak [accessed 2024-08-30]. Available from WWW: <<https://wiki.pirati.cz/to/technicke-systemy/keycloak>>.
- PIRATES (2023a). Pravidla internetové komunikace [accessed 2024-04-15]. Available from WWW: <<https://wiki.pirati.cz/ao/pravidla/forum>>.
- PIRATES (2023b). Jednací řád celostátního fóra [accessed 2024-04-15]. Available from WWW: <<https://wiki.pirati.cz/rules/jdr>>.
- PIRATES (2023c). Hlasovací systém Helios [accessed 2024-08-15]. Available from WWW: <<https://wiki.pirati.cz/ao/navody/helios>>.

PIRATES (2024a). Stanovy České pirátské strany [accessed 2024-08-30]. Available from WWW: <<https://wiki.pirati.cz/rules/st>>.

PIRATES (2024b). Registrace příznivců [accessed 2024-08-30]. Available from WWW: <<https://wiki.pirati.cz/ao/navody/priznivec>>.

PIRATES (2024c). Zulip [accessed 2024-08-30]. Available from WWW: <<https://wiki.pirati.cz/to/technicke-systemy/zulip>>.

PIRATES (2024d). Vyhláška k jednání celostátního fóra [accessed 2024-04-15]. Available from WWW: <<https://wiki.pirati.cz/ao/pravidla/cf>>.

PIRATES (2024e). Náповěda k internetovému fóru [accessed 2024-08-15]. Available from WWW: <<https://wiki.pirati.cz/ao/navody/forum>>.

Respondent 1 - Head of the administrative department, party member. The unstructured interview was conducted several times between February and August 2024 via Messenger communication.

Příloha K: Preprint Hodnocení demokracie na českých vysokých školách používajících systém internetového hlasování pro volby do akademického senátu

MARTÍNEK, Tomáš, Michal MALÝ a Jakub KONOPÁSEK

PREPRINT

/připravovaný článek v rámci výzkumu autora práce/

Evaluation of democracy at Czech universities using the i-voting system for elections to the academic senate

Tomáš Martínek, Michal Malý, Jakub Konopásek

Abstract: The shift towards increased remote work and digital communication, driven by recent global developments, has led to the widespread adoption of i-voting systems, including in academic institutions. This paper critically evaluates the use of i-voting platforms for elections to academic senates at Czech public universities, focusing on the democratic and technical challenges they present. A total of 18 out of 26 Czech public universities have implemented remote electronic voting for these elections. Yet, the systems often lack the necessary transparency, raising significant concerns regarding their adherence to democratic norms, such as election security, voter privacy, and the integrity of the process. Through interviews with system developers and administrators, along with a survey of potential voters, the study underscores the critical need for transparency. Without it, a comprehensive assessment of the technical standards and the overall legitimacy of the i-voting systems remains unattainable, potentially undermining the credibility of the electoral outcomes.

Keywords: E-voting, E-democracy, Internet voting, System evaluation, Czech Republic

1. Introduction

Universities have been pioneers in digitizing various processes, and this trend has been accelerated by the COVID-19 pandemic, which necessitated greater remote communication via online tools. As part of this digital transformation, universities have integrated remote internet voting (i-voting) for their electoral processes, including the election of academic senate members.

The Magna Charta Universitatum of 1988 already established the fundamental principles of university autonomy, emphasizing that universities should be independent of political and economic power. The Czech Higher Education Act (Czech Republic 2024) further guarantees the democratic rights of university members to elect their representative bodies through direct and secret elections.

The primary goal of this paper is to analyze the use of i-voting systems at Czech public universities in the context of their compliance with democratic norms, such as transparency, security, representation, and participation. The paper applies the evaluation framework proposed by Von Nostitz et al. (2021) to assess how well these systems meet both democratic and technical standards across a sample of Czech universities.

2. Literature review

2.1. Academic freedoms

Already in 1988, in Bologna, during the celebration of the 900th anniversary of the world's oldest university, university rectors signed the basic principles (Magna Charta Universitatum, 2022) on which the role of universities must be based. Among the signatories was the rector of Charles University in Prague, which at that time was still under the rule of a totalitarian communist regime that would not have considered the given charter text compatible with the state ideology (Jařab, 2008). According to the 1988 Magna Charta, in terms of democracy, a university is an autonomous institution where research and teaching are morally and intellectually independent of any political and economic power. Every university must guarantee its students basic freedoms. The Czech Higher Education Act (Czech Republic, 2024) guarantees the academic right of members of the academic community to elect representative academic bodies. The Academic Senate of a public university is its self-governing representative academic body with at least 11 members, of which at least one-third and no more than half are students. The powers of the Academic Senate include, *inter alia*, deciding on the establishment, merger, amalgamation, division or abolition of units of the university, approving internal regulations, the budget, and annual reports, and deliberating on a proposal for the appointment of the Rector or a proposal for his/her removal from office.

2.2. I-voting at world universities

Voting is a fundamental element of democracy, and it is crucial that elections are not only free but also fair. The secrecy of the ballot is essential as it ensures that each voter can cast their vote without fear of coercion or retribution. To maintain the fairness of elections, it is imperative that they operate on the principle of "one person, one vote" and that they are safeguarded against manipulations such as multiple voting or the destruction of valid ballots (Bishop and Hoeffler 2016). This is particularly important in the context of i-voting platforms, where these principles must be rigorously upheld to ensure the legitimacy and credibility of the tool. In the academic environment, it can be used for secret elections to the Academic Senate or College Councils, for secret ballots of councils or committees, voting for Dean's and Rector's awards, anonymous point evaluation of teaching, within student associations, and elsewhere. Although the effects of voting in universities are not as significant as in national political elections, academic senates still have some significant powers. Therefore, even i-voting in universities should meet at least the basic security requirements (Qadah & Taha, 2007) to ensure the integrity and credibility of the entire election system. I-voting systems are voting systems that allow remote casting of votes over the Internet in an uncontrolled environment using a client device. A broader group are e-voting systems, which include other methods of electronic voting. I-voting systems are used in universities primarily to save time and improve convenience for voters and committee members, eliminate errors in filling out the ballot, speed up the counting process, and increase the accessibility of independent voting (Pawar et al., 2020). Accessible i-voting systems also have the advantage of allowing blind and otherwise disabled people to vote independently (Huarte et al., 2008). In Estonia, i-voting has also been calculated to be the cheapest way to cast a vote in a multi-channel voting system (Krimmer et al., 2018), which also has the lowest environmental impact (Willemson & Krips, 2023). The tradition of remote electronic voting at Czech universities is

quite long, with the Academic Senate being elected electronically at the Faculty of Science of Charles University in Prague as early as 2003 (AS PFF UK, 2007).

The implementation of a secret and verifiable Internet-based voting system in a university setting was described in detail by Adida et al. (2009), where the author of the Helios Voting Adida system worked with academics during the election of the Rector of the Belgian Catholic University of Louvain (UCL) in Louvain-la-Neuve in March 2009. The open-source Helios system uses a modified exponential asymmetric encryption of ElGamal (1985) with an additive homomorphic property for vote secrecy, which allows aggregation of votes by multiplying the encrypted votes without having to decrypt them individually. The individual votes are encrypted while still in the voter's device before being sent to the electronic ballot box of the Helios system. Distributed decryption is used to decrypt the overall results, where multiple trustees' keys are needed. Of the 25,000 eligible voters at the University of Leuven, 5,000 registered to vote, with nearly 4,000 voters voting in each of the two rounds.

A security analysis of the use of the Helios Voting system in a university setting was conducted by Junior et al. (2022), who focused on its use in Brazilian universities - mainly the Federal University Agreste de Pernambuco in 2020, as well as other universities including the University of São Paulo, the Federal University of Pelotas, and the Federal University of Technology Paraná.

Other well-documented (Baloglu et al., 2021) open-source i-voting systems used in universities around the world include software developed by academics at the University of Lorraine - Belenios (Cortier et al., 2019), which also complies with the second level security requirements of the French CNIL recommendations (Cortier et al., 2020).

