ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

Ασφάλεια Πληροφοριακών & Επικοινωνιακών Συστημάτων

Ηλεκτρονική Ψηφοφορία: Ασφάλεια και Ιδιωτικότητα στα συστήματα ηλεκτρονικής ψηφοφορίας

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Βανδώρου Ελευθέριου

Επιβλέπων : Κυρία Μαρία Καρύδα, Αναπληρώτρια Καθηγήτρια, Πανεπιστήμιο Αιγαίου

Μέλη εξεταστικής επιτροπής:

- Κύριος Σπυρίδων Κοκολάκης, Καθηγητής, Πανεπιστήμιο Αιγαίου
- Κυρία Ευαγγελία Μήτρου, Καθηγήτρια, Πανεπιστήμιο Αιγαίου

Σάμος, [06/2020]

Υπεύθυνη Δήλωση

Βεβαιώνω ότι είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην διπλωματική εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η διπλωματική εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών.

του
Βανδώρου Ελευθέριου
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Ευχαριστίες

Ευχαριστώ θερμά την επιβλέπουσα καθηγήτρια αυτής της εργασίας, κυρία Καρύδα Μαρία, για την καθοδήγηση, τις συμβουλές και τις τελικές διορθώσεις. Μου επέτρεψε να προσεγγίσω τη συγκεκριμένη θεματολογία με τον τρόπο που επιθυμούσα, ενώ το δικό της επιστημονικό και συγγραφικό έργο αποτέλεσε σημαντική πηγή πληροφοριών και σημείο εκκίνησης της παρούσας διπλωματικής εργασίας.

Αισθάνομαι ακόμη πως οφείλω ένα ευχαριστώ και στο σύνολο των καθηγητών μου, κατά τη φοίτησή μου στο Πανεπιστήμιο Αιγαίου στο Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων για τις γνώσεις που μου μετέδωσαν και οι οποίες με βοήθησαν στην ορθή προσέγγιση του θέματος.

Περιεχόμενα

Λίστα Πινάκων

Ακρωνύμια

ATM	Automated Teller Machines
IRV	Instant Runoff Voting-άμεση ψηφοφορία.
STV	Single Transferable Vote-μεταφερόμενη μονοσταυρία
EBM	Electronic Ballot Marker - Ηλεκτρονικός Σηματοδότης
ITV	Interactive television systems
EMB	Electoral Management Board

Περίληψη

Η παρούσα εργασία ασχολείται με την ηλεκτρονική ψηφοφορία. Συγκεκριμένα, η μελέτη εστιάζει στους διάφορους τρόπους εφαρμογής της ηλεκτρονικής ψηφοφορίας σε διάφορες χώρες, την ασφάλεια της ιδιωτικότητας των χρηστών της και την διαμόρφωση του νομικού πλαισίου. Παράλληλα, προσδιορίζεται ο όρος ηλεκτρονική ψηφοφορία, όπως επίσης οι μορφές της. Ειδικότερα, γίνεται αποσαφήνιση των όρων e-voting και i-voting. Στη συνέχεια, παρουσιάζονται μηχανήματα ηλεκτρονικής ψηφοφορίας και οι ευπάθειες αυτών.

Η ηλεκτρονική ψηφοφορία είναι μια πολλά υποσχόμενη εξέλιξη που μπορεί να συμβάλει στην ενίσχυση της συμμετοχής των πολιτών στη δημοκρατική διαδικασία. Ωστόσο, προκειμένου να διασφαλιστεί η επιτυχής υιοθέτηση της ηλεκτρονικής ψηφοφορίας, τα θέματα ασφάλειας και προστασίας της ιδιωτικής ζωής πρέπει να αντιμετωπιστούν και να επιλυθούν επαρκώς.

Όπως αναφέρθηκε παραπάνω, η μελέτη εστιάζει κυρίως στην εφαρμογή της ηλεκτρονικής ψηφοφορίας σε χώρες της Ευρώπης, σε διάφορες αναπτυσσόμενες χώρες, στην Ινδία, στις ΗΠΑ και στην Αυστραλία. Επίσης, περιγράφονται τα κυριότερα προβλήματα που συνάντησε η εφαρμογή της ηλεκτρονικής ψηφοφορίας σε αυτές τις χώρες. Στο τέλος της εργασίας παρουσιάζονται τα συμπεράσματα.