Among the commercial tools, the Invote system from the Spanish company ScytI (Finogina et al., 2024), which is used at the University of Zaragoza, the Autonomous University of Barcelona or the University of Oviedo (ScytI, 2024), is well known and academically evaluated (Marcos del Blanco & Gascó, 2019). Another Spanish i-voting system evaluated (Marcos del Blanco et al., 2020) is Nvotes, which is used at the National University of Distance Education, the second-largest university in Europe by student numbers (nVotes, 2024).

2.3. Academic senates

Academic senates play a key role in university governance, providing a platform for faculty involvement in decision-making processes, especially in academic matters. They are responsible for setting academic policies, approving new courses, and overseeing the quality of education (Jones, Shanahan, & Goyan, 2002). The structure of academic senates varies among institutions but typically reflects a bicameral system where the senate handles academic matters while the board of trustees handles administrative and financial matters. This system aims to balance academic and administrative interests, although there is often tension and confusion in roles (Jones, Shanahan, & Goyan, 2002).

A number of studies highlight several challenges facing academic senates, including role ambiguity, limited influence over budgetary matters, and difficulties in adapting to rapid policy changes (Pennock et al., 2015; Birnbaum, 1989). Bradshaw and Fredette (2008) highlight the

complexity of academic governance and the need for strategic management. Birnbaum (1989) identifies the latent organizational functions of academic senates in his study "The Latent Organizational Functions of the Academic Senate". He argues that senates, while often not functioning as expected, perform important symbolic and stabilizing roles that contribute to their longevity despite their apparent failures in some areas. A study by Pennock et al. (2015) analyzes changes in the structure and role of academic senates in Canadian universities between 2000 and 2012. The results point to the need for improved orientation programs for senators, better oversight of academic quality, and clarification of roles between the senate, the board, and the administration.

Jones, Shanahan, and Goyan (2002) examine the effects of fiscal restraint and market-based research funding on the governance of Canadian universities, focusing in particular on the role and effectiveness of university senates. The research shows that senates face a disconnect between their intended and actual roles in academic decision-making, highlighting the challenges these bodies face in the context of contemporary political pressures.

Kouba's study focuses on the determinants of student participation in academic senate elections at public universities in the Czech Republic. The research applies the rational choice model to academic elections, which is relatively uncommon, and examines how various factors influence students' decisions to participate in elections for bodies that can have a significant impact on the governance of universities (Kouba, 2017). He finds that smaller academic units tend to have higher turnout in elections, which the author interprets as a result of a stronger sense of community and personal interest in election outcomes. Conversely, larger units often show lower participation, which may be due to anonymity and a lower sense of accountability to the academic community. The competitiveness of elections leads to greater participation, and technological innovations such as Internet voting have a positive but less significant effect on participation. This research offers important insights into how students choose to participate in academic elections and what factors institutions can influence to increase student engagement in college governance (Kouba, 2017).

2.4. Digital Democracy Platforms

Online and internet voting (i-voting) represents a significant advance in modern political participation, allowing for greater involvement of party members and voters in decision-making processes.

Deseriis (2021) highlights that digital participation platforms, including those that enable i-voting, reduce the costs of political participation, thereby enabling greater participation of individuals. Deseriis analyses the different strategies by which designers and administrators of decision-making software such as LiquidFeedback, Consul, and others facilitate voting processes for users. These platforms are designed to improve stakeholder participation, give them access to decision-making processes, and enhance political equality (Deseriis, 2021).

Von Nostitz and Sandri (2021) focus on the digitalization of electoral processes within political parties. They identify several key indicators of successful i-voting, including accessibility and user-friendliness, data security and protection, regulation and platform governance, integration, and communication among members. These indicators are essential for ensuring member

confidence in the voting process and preventing manipulation of results (Von Nostitz & Sandri, 2021).

Paolo Gerbaudo (2019) analyses the democratic quality of online participation platforms in the Five Star Movement in Italy and Podemos in Spain. He finds that despite the promises of these digital parties to introduce more member-driven and inclusive democracy, internal democracy in digital parties is highly centralized and plebiscitary in nature. Members have limited influence over decision-making processes and platforms are tools for affirming leadership decisions rather than for genuine deliberation and participation (Gerbaudo, 2019).

In his comparative analysis of the technopolitical cultures and participation platforms of the Pirate Party of Germany and the Five Star Movement, Deseriis (2020) shows how different technopolitical cultures influence the organization of these parties and how the subsequent adoption and use of online participation platforms has led to internal conflicts and disputes within the Pirate Party and increased centralization within the Five Star Movement. This research highlights the importance of cultural context and organizational practices in the implementation of i-voting (Deseriis, 2020).

Overall, online and web-based voting has the potential to transform political participation and decision-making, but its success depends on a number of factors, including software design, regulatory standards, and how they are implemented and used by political actors. Gerbaudo (2021) describes that for digital participatory platforms to be effective, they must be transparent and have clearly defined rules of operation; otherwise, there is a risk of losing legitimacy and voter passivity. Further empirical research is needed to understand the specific impacts of these technologies on political equality and the effectiveness of decision-making processes (Deseriis, 2021; Von Nostitz & Sandri, 2021; Gerbaudo, 2019). Based on these findings, our study will evaluate online voting for academic senate elections using the concepts of Von Nostitz and Sandri (2021).

3. Research methods

Analysis of relevant articles was conducted from the scientific databases Web of Science and Scopus. Based on those, our analysis of the use of remote electronic systems at Czech public universities for academic senate elections is conducted using online interviews with administrators and developers of IS of Czech public universities, publicly available documents, system testing, and available source code.

3.1. Methodology for evaluation of the systems of Czech public universities

The semi-structured interviews ask questions about system development and administration, verifiability, confidentiality and security of the election, voter authentication, resistance to coercion, integrity, voter awareness, and how to deal with possible problematic situations where, for example, a voter could vote for both student and staff senate chambers at the same time. Representatives of all 26 Czech public universities were contacted and structured interviews were conducted with representatives of four Czech public universities that use the four most commonly

used i-voting systems, namely from DERS Group, IS4U, Faculty of Informatics Masaryk University in Brno (FI MUNI) and Computer Center Palacky University Olomouc (CVT UPOL). The paper discusses in detail a sample of i-voting systems used at more than one public university, which includes 4 i-voting systems evaluated through interviews supplemented by the Elections system from Faculty of Arts Charles University in Prague (FA CUNI).

For a comprehensive evaluation of the i-voting systems of Czech universities, the concept proposed by Von Nostitz et al. (2021) is used, which defines an evaluation framework for democratic norms including participation, representation, competitiveness, responsiveness, and transparency. It further defines an evaluation framework for technical standards including security, verification process, data ownership, and control. For the framework, a descriptive analysis of voting systems in Czech public universities is conducted based on research findings.

Representation (Von Nostitz et al., 2021) in the context of academic senate elections refers to the extent to which election outcomes reflect the diverse composition of the university community, including students, faculty, and staff from different faculties and departments. The i-voting system should ensure equal access for all eligible voters, regardless of their socio-economic status, technical resources, or other barriers, to ensure that the election results truly represent the voices of all groups, including minority or marginalized constituencies within the academic environment.

Competitiveness (Von Nostitz et al., 2021) ensures that elections allow fair competition among candidates and that all candidates have equal opportunities to participate. In i-voting systems for academic senates, it is crucial to ensure that candidates from different faculties and academic positions are not given unequal advantages and that the system does not favor certain groups or individuals, promoting a fair electoral process.

Transparency (Von Nostitz et al., 2021) means that the entire electronic voting process, from voting to vote counting, is open to independent audit and verification. In i-voting systems for academic senates, transparency should be ensured through the use of open-source software or independent audits, allowing verification that the election was free from manipulation and that the results accurately reflect the will of the voters.

Responsiveness (Von Nostitz et al., 2021) refers to how quickly and effectively issues and concerns are addressed during the election process. In the context of i-voting for academic senates, this means that universities should have mechanisms in place to swiftly resolve technical issues, protect voter privacy, and transparently handle disputes, thereby fostering trust in the electronic voting system.

In the framework of the participation evaluation, data from the Faculty of Arts at Charles University in Prague is used (Charles University, 2024). This faculty has the highest number of full-time students among the faculties using i-voting in the Czech Republic (Ministry of Education of the Czech Republic, 2024).

No university representative or developer provided access to publicly unavailable parts of the source code of the i-voting application nor did an independent audit, therefore some of the results are declarations of interviewees without any possibility of verification. Given the only partial knowledge of the systems and the trade secrets of the developers, the rating is not definitive but is

chosen based on all information gathered at the time of writing. Based on the given findings, final recommendations are made.

3.2. Questionnaire survey of university students and graduates focused on i-voting systems

In order to find out the opinions on i-voting of Czech students and graduates of universities, including academic staff, an online survey was conducted from 24 October 2023 to 12 May 2024 through the application *Dotaznik.czu.cz*, which uses the LimeSurvey system. Respondents answered questions defined in the Agbesi et al. (2023) framework focusing on Information Availability, Understandability, Monitoring and verifiability, Remedial Measures, Testing, Transparency, and several additional questions. All information, including consent for data processing, was displayed to participants on the survey homepage.

Respondents answered questions on a seven-point Likert scale ranging from Strongly disagree (0) to Strongly agree (6). A total of 177 people were recorded completing the questionnaire. A total of 108 questionnaires were completed in full. Of these, eight additional questionnaires were removed because the control question "This question is not part of the survey and just helps us to detect bots and automated scripts. To confirm that you are a human, please choose 'Strongly agree' here" other than Strongly agree. Of the 100 responses, 64 were male, 35 were female, and one respondent did not indicate gender. 72 respondents were aged 18-30, 18 were aged 31-40, five were aged 41-50, two were aged 51-60, and three were aged 61-70. 72 respondents have a high school degree, ten have a bachelor's degree, 12 have a master's degree, and six have a PhD.

The Statistica 14 software was used to produce the exact results of the descriptive statistics. Descriptive statistics were calculated separately for each variable, providing fundamental information such as the mean, minimum and maximum values, various measures of variation, and data regarding the shape of the variable's distribution (including the standard deviation and the standard error). An important aspect of the description of a variable was the shape of its distribution, which indicates the frequency of values within different ranges of the variables. More precise information was obtained by performing normality tests to determine the probability that the sample originated from a normally distributed population of observations, specifically using the Shapiro-Wilk test. These statistics were included in the dataset (Martínek & Tyrychtr, 2024).

For simplicity, we use in this paper the calculated average of the responses divided by the maximum (six), which allows us to present values on a scale from zero to one, where values above 0.5 to one (max) indicate the level of agreement with the question and values below 0.5 to zero (max) indicates the level of disagreement with the question. The value is rounded to three decimal places.

4. Results

Out of 26 Czech public universities, 18 institutions have already used the electronic system for remote voting in the Academic Senate elections in the past. In addition, three more, the Academy of Arts, Architecture and Design in Prague, Jan Evangelista Purkyně University in Ústí nad Labem,

and the Institute of Technology and Business in České Budějovice, already have an electronic voting system in place, but it has not yet been used in the senate elections. Basic data on the address and developer of the systems used at these 18 institutions are described in the following table.

Table 1: Systems for electronic election of the Academic Senate of Czech public universities (source: own elaboration based on interviews)

Public university	E-voting system (URL)	Developer
Academy of Performing Arts in Prague	volby.amu.cz	CVT UPOL
Brno University of Technology	vut.cz	VUT
Czech Technical University in Prague	volby.cvut.cz	ČVUT
Charles University	hlasovani.is.cuni.cz volby.ff.cuni.cz	DERS Group FA CUNI
Janáček Academy of Performing Arts	is.jamu.cz/auth/volby/	FI MUNI
Masaryk University	is.muni.cz	FI MUNI
Mendel University in Brno	is.mendelu.cz/auth/evolby/	IS4U
Palacky University Olomouc	volby.upol.cz	CVT UPOL
Prague University of Economics and Business	insis.vse.cz/auth/evolby/	IS4U
Silesian University in Opava	is.slu.cz/auth/volby/	FI MUNI
Technical University of Liberec	fraxinus.is.tul.cz/volby	TUL
Technical University of Ostrava	uzivatel.sso.vsb.cz/wps/myportal/uzivatel/volby-as/hlasovani/	VŠB
Tomas Bata University in Zlín	volby.utb.cz	DERS Group
University of Chemistry and Technology, Prague	hlasovani.vscht.cz	DERS Group
University of Ostrava	portal.osu.cz/wps/portal/as	OSU
University of Pardubice	evolby.upce.cz	CVT UPOL
University of South Bohemia in České Budějovice	volby.jcu.cz	FA CUNI
University of West Bohemia	volby.zcu.cz	DERS Group

For further evaluation, primarily Internet voting systems that have been choice tested at more than one Czech public university were considered. Specifically, these are the E-voting system from Faculty of Informatics Masaryk University in Brno (FI MUNI), the Elections system from Computer Center Palacky University Olomouc (CVT UPOL), the E-voting module of the UIS system from IS4U, the POLL system from DERS Group and the Elections system from Faculty of Arts Charles University in Prague (FA CUNI).

4.1. Regulations

In the Czech Republic, the election to the academic senates of universities is regulated by the Higher Education Act (Czech Republic, 2024), which defines that the election should be direct and secret. Direct suffrage means that members of the Senate cannot be elected by delegates. The procedure for election to the academic senate is addressed by universities and their faculties in the election rules of the academic senate or other internal regulations of the university. In the context of a remote electronic election in an uncontrolled environment, it is difficult to verify that the election was indeed direct, i.e. that the voter voted in person and did not, for example, hand over access data to another person. This issue is also addressed in the case of correspondence voting, where in both cases, even voting in an uncontrolled environment is generally accepted as direct in many cases. In order to verify that the election is indeed secret, at a minimum an independent security analysis of the system used should be carried out, and ideally the system should be open-source so that the method of secrecy can be transparently verified by the general public.

From the point of view of usability and accessibility, it is useful to distinguish between these two related but distinct concepts. Usability refers to how easily and efficiently the system can be used by all users. A highly usable system ensures that voters, regardless of their technical knowledge, can navigate the voting process smoothly and without confusion. Accessibility, on the other hand, specifically focuses on making the system accessible to people with disabilities, such as the visually impaired or those with physical limitations. An accessible system ensures that everyone, including people with disabilities, can fully participate in the voting process by providing them with necessary accommodations such as screen readers or keyboard navigation.

Also relevant in this context is the Law on Accessibility of Websites and Mobile Applications (Czech Republic, 2019), which obliges universities, as public institutions, to ensure the accessibility of content published on their websites. This Act also applies to content that a higher education institution is obliged to publish under other legislation, e.g. in the exercise of public administration in education, science, research, development, innovation and care for children and youth, or under the Act on Free Access to Information.

When it comes to the handling of personal data of constituents, universities must comply with the General Data Protection Regulation (EU, 2016). The GDPR applies directly in all EU Member States, in the Czech Republic it has been implemented through an amendment to some related laws. This ensures that the provisions of the GDPR are fully integrated into the Czech legal framework. Universities are obliged to handle personal data processed during the electoral process in accordance with these regulations, thus ensuring the protection and privacy of voters' data.