Λέξεις κλειδιά: Μηχανήματα ηλεκτρονικής ψηφοφορίας , e-voting, i-voting, ηλεκτρονική ψηφοφορία, διαδικτυακή ψηφοφορία, ψηφιακή ψηφοφορία

Abstract

This paper deals with electronic voting. Specifically, the study focuses on the different ways in which e-voting is implemented in different countries. At the same time, the term electronic voting, as well as its forms, is described. Furthermore, the terms e-voting and i-voting are being clarified. Also, electronic voting machines and their vulnerabilities are presented.

Electronic voting is a very promising development that may serve to enhance citizens' participation in the democratic process. Nevertheless, in order to ensure the successful adoption of e-voting, security, and privacy issues must be adequately addressed and solved.

As mentioned above, the study focuses mainly on the application of electronic voting in European countries, in various developing countries, in India, in the USA and in Australia. It also outlines the main problems encountered in the implementation of e-voting in these countries. At the end of the paper the conclusions are presented.

Key Words: Electronic voting machines, e-voting, i-voting, security in electronic and internet voting, e-enabled voting, digital voting

1

Ηλεκτρονική Ψηφοφορία (e-Voting)

Εισαγωγή

Με την ραγδαία ανάπτυξη της τεχνολογίας έχει δημιουργηθεί η επιθυμία στον άνθρωπο να πραγματοποιεί τις καθημερινές του δραστηριότητες μέσω ηλεκτρονικών συστημάτων ώστε να εξοικονομεί χρόνο και να ελαττώσει την κούραση του (πχ e-banking). Η τεχνολογία έκανε την επανάστασή της και στον τομέα της ψηφοφορίας φέρνοντας το I-voting (Ηλεκτρονική Διαδικτυακή Ψηφοφορία) και το E-Voting (Ηλεκτρονική ψηφοφορία). Σε μία σύγχρονη δημοκρατική χώρα, οι εκλογές γίνονται με την χρήση ενός συστήματος ηλεκτρονικής ψηφοφορίας. Η χρήση ηλεκτρονικών υπολογιστών καθιστά την εκλογική διαδικασία πιο αποτελεσματική για την λήψη των ψήφων και για την αύξηση του αριθμού των ψηφοφόρων.

Ο σκοπός μίας ψηφοφορίας δεν είναι μόνο να αναδείξει έναν νικητή αλλά και να πείσει τον ηττημένο και τους υποστηρικτές του πως ηττήθηκαν . Το βασικότερο στοιχείο στην διαδικασία ψηφοφορίας με όποιο μέσω και να διεκπεραιώνεται είναι η εμπιστοσύνη του ψηφοφόρου στο σύστημα αυτό.

Η ηλεκτρονική ψηφοφορία είναι πολύ ελπιδοφόρα, αλλά θέτει πολλές τεχνολογικές και κοινωνικοπολιτικές προκλήσεις. Μεταξύ των τεχνολογικών προκλήσεων, η ασφάλεια και το απόρρητο θεωρούνται οι πιο σημαντικές και η επίλυσή τους είναι υψίστης σημασίας για την ομαλή μετάβαση από τις συμβατικές μεθόδους ψηφοφορίας στην ηλεκτρονική ψηφοφορία.

Είναι σημαντικό να τονιστεί ότι η τεχνολογία ψηφοφορίας δεν μπορεί να αξιολογηθεί μεμονωμένα. Κάθε τεχνολογία ψηφοφορίας χρησιμοποιείται στο πλαίσιο ενός ευρύτερου συστήματος, είτε η τεχνολογία ψηφοφορίας βασίζεται σε χάρτινα ψηφοδέλτια είτε σε ηλεκτρονικά. Ορισμένα στοιχεία αυτού του μεγαλύτερου συστήματος μπορεί να είναι μηχανικά ή ηλεκτρονικά, αλλά το σύστημα περιλαμβάνει επίσης τους νόμους, τους διοικητικούς κανόνες και τις μη αυτόματες διαδικασίες που αφορούν την τεχνολογία ψηφοφορίας.

Όπως κάθε φορά που μετράμε τους ψήφους με το χέρι, πρέπει να εξετάσουμε τους νόμους και τους διοικητικούς κανόνες που διέπουν την καταμέτρηση, έτσι και όταν

υπάρχουν μηχανικές διαδικασίες, πρέπει να ρωτήσουμε πώς προετοιμάζονται, συντηρούνται και ελέγχονται οι μηχανισμοί. Όταν εμπλέκονται συστήματα υπολογιστών, πρέπει να ρωτήσουμε πώς προγραμματίζονται οι υπολογιστές και ποιες διαβεβαιώσεις έχουμε ότι τα προγράμματα που προορίζονται για χρήση είναι και αυτά που χρησιμοποιούνται για τη διαχείριση των εκλογών.

Η πρόταση ότι ένα έντιμο εκλογικό σύστημα πρέπει να βασίζεται στην εμπιστοσύνη είναι επικίνδυνη. Εάν επεκτείνουμε την εμπιστοσύνη μας σε οποιοδήποτε άτομο ή οργανισμό, οι απατεώνες που προτίθενται να ανατρέψουν το εκλογικό σύστημα σίγουρα θα βρουν έναν τρόπο να υπονομεύσουν αυτό το άτομο ή τον οργανισμό. Επομένως, πρέπει να σχεδιαστούν τα εκλογικά συστήματα υπό την προϋπόθεση ότι κάθε συμμετέχων είναι κομμάτι κάποιων υποψηφίων και δεν είναι απόλυτα αξιόπιστος.

Πολλά ψηφιακά μέτρα ασφαλείας υπάρχουν ήδη στην αγορά και μπορούν να εφαρμοστούν σε συστήματα Remote Electronic Voting (REV). Παρόλο που ορισμένα από αυτά τα μέτρα ασφαλείας (όπως firewalls, transport-level encryption, intrusion detection systems, κ.λπ.) μπορούν να είναι αξιόπιστα εάν διαχειρίζονται καλά, είναι πολύ γενικά ορισμένα και επομένως δεν ανταποκρίνονται καλά στις συγκεκριμένες απαιτήσεις ασφαλείας που τίθενται με τις εφαρμογές για την ηλεκτρονική ψηφοφορία. Ένα σύστημα ηλεκτρονικής ψηφοφορίας από τη φύση του δημιουργεί πολλαπλές ανησυχίες για την ασφάλεια που δεν αντιμετωπίζονται επαρκώς από τις τρέχουσες τεχνολογίες ασφάλειας. Επιπλέον, αυτές οι τεχνολογίες ασφάλειας εστιάζουν στην πρόληψη επιθέσεων από εξωτερικούς εισβολείς, αφήνοντας τα συστήματα εκτεθειμένα στην πιθανότητα επιθέσεων που προέρχονται από το εσωτερικό (που είναι πολύ πιο επικίνδυνες δεδομένης της προνομιακής θέσης των επιτιθέμενων).

Οι ικανότητες της ηλεκτρονικής ψηφοφορίας φαίνονται προς το παρόν με μεγάλο ενδιαφέρον, και έτσι σήμερα η ηλεκτρονική ψηφοφορία έχει την ευκαιρία να υιοθετηθεί ευρέως στο εγγύς μέλλον. Ωστόσο, εάν κάτι πάει στραβά με την ασφάλεια (την ακεραιότητα των αποτελεσμάτων, το απόρρητο των ψηφοφόρων κ.λπ.) κατά τη διάρκεια μιας μεγάλης εκδήλωσης ή πιλοτικού προγράμματος ηλεκτρονικής ψηφοφορίας, αυτό θα μπορούσε να καταστρέψει την εμπιστοσύνη του κοινού και να υπονομεύσει όλες τις τρέχουσες εργασίες για την εισαγωγή της ηλεκτρονικής ψηφοφορίας στην κοινωνία. Αυτή είναι στην πραγματικότητα μια πολύ τρομακτική

προοπτική, διότι καθώς η ηλεκτρονική ψηφοφορία αποκτά σημασία και εύρος, θα γίνει πιο ελκυστικός στόχος για κάθε είδους εισβολείς. Τα τρέχοντα ψηφιακά μέτρα ασφάλειας ενδέχεται να παρέχουν μια ψευδή αίσθηση ασφάλειας που μπορεί να οδηγήσει σε καταστροφικά αποτελέσματα.