4.2. Democratic norms for i-voting

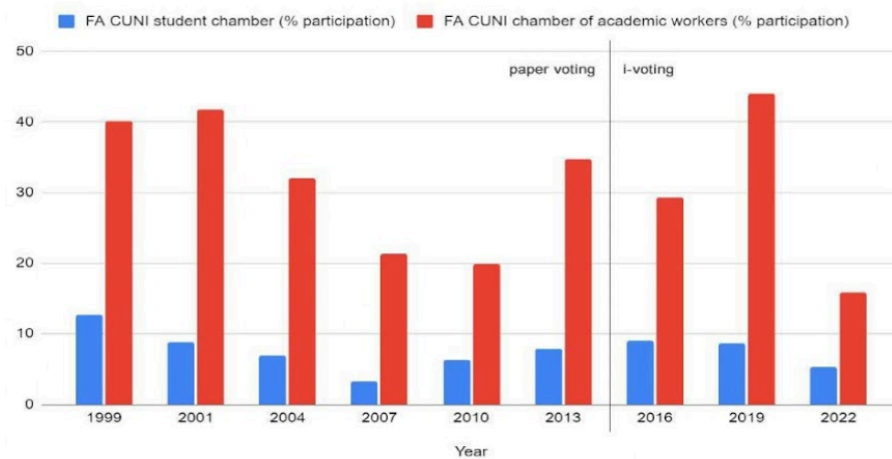
4.2.1. Participation

In the case of the student chamber of the Academic Senate, every person with student status has the right to vote, while every teaching staff member has the right to vote for the pedagogical chamber. As part of eligibility, universities use their own voter registry to verify users, where voter verification has already occurred when students register or begin employment. Each employee has

1 vote, regardless of the amount of working time. Any student or employee who registers as a candidate may be elected. A problematic situation arises when one person is both a student and a faculty member, where each college must determine the procedure so that a given voter can vote only once. Some online voting systems allow the voter to choose which chamber they want to vote for and then block the ability to vote for the other chamber of the Academic Senate. Elsewhere, a person is primarily placed in the academic staff chamber election unless they directly request to be placed in the student chamber. Voters' lists are normally approved by the designated Elections Committee before the election is run.

According to the number of full-time students, the largest faculty in the Czech Republic that has already used remote electronic voting for elections to the Academic Senate is the Faculty of Arts at Charles University in Prague, which has 5,560 full-time students (Ministry of Education of the Czech Republic, 2024). Electronic elections have been used at FA CUNI from 2016 to the present. The following graph (Figure 1) of voter turnout indicates that the implementation of remote electronic voting has not had a significant impact on voter turnout to define a clear trend. Of the years studied, the student chamber had the highest turnout of 12.7% in 1999 during the traditional paper ballot election, while the academic staff chamber had the highest turnout of 44% during the remote electronic election in 2019. Conversely, the lowest turnout during the study period for the student chamber was 3.2% in 2007 for the traditional paper ballot election and 15.8% for the academic staff chamber electronically in 2022 (Charles University, 2024). The higher student turnout at the turn of the millennium may be related to the minimum quota for validity in place at the time, with faculties attempting to increase student participation in various ways to ensure the validity of elections.

Figure 1: Chart of voter turnout at FA CUNI from 1999-2022, remote electronic voting introduced in 2016 (source: own processing according to Charles University (2024))



In the survey, the agreement rate was 0.723 for the question that respondents would use remote electronic voting if this option were available in the event of an election.

4.2.2. Representation

Within the academic senates, the ratio of representatives of the teaching chamber to representatives of the student chamber usually prevails; at Charles University, the ratio of academic staff and students is balanced. In the case of elections to the university academic senate, inequality arises because each faculty usually has a certain number of representatives, which may not sufficiently reflect the size of the faculty. In faculty academic senate elections, each student usually has an equal vote for student representation, and each teacher has an equal vote for student representation. However, some faculty academic senates also have a split number of representatives for each discipline or department under the faculty. The CVT system of UPOL allows combining the election for both chambers, so it is possible to vote for up to 6 academic staff and one student in the pedagogical curia, while in the student curia, the voter can vote for up to two academic staff and three students. The possibility of selecting candidates and the method of determining the order in the CVT UPOL i-voting system is shown in Figure 2.

Figure 2: Candidate selection in the CVT UPOL i-voting system, 1 is the list of candidates with the option to remove, 2 indicates a change in order, 3 indicates proceeding to submit the ballot (UPOL, 2022)

The screenshot displays the 'Oblíbená zvířata' (Favorite animals) section of the CVT UPOL i-voting system. It is divided into two main panels: 'Kandidáti' (Candidates) on the left and 'Moje volba' (My vote) on the right.

Kandidáti (Candidates): A list of six candidates is shown, each with a number and a name, and a right-pointing arrow for selection:

- 1. Barevný Chameleon
- 2. Čistotné Prase
- 3. Chudá Myš
- 4. Drzá Veverka
- 5. Liná Veš
- 6. Lstivá Liška

Moje volba (My vote): This panel shows the selected candidates and their order. It includes a '1' indicating the list of candidates with the option to remove, and a '2' indicating a change in order. The selected candidates are:

- 1. Barevný Chameleon
- 2. Čistotné Prase
- 3. Chudá Myš

Below the list, it states 'Máte vybráno 3 z 11 možných kandidátů' (You have selected 3 out of 11 possible candidates). A yellow button labeled '3 Pokračovat na rekapitulaci' (Continue to recapitulation) is visible at the bottom.

Most institutions allow any nominee who agrees to run to run. Mendel University in Brno also conducts a remote electronic nomination round where each member of the academic community can nominate up to ten candidates for the Academic Staff Chamber or up to five candidates for the Student Chamber. After the nomination round is completed, the results are published and requests for consent to candidacy are sent out to the nominees. Subsequently, lists of candidates are drawn up on the basis of the nomination support, with no more than twice as many candidates who have consented to stand as the number of Academic Senate seats to be filled. Only then is there an election round.

4.2.3. Competitiveness

Candidates are nominated by members of the academic community. Each candidate who agrees to be nominated normally submits basic information about themselves and their election program, which is normally announced on the institution's website. An example of filling in the ballot paper, which contains not only the name of the candidates but also their photo, job position and a link to more detailed information, in the FI MUNI i-voting system is shown in Figure 3.

Figure 3: Candidate selection in the FI MUNI i-voting system, where it is also possible to view the candidates' photos, the option "I abstain from voting" is displayed and the arrow indicates the button to save the vote (SLU, 2020)

Označuje se právě jedna možnost. Volbu potvrďte kliknutím na tlačítko 'Uložit volbu'.

☐ Zvolit	 Mgr. [Name] učo: [ID]
☒ Zvolit	 Mgr. [Name] Koordinátor IS učo: [ID]
☐ Zvolit	Zdržuji se hlasování
☐ Zvolit	Nebudu hlasovat. Tuto volbu nechci nadále nabízet.

Uložit volbu 3 ←

4.2.4. Transparency (and accountability)

The internet voting systems used at Czech universities are not very transparent, the source codes of the voting systems used are not published to the public, and voters usually only have access to basic documentation containing mainly voting instructions.

Responsibility for the election rests with the election committee established by the Academic Senate. Individual faculties of some universities usually have to adapt to the election method determined by the university academic senate, so the university academic senate may also have some responsibility for choosing the election method.

In the questionnaire survey, for the question that the online voting system should be transparent, the level of agreement of respondents is 0.807. Transparency as an integral part of the Internet voting system is reflected in an agreement rate of 0.778. Transparency as an important feature of the internet voting system is expressed by an agreement rate of 0.785.

4.2.5. Responsiveness

Elections at Czech universities are secret, so the elected senator has no clear idea which voters' preferences he or she represents. Candidates may have election programs that are often brief or missing altogether. All voters have the option of directly approaching academic senators to whom they can convey their demands, who then represent them as they see fit. Meetings of the Academic Senate are normally open to the public and records of proceedings are openly published. The activities of each senator are then reflected by voters in the next election.

The election results are generally accepted once the protocol has been certified by the Electoral Commission. As a rule, voters and candidates have the opportunity to lodge a complaint about the conduct of the election. Once the complaints have been settled by the Electoral Commission, the

results are considered valid and the newly elected Senators take over the certificates of election and take office from the beginning of the new term of the Academic Senate.

The introduction of remote electronic voting has also encountered problems at universities in the Czech Republic. After the remote electronic elections to the Academic Senate of Charles University in Prague at the Faculty of Science in 2006, a complaint was filed that the elections were invalid due to their form not complying with the existing regulations, which was upheld by the main election commission by invalidating the elections (AS PrF UK, 2007).

In the survey, respondents report an agreement rate of 0.735 on the question that a responsible party should be identified in case of any problems with the electoral process.

4.3. Technical standards for i-voting

4.3.1. Security

Because the voting systems used in Czech public universities are not transparent, in that they do not publish source code or detailed information about their operation, it is difficult to verify their security and integrity. Based on the interviews conducted, only basic information about the functioning of the systems is available for research, which cannot be independently verified. The systems in use eliminate the possibility of inadvertently filling in a ballot paper by mistake; some leave the option of submitting a blank ballot paper. All systems examined use Hypertext Transfer Protocol Secure (HTTPS) for secure connections.

The Prague University of Economics and Business states that it has had an independent security audit of the system carried out according to the methodology of the National Office for Cyber and Information Security (NÚKIB, 2023). The audit, conducted by a company certified to ISO security standards, also included vulnerability tests from both internal and external networks. The audit did not reveal vulnerabilities, but it is not publicly available.

The CVT UPOL's Voting system uses asymmetric encryption for sending the vote, where the vote is encrypted already in the voter's device, the votes cannot be manipulated externally - the database antitampering is at the level of symmetric encryption and checksums over the database, so it is possible to detect possible violations of election integrity in the database or in the application. The application symmetrically encrypts the votes on the database and continuously generates checksum. Check is done when the election is evaluated or can be done as needed. Organizationally, this is ensured by the fact that the database and web server administrator does not know the symmetric key that is stored in the application; the developer, on the other hand, does not have access to the web server and database.

Figure 4: Example of DERS Group's POLL electronic ballot with the Abstain option, the arrow indicates the recap button where the choice must be confirmed before submitting (ZČU, 2023)

In the event of an outage, systems including POLL (DERS Group, 2021) allow for extended voting at the discretion of the Election Commission. All operations including importing lists, modifying lists, and exporting results are logged within the POLL system for possible review. An example of an abstention vote and requiring confirmation in the POLL i-voting system is shown in Figure 4.

An agreement rate of 0.85 respondents presents the requirement for there to be an assurance that any security breach will be detected and repaired. The requirement for thorough testing for security vulnerabilities by independent security experts is represented by a high agreement rate of 0.89.

4.3.2. Verification process and secrecy

Single sign-on credentials are used to log in to the electoral system and are also used by academic staff and students to access other College systems. The system from DERS Group uses Eduid.cz operated by CESNET, where all Czech public universities are full members of the association. The IS4U system allows setting up multi-factor authentication. For example, Prague University of Economics and Business requires two-factor authentication from 2023. Specifically, after entering the correct login name and password, the user is prompted to enter an authentication code from the mobile app. If the user designates the device as secure, the user is not required to provide a login code for 30 days.

In order to increase coercion resistance, the FI MUNI system offers the possibility of repeated voting, where only the last vote cast is counted. However, most of the systems used at Czech universities do not allow repeated voting, so the only way to reduce the risk of pressure from colleagues and others is to cast your vote early.

Figure 5: The page after selecting the options in the IS4U system, where the voter is informed that the ballot has been encrypted in the voter's browser, the ballot's digital signature string is displayed to check the vote count, and the button to cast the encrypted vote is displayed (VSE, 2021)

Portál voliče – Volební lístek

[Aktuální volby](#) [Proběhlé volby](#)

Název voleb: test 1
Druh voleb: Výběr z možností
Stav voleb: Probíhá hlasování
Začátek voleb: 26.02.2021 09:40
Konec voleb: nenastaveno
Způsob voleb: tajný

Svůj návrh potvrďte stisknutím tlačítka **Zašifrovat volební lístek**.

Předmět hlasování: Usnesení, o kterém se hlasuje.

 **Poté, co odhlasujete, nebude možné hlas změnit ani zobrazit.**

Všechny vaše odpovědi byly před chvílí zašifrovány ve vašem prohlížeči a jsou připraveny k odeslání na server. Budete-li si chtít později ověřit, že váš volební lístek je k dispozici pro sčítání hlasů, zkopírujte si prosím následující řetězec **Quwh8YmkumdkPRAfVbAZf5Ugaoat4FbG1Mg7s5iUpGY=**. Tento řetězec je digitálním podpisem vašeho volebního lístku.

[Odevzdat hlasovací lístek](#)

Figure 6: Post-submission page showing the vote control code in the UPOL CVT system (UPOL, 2022)

Vaše volba byla úspěšná. Děkujeme

Váš hlas vypadá takto:

RLZY -

Zda se váš hlas nachází v seznamu hlasů si můžete ověřit zde: [LINK](#)

The systems from FI MUNI, CVT UPOL (Figure 6), or IS4U (Figure 5; Figure 7) allow to individually verify the counting of the sent vote. Universal verifiability for independent verification of election results including their integrity and ensuring high credibility of elections is not offered by standard systems at Czech public universities.

Figure 7: IS4U ballot box page with a list of digital signatures of individual votes with the option to switch to the voters list (VSE, 2021)

Ověření hlasování

[Seznam voličů](#) [Seznam hlasů](#)

Vybrané volby: **Volby cvičné**
Stav voleb: **Volby uzavřeny**

V tabulce je seznam všech hlasů. Pokud jste hlasovali, můžete svůj hlas dohledat. Hlas byl zobrazen při hlasování.

Poř.	Hlas
1.	Vs4gY3Bsqds2S1hX6IXAu3QH0JaUXz5yU92M99ToLU5=

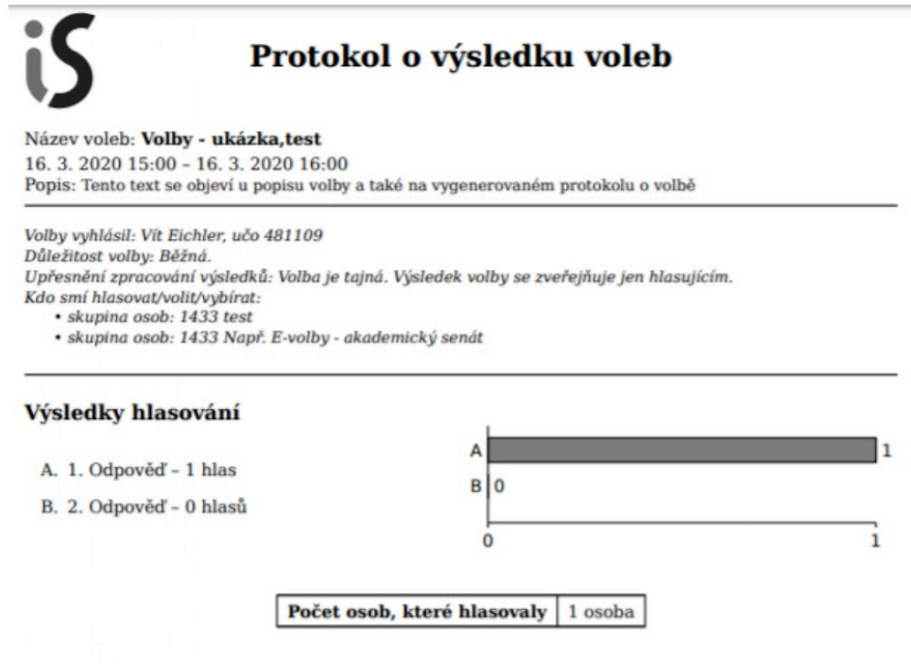
Due to the lack of transparency, we were unable to determine the method of vote secrecy for most of the systems used to ensure voter privacy. For example, the POLL system is based on documents mandatorily published in the Register of Contracts (DERS Group, 2021), where, according to the technical requirements of the contract, confidentiality is addressed after submission by storing the anonymized vote and indicating that the voter has already voted. The voter subsequently receives information that the vote was saved.