Η παραδοσιακή εκλογική διαδικασία, έχει ως μειονεκτήματα ότι είναι χρονοβόρα, δαπανηρή και καθιστά αναγκαία την καταμέτρηση των ψηφοδελτίων από ανθρώπινο δυναμικό. Χρονοβόρα καθίσταται διότι απαιτεί πολύ χρόνο για την καταμέτρηση των ψήφων και για την εμφάνιση των αποτελεσμάτων. Ακόμα καθίσταται δαπανηρή για το προσωπικό που χρησιμοποιεί, τις μεγάλες ποσότητες χαρτιού και από την μεριά του ψηφοφόρου για να μεταβεί στο μέρος της ψηφοφορίας. Με αποτέλεσμα οι λόγοι αυτοί να καθιστούν ελκυστικά τα μηχανικά ή ηλεκτρονικά συστήματα ψηφοφορίας. Η ηλεκτρονική ψηφοφορία έχει γίνει ολοένα και πιο δημοφιλής στον κόσμο που βασίζεται στην τεχνολογία.

Αντιθέτως, με τα μηχανήματα για την ηλεκτρονική ψηφοφορία, με την ψηφοφορία μέσω διαδικτύου δίνεται η δυνατότητα στους ψηφοφόρους να ψηφίζουν μέσω μίας ιστοσελίδας με ένα μόνο κλίκ ή ένα άγγιγμα με το δάκτυλο τους. Τα μηχανήματα ηλεκτρονικής ψηφοφορίας θα μπορούσαν κάποια μέρα να χρησιμοποιηθούν σε συνδυασμό με την χρήση χάρτινου ψηφοδελτίου για την αύξηση της ασφάλειας ενώ η ηλεκτρονική ψηφοφορία μέσω διαδικτύου δεν είναι ασφαλής και είναι ακατόρθωτο να επιτευχθεί με ασφάλεια, τουλάχιστον μέχρι σήμερα.

Ωστόσο οι πολιτικοί σχεδιάζουν να εισάγουν την διαδικτυακή ψηφοφορία, αψηφώντας τον ξεκάθαρο κίνδυνο που διατρέχει η ακεραιότητα της δημοκρατικής διαδικασίας. Η κυρία Teague σε μια συνέντευξη της (Dr. VanessaTeague είναι ερευνήτρια και κρυπτογράφος στο Πανεπιστήμιο της Μελβούρνης στην Αυστραλία) επισήμανε πως «Οτιδήποτε είναι στο διαδίκτυο δεν είναι ασφαλές ,έτσι και η διαδικτυακή ψηφοφορία δεν αποτελεί εξαίρεση. Αλλά το σημαντικότερο για τις εκλογές είναι πως δεν είναι ποτέ σε θέση , η εφορευτική επιτροπή, να απαντήσει με απόλυτη σιγουριά αν το αποτέλεσμα έχει νοθευτεί η όχι.

Επομένως, τα προαναφερθέντα αποτελέσαν τον σκοπό της συγγραφής της συγκεκριμένης διπλωματικής εργασίας. Απλούστερα, η εργασία έχει ως στόχο να εξετάσει τις ευπάθειες της ηλεκτρονικής αλλά και της ψηφιακής ψηφοφορίας, την

ασφάλεια της ιδιωτικότητας και να προτείνει λύσεις για την εισαγωγή της σε ένα κράτος. Ακόμη γίνεται μία προσέγγιση στην διαμόρφωση του νομικού πλαισίου.

Αρχικά γίνεται μία παρουσίαση των ειδών της ηλεκτρονικής ψηφοφορίας, με απώτερο σκοπό την κατανόηση για τον τρόπο λειτουργίας της. Στο πλαίσιο αυτό γίνεται αναφορά στα μηχανήματα που χρησιμοποιούνται από την ηλεκτρονική ψηφοφορία. Γίνεται παρατήρηση στην ασφάλεια της ψηφοφορίας και τα πρωτόκολλα που χρησιμοποιεί ή θα ήταν πρέπον να χρησιμοποιούνται για την ασφάλεια της ψηφοφορίας, εφόσον διαφέρει από οποιαδήποτε άλλη διαδικασία που πραγματοποιείται στο διαδίκτυο. Έπειτα η τεκμηριώνει τις ευπάθειες της ηλεκτρονικής ψηφοφορίας μέσω διαδικτύου αλλά και μέσω των μηχανημάτων. Συνεχίζει με την αναφορά διαφόρων πιθανών επιθέσεων και σα δύο είδη ψηφοφορίας . Έπειτα, διαμορφώνει μία πλήρης εικόνα για το νομικό πλαίσιο μιας χώρας ώστε να πραγματοποιείται έγκυρα αλλά και με ασφάλεια η διαδικασία. Ακόμη δεν παραλείπεται η αναφορά των λύσεων επιστημόνων για την βελτίωση των REV μηχανημάτων. Τέλος, επισημαίνει τα συμπεράσματα και τις λύσεις των χωρών που εφάρμοσαν την ψηφιακή ή την ηλεκτρονική ψηφοφορία.