Within the survey, a high agreement rate of 0.885 is recorded for the question asking for the ability to verify that the online voting system recorded the voter's vote as intended. The requirement for public availability of external audits after the election is represented by an agreement rate of 0.79.

4.3.3. Data Ownership and Control

Some Czech higher education institutions such as FA CUNI or FI MUNI develop voting systems for their school and possibly other universities on their own. In this case, they have full control over the data and the whole system. On the other hand, universities that use the services of IS4U or DERS Group rely on a commercial system operator by way of a contractual relationship. In most cases, the systems run on servers located in the Czech Republic. In terms of election administration, it is not common for the administration to be distributed - in many cases, one person sets up the elections in the system. FI MUNI's I-voting system allows the generation of a final report for each election, as shown in Figure 8.

Figure 8: Election result log generated by the FI MUNI E-voting system, the log includes the name, description, and date of the election, as well as the name of the election administrator, importance, results, and other information (MUNI, 2024)



4.4. Overall assessment of compliance with democratic principles in the use of i-voting systems at Czech public universities

From the available information, it cannot be clearly assessed whether the i-voting systems used in Czech public universities meet basic democratic requirements. Universities and developers do not publish the source codes of the applications used, offer only weak documentation, and are often unwilling to disclose the information needed to verify how the i-voting systems work. This information is not only unavailable to the general public, but also to the eligible voters themselves, who must therefore blindly trust i-voting systems. The interviews show that often even the responsible representatives of the universities do not know more detailed information about the functioning of the i-voting systems, and thus again put their full trust in the developers and operators. The current legislative regulation does not force universities or developers to publish substantial information about the functioning of i-voting systems, even though the specifics of the electoral process require such public information in a democratic society.

Based on a basic descriptive evaluation and the assumptions required by potential voters, a system should be used that ensures security, privacy, verifiability, voting integrity, and transparency. Since no i-voting system used in Czech universities is fully transparent, a publicly

accessible independent audit of the system would have to be made to guarantee these properties. Systems with individual verifiability from FI MUNI, CVT UPOL or IS4U are close to meeting the expected requirements.

5. Discussion

In contrast to the transparent approach of Adida et al. (2009), it is difficult to access information in Czech public universities. The documentation is very limited, the persons in charge only answer basic questions in general or not at all, and it is often not clear whether the way i-voting systems work is at least known by the persons in charge at the universities. Without adherence to democratic norms involving transparency, the i-voting systems used in Czech universities cannot be sufficiently evaluated in terms of compliance with technical standards involving privacy, security or election integrity. On the other hand, a detailed evaluation can be carried out for the system of the Czech Pirate Party, which publishes all source code and other necessary information about its i-voting system (Martínek & Malý, 2024). I-voting systems differ to a large extent from other information systems, where a possible error or manipulation can be discovered and corrected. Prioritizing electoral efficiency over electoral transparency in the case of a "black box" i-voting system is not desirable (Cheeseman et al., 2018), as suggested by potential users of i-voting systems themselves in our survey. Interviewees often justified their reluctance to provide sufficient information by citing system security. In some cases, they themselves did not have information on how the system in question ensures its functionality. The lack of transparency needed to evaluate the system has a negative impact on the credibility of the electoral process.

The security analyses of the Helios system (Bernhard et al., 2012; Cortier & Smyth, 2013; Acemyan et al., 2015; Panizo Alonso et al., 2018) used at the University of Leuven allow correcting the errors found and building confidence in the integrity of the election among its users. There are no publicly available security analyses regarding the software used in Czech public universities. It is worth adding that similarly low transparency exists in other universities around the world. For example, Harvard University offers more detailed information regarding remote electronic voting (Harvard University, 2024), including a link to the operator of the voting system (ESC, 2024), which offers a basic FAQ and other materials, but the source code of the system or independent audits are not publicly available.

Despite the lack of transparency of i-voting systems at Czech public universities, the practice of remote voting via the Internet for the Academic Senate is widespread, with 18 out of 26 Czech public universities using i-voting systems. These platforms can serve the purpose of reducing costs and administrative burdens. However, it is quite concerning given that these platforms are being used to elect individuals to significant positions, which manage large financial budgets and oversee faculties or universities. At the same time, even potential voters themselves in the questionnaire survey express a high level of agreement with the requirements for transparency, verifiability, clarity or security.

Similar to studies in national elections (Germann & Serdtült, 2017; Goodman & Stokes, 2020), it is difficult to determine whether the introduction of i-voting at universities affects voter turnout; we do not find a clear trend in the university turnout we observe.

In order to enable the general public to scrutinize their i-voting systems and to ensure the credibility of democratic elections, the possibility of developing a recommendation, following the example of the French CNIL (La Commission nationale de l'informatique et des libertés, 2019), which would require public institutions, including public schools, to comply with the basic requirements for a secret online voting system where the outcome of the vote has a significant impact, such as in the case of the election of members of the Academic Senate. A national recommendation with binding requirements for public administrations could be based on Recommendation CM/Rec(2017)5 of the Committee of Ministers of Member States on standards for electronic voting (Council of Europe, 2017), which is a valid recommendation for Council of Europe member states.

Inspiration can also be found in the transparently managed introduction and control of i-voting systems in the context of politically binding elections. In the implementation of a remote e-voting project in Norway, a transparent tender was conducted (Ministry of Local Government and Regional Development, 2010), where an additional open source requirement allowed for a technical analysis of the system (Bjørstad, 2013), which discovered vulnerabilities for remediation. Similarly, in Estonia, most of the source code of the system in use is made public (Valimised, 2024). Transparency allowed security analyses to be conducted (Springall et al., 2014; Heiberg et al., 2015; Pereira, 2023), based on which modifications could be made to the system to improve its security. Thus, in Estonia, the system is regularly updated to ensure greater security and integrity of the elections, which is intended to increase the credibility of the entire remote e-voting system. A specific description of the possibility of implementing a transparent open-source i-voting solution including its verification is described in Martínek et al. (2024).

The recommendation for academic senates and university administrations is that they require open-source systems, or at least have the possibility of an independent audit of the system, including access to the source code by experts who can sign a non-disclosure agreement (NDA). In the event that student and academic staff constituents do not have sufficient assurance that the i-voting system is functioning properly, they should demand that elected representatives to the Academic Senate provide information or an audit. A recommendation for the state may be to require public institutions within i-voting systems to comply with Recommendation CM/Rec(2017)5 of the Committee of Ministers of Member States on standards for electronic voting (Council of Europe, 2017). Nevertheless, it should be borne in mind that even Recommendation CM/Rec(2017)5 of the Council of Europe is not the final perfect list of requirements and needs updating (Rodríguez-Pérez, 2022).

6. Conclusion

This paper has provided a comprehensive analysis of the implementation of i-voting systems at Czech public universities, applying the evaluation framework proposed by Von Nostitz et al. (2021). The findings highlight several key areas for improvement, particularly in terms of transparency and security. While the adoption of i-voting systems has undoubtedly improved convenience and accessibility for voters, these systems often lack sufficient transparency, which is crucial for maintaining voter confidence in the integrity of the electoral process.

The analysis also underscores the need for universities to ensure that their i-voting systems meet both democratic and technical standards, particularly as these systems are used to elect representatives to significant positions within university governance. Recommendations for enhancing the transparency of these systems include the adoption of open-source platforms or, at a minimum, allowing independent audits of the systems used.

Overall, while i-voting systems have the potential to streamline the electoral process, the findings indicate that without improved transparency and security measures, these systems may undermine the democratic legitimacy of elections at Czech universities. Future research should focus on conducting more in-depth evaluations of these systems and exploring ways to further improve their adherence to democratic principles.