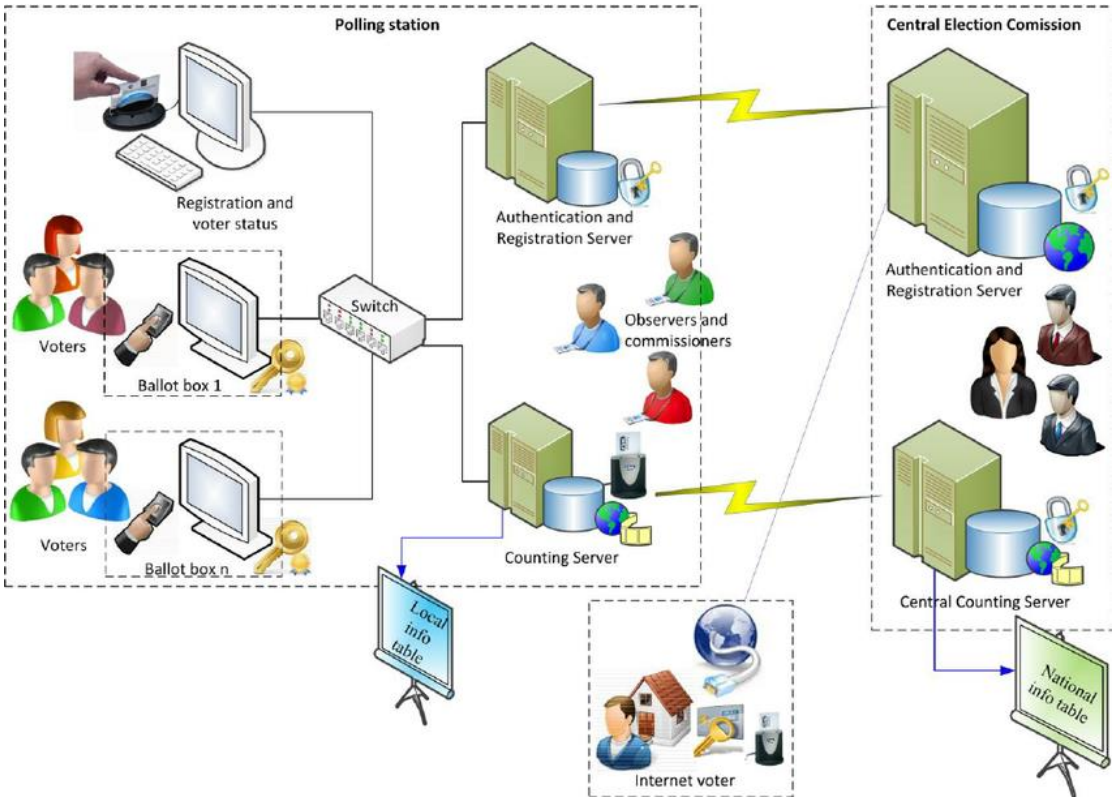
1.1 Ηλεκτρονική ψηφοφορία

Η αυξημένη χρήση της τεχνολογίας πληροφοριών υπόσχεται να φέρει επανάσταση τόσο στην παροχή κρατικών υπηρεσιών όσο και στη ζωντάνια της δημοκρατίας[1]. Η αναδυόμενη κοινωνία της πληροφορίας επέτρεψε στους ανθρώπους των ανεπτυγμένων χωρών να εκτελούν πολλές από τις δραστηριότητές τους με άμεσο, ηλεκτρονικά αυτοματοποιημένο και αποτελεσματικό τρόπο. Για να συμβαδίσουν με τις ανάγκες της εποχής αλλά και των πολιτών, τα κράτη επιχειρούν να προβούν σε χρήση της δυνατότητας και να επωφεληθούν από υπηρεσίες μέσω δικτύων. Οι κυβερνήσεις των αναπτυγμένων χωρών προσπαθούν να μεταφέρουν όλο και περισσότερες δραστηριότητες σε ηλεκτρονική μορφή ώστε να καταφέρουν την μείωση του κόστους και της γραφειοκρατίας της δημόσιας διοίκησης. Η ηλεκτρονική ψηφοφορία είναι μια

από τι ς υπηρεσίες που αποσκοπούν τα αναπτυγμένα κράτη να προωθήσουν με αυτή τη λογική.

Ο όρος