References

- Acemyan, C. Z., Kortum, P., Byrne, M. D., & Wallach, D. S. (2015). From Error to Error: Why Voters Could not Cast a Ballot and Verify Their Vote With Helios, Prêt à Voter, and Scantegrity II. In *USENIX Journal of Election Technology and Systems (JETS)* 3 (pp. 1-25). <https://www.usenix.org/jets/issues/0302/acemyan>
- Adida, B., de Marneffe, O., Pereira, O., & Quisquater, J. -J. (2009). Electing a University President using Open-Audit Voting: Analysis of real-world use of Helios. In *Proceedings of the 2009 Conference on Electronic Voting Technology/Workshop on Trustworthy Elections. EVT/WOTE*. https://www.usenix.org/legacy/event/evtwote09/tech/full_papers/adida-helios.pdf
- Agbesi, S., Budurushi, J., Dalela, A., & Kulyk, O. (2023). Investigating Transparency Dimensions for Internet Voting. *Electronic Voting*, 1-17. https://doi.org/10.1007/978-3-031-43756-4_1
- AS PrF UK. (2007). *Zápis z mimořádného zasedání Akademického senátu PrF UK dne 29. 01. 2007*. Přírodovědecká fakulta UK. Retrieved April 25, 2024, from <https://www.natur.cuni.cz/fakulta/senat/zasedani/zapisy/2007/zapis-z-mimoradneho-zasedani-akademickeho-senatu-prf-uk-dne-29-01-2007>
- Baloglu, S., Bursuc, S., Mauw, S., & Pang, J. (2021). Election Verifiability Revisited: Automated Security Proofs and Attacks on Helios and Belenios. *2021 IEEE 34th Computer Security Foundations Symposium (CSF)*, 1-15. <https://doi.org/10.1109/CSF51468.2021.00019>
- Bernhard, D., Pereira, O., & Warinschi, B. (2012). How Not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios. In *Advances in Cryptology – ASIACRYPT 2012* (pp. 626-643). Springer. https://doi.org/10.1007/978-3-642-34961-4_38
- Birnbaum, R. (1989). The Latent Organizational Functions of the Academic Senate. *Journal of Higher Education*, 60(4), 423-443. <https://doi.org/10.1080/00221546.1989.11775050>
- Bishop, S., & Hoeffler, A. (2016). Free and fair elections. *Journal of Peace Research*, 53(4), 608-616. <https://doi.org/10.1177/0022343316642508>
- Bjørstad, T. E. (2013). Source code audit of Norwegian electronic voting system. *Ministry of Local Government and Regional Development*. https://www.regjeringen.no/globalassets/upload/krd/prosjekter/e-valg/kildekode/evalg_rapport_kildekodejennomgang.pdf

- Bradshaw, P., & Fredette, C. (2008). Academic Governance of Universities. *Journal of Management Inquiry*, 18(2), 123-133. <https://doi.org/10.1177/1056492608326320>
- Cortier, V., Gaudry, P., & Glondou, S. (2019). Belenios: A Simple Private and Verifiable Electronic Voting System. In J. D. Guttman, C. E. Landwehr, J. Meseguer, & D. Pavlovic (Eds.), *Foundations of Security, Protocols, and Equational Reasoning, Lecture Notes in Computer Science* (11565 ed., pp. 214-238). Springer International Publishing. https://doi.org/10.1007/978-3-030-19052-1_14
- Cortier, V., & Smyth, B. (2013). Attacking and fixing Helios: An analysis of ballot secrecy. In *Journal of Computer Security*. <https://dl.acm.org/doi/10.5555/2595846.2595849>
- Council of Europe. (2017). *Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting: (Adopted by the Committee of Ministers on 14 June 2017 at the 1189th meeting of the Ministers' Deputies)*. Retrieved May 24, 2024, from https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f
- Czech Republic. (2024). *Zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách)*. Sbírka zákonů. Retrieved April 21, 2024, from <https://www.e-sbirka.cz/sb/1998/111?zalozka=text>
- Czech Republic. (2019). *Zákon o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů*. Sbírka zákonů. <https://www.e-sbirka.cz/sb/2019/99/2023-04-01>
- DERS Group. (2021). *Smlouva o dílo: UTB – modul Tajné hlasování (POLL)*. Registr smluv. Retrieved April 24, 2024, from https://smlouvy.gov.cz/smlouva/soubor/19253499/Smlouva_o_dilo_2021000002.pdf
- Deseriis, M. (2021). Rethinking the digital democratic affordance and its impact on political representation: Toward a new framework. *New Media & Society*, 23(8), 146144482092967. <https://doi.org/10.1177/1461444820929678>
- Deseriis, M. (2020). Digital movement parties: a comparative analysis of the technopolitical cultures and the participation platforms of the Movimento 5 Stelle and the Piratenpartei. *Information, Communication & Society*, 23(12), 1770-1786. <https://doi.org/10.1080/1369118x.2019.1631375>
- ElGamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In G. R. Blakley & D. Chaum (Eds.), *Advances in Cryptology* (pp. 10-18). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-39568-7_2
- ESC. (2024). *Frequently Asked Questions*. Election Services Co. Retrieved April 26, 2024, from <http://electionservicesco.com/pages/faqs.php>
- EU. (2016). *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Text s významem pro EHP)*. EUR-Lex. Retrieved April 22, 2024, from <https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex%3A32016R0679>

- Finogina, T., Cucurull Juan, J., & Costa, N. (2024). Selective comparison of verifiable online voting systems. *SECURITY AND PRIVACY*. <https://doi.org/10.1002/spy2.394>
- Gerbaudo, P. (2019). *The digital party: political organisation and online democracy: political organisation and online democracy*. London Pluto Press.
- Gerbaudo, P. (2021). Are digital parties more democratic than traditional parties? Evaluating Podemos and Movimiento 5 Stelle's online decision-making platforms. *Party Politics*, 27(4), 730-742. <https://doi.org/10.1177/1354068819884878>
- Germann, M., & Serdült, U. (2017). Internet voting and turnout: Evidence from Switzerland. In *Electoral Studies* (Vol. 47, pp. 1-12). <https://doi.org/10.1016/j.electstud.2017.03.001>
- Goodman, N., & Stokes, L. C. (2020). Reducing the Cost of Voting: An Evaluation of Internet Voting's Effect on Turnout. In *British Journal of Political Science* (Vol. 50, pp. 1155-1167). <https://doi.org/10.1017/S0007123417000849>
- Cheeseman, N., Lynch, G., & Willis, J. (2018). Digital dilemmas: the unintended consequences of election technology. *Democratization*, 25(8), 1397-1418. <https://doi.org/10.1080/13510347.2018.1470165>
- Harvard University. (2024). *Frequently Asked Questions*. Harvard Elections. Retrieved April 26, 2024, from <https://elections.harvard.edu/faq>
- Heiberg, S., Parsovs, A., & Willemson, J. (2015). Log Analysis of Estonian Internet Voting 2013-2015. <https://eprint.iacr.org/2015/1211>
- Huarte, M., Madarieta, M., Goirizelaia, I., & Unzilla, J. J. (2008). An Analysis of Improvements for Voter Interfaces in Polling Station and Remote Electronic Voting Systems. In *Visual Information Systems. Web-Based Visual Information Search and Management* (pp. 291-301). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-85891-1_32
- Charles University. (2024). *Volby do AS UK*. Univerzita Karlova. Retrieved April 19, 2024, from <https://cuni.cz/UK-1407.html>
- Jařab, J. (2008). Reforming systems and institutions of higher learning. In *Education, Citizenship and Social Justice* (Vol. 3, pp. 85-96). <https://doi.org/10.1177/1746197907086720>
- Jones, G. A., Shanahan, T., & Goyan, P. (2002). Traditional governance structures - current policy pressures: The academic senate and Canadian universities. *Tertiary Education and Management*, 8(1), 29-45. <https://doi.org/10.1080/13583883.2002.9967067>
- Junior, C. J. D. L. E. S., Vanderlei, I. M., Araujo, J. C. T. D., & Rocha, R. (2022). Evaluation of Open-Source E-Voting Systems Using Helios Voting in Public University Elections. In *Proceedings of the Brazilian Symposium on Multimedia and the Web* (pp. 11-18). ACM. <https://doi.org/10.1145/3539637.3557061>
- Kouba, K. (2017). Determinants of student participation in higher education governance: the case of student turnout in academic senate elections in Czechia. *Higher Education*, 76(1), 67-84. <https://doi.org/10.1007/s10734-017-0194-1>
- Krimmer, R., Duenas-Cid, D., Krivososova, I., Vinkel, P., & Koitmae, A. (2018). How Much Does an e-Vote Cost? Cost Comparison per Vote in Multichannel Elections in Estonia. In R. Krimmer,

- M. Volkamer, V. Cortier, R. Goré, M. Hapsara, U. Serdült, & D. Duenas-Cid (Eds.), *Electronic Voting* (pp. 117-131). Springer International Publishing. https://doi.org/10.1007/978-3-030-00419-4_8
- La Commission nationale de l'informatique et des libertés. (2019). *Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet: NOR : CNIL1917529X*. Légifrance. Retrieved April 6, 2023, from <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038661239>
- Magna Charta Universitatum. (2022). *Magna Charta 1988*. Observatory Magna Charta Universitatum. Retrieved April 26, 2024, from <https://www.magna-charta.org/magna-charta-universitatum/mcu-1988>
- Marcos del Blanco, D. Y., Duenas-Cid, D., & Aláiz Moretón, H. (2020). E-Voting System Evaluation Based on the Council of Europe Recommendations: nVotes. In R. Krimmer, M. Volkamer, B. Beckert, R. Küsters, O. Kulyk, D. Duenas-Cid, & M. Solvak (Eds.), *Electronic Voting* (pp. 147-166). Springer International Publishing. https://doi.org/10.1007/978-3-030-60347-2_10
- Marcos del Blanco, D. Y., & Gascó, M. (2019). A Protocolized, Comparative Study of Helios Voting and Scytl/iVote. In *2019 Sixth International Conference on eDemocracy & eGovernment (ICEDEG)* (pp. 31-38). IEEE. <https://doi.org/10.1109/ICEDEG.2019.8734351>
- Martínek, T., & Malý, M. (2024). Evaluation of the I-Voting System for Remote Primary Elections of the Czech Pirate Party. *Acta Informatica Pragensia*. <https://doi.org/10.18267/j.aip.249>
- Martínek, T., Pelikán, M., Tyrychtr, J., & Konopásek, J. (2024). Implementation of a Secret and Verifiable Personal Remote Electronic Election of an Agrarian Organization per the Recommendation of the Council of Europe. *AGRIS on-line Papers in Economics and Informatics*, 16(3), 59-73. <https://doi.org/10.7160/aol.2024.160305>
- Martínek, T., & Tyrychtr, J. (2024). A questionnaire survey of expected characteristics of i-voting systems among students and graduates of agricultural colleges: [Data set]. In *Zenodo*. <https://doi.org/10.5281/zenodo.11234690>
- Ministry of Education of the Czech Republic. (2024). *Data o studentech, poprvé zapsaných a absolventech vysokých škol*. MSMT.cz. Retrieved April 22, 2024, from <https://www.msmt.cz/vzdelavani/skolstvi-v-cr/statistika-skolstvi/data-o-studentech-poprve-zapsanych-a-absolventech-vysokych>
- Ministry of Local Government and Regional Development. (2010). *Specification, tenders, evaluation and contract*. Government.no. Retrieved January 6, 2024, from <https://www.regjeringen.no/en/historical-archive/Stoltenbergs-2nd-Government/Ministry-of-Local-Government-and-Regiona/tema-og-redaksjonelt-innhold/kampanjesider/e-vote-trial/System-documentation/specification-tenders-evaluation-and-con/id612121/>
- MUNI. (2024). Realizace tajných hlasování s využitím aplikace E-volby v IS MU. Retrieved July 30, 2024, from <https://is.muni.cz/do/mu/schuze/pages/02-evolby.html>
- NÚKIB. (2023). *Minimální bezpečnostní standard*. Národní úřad pro kybernetickou a informační bezpečnost. Retrieved April 24, 2024, from https://nukib.gov.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

- nVotes. (2024). *Some of our customers*. NVotes online voting system. Retrieved April 26, 2024, from <https://nvotes.com/customers/>
- Panizo Alonso, L., Gascó, M., Marcos del Blanco, D. Y., Alonso, J. Á. H., Barrat, J., & Moreton, H. A. (2018). E-Voting System Evaluation Based on The Council of Europe Recommendations: Helios Voting. *IEEE Transactions on Emerging Topics in Computing*, 9(1), 161-173. <https://doi.org/10.1109/TETC.2018.2881891>
- Pawar, B. M., Patode, S. H., Potbhare, Y. R., & Mohota, N. A. (2020). An Efficient and Secure Students Online Voting Application. In *2020 Fourth International Conference on Inventive Systems and Control (ICISC)* (pp. 1-4). IEEE. <https://doi.org/10.1109/ICISC47916.2020.9171063>
- Pennock, L., Jones, G. A., Leclerc, J. M., & Li, S. X. (2015). Challenges and Opportunities for Collegial Governance at Canadian Universities: Reflections on a Survey of Academic Senates. *Canadian Journal of Higher Education*, 46(3), 73-89. <https://doi.org/10.47678/cjhe.v46i3.188017>
- Rodríguez-Pérez, A. (2022). The Council of Europe's CM/Rec(2017)5 on e-voting and Secret Suffrage: Time for yet Another Update? In R. Krimmer, M. Volkamer, D. Duenas-Cid, P. Rønne, & M. Germann (Eds.), *Electronic Voting* (13553rd ed., pp. 90-105). Springer International Publishing. https://doi.org/10.1007/978-3-031-15911-4_6
- Qadah, G. Z., & Taha, R. (2007). Electronic voting systems: Requirements, design, and implementation. In (Vol. 29, pp. 376-386). <https://doi.org/10.1016/j.csi.2006.06.001>
- Scytl. (2024). *Online Voting for Universities*. Scytl. Retrieved April 26, 2024, from <https://scytl.com/online-voting/industries/university/>
- SLU. (2020). E-volby. Retrieved July 30, 2024, from <https://www.slu.cz/opf/cz/file/cul/bddad904-c39b-4945-a532-6c6a01e1d554>
- Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014). Security Analysis of the Estonian Internet Voting System. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 703-715). ACM. <https://doi.org/10.1145/2660267.2660315>
- UPOL. (2022). Volby. Retrieved July 30, 2024, from <https://wiki.upol.cz/upwiki/Volby>
- Valimised. (2024). *IVXV online voting system*. GitHub. Retrieved January 6, 2024, from <https://github.com/valimised/ivxv>
- von Nostitz, F., & Sandri, G. (2021). I-Voting Regulation Within Digital Parties: The Case of Podemos and Five Stars Movement [Online]. In O. Barberà, G. Sandri, P. Correa, & J. Rodríguez-Teruel (Eds.), *Digital Parties* (pp. 85-107). Springer International Publishing. https://doi.org/10.1007/978-3-030-78668-7_5
- von Nostitz, F., Sandri, G., & Esteve, J. B. i. (2021). Regulating i-Voting Within Countries and Parties. In O. Barberà, G. Sandri, P. Correa, & J. Rodríguez-Teruel (Eds.), *Digital Parties* (pp. 43-66). Springer International Publishing. https://doi.org/10.1007/978-3-030-78668-7_3
- VŠE. (2021). Elektronické hlasování a volby v InSIS. Retrieved July 30, 2024, from <https://fis.vse.cz/wp-content/uploads/InSIS-volby-manual-pro-volice-FIS.pdf>

- Willemson, J., & Krips, K. (2023). Estimating Carbon Footprint of Paper and Internet Voting. *Electronic Voting*, 140-155. https://doi.org/10.1007/978-3-031-43756-4_9
- ZČU. (2023). Průvodce volbami do AS FPE. Retrieved July 30, 2024, from <https://www.fpe.zcu.cz/rest/cmis/document/workspace://SpacesStore/2f10475d-1392-4350-8453-e53371e1b151;1.0/content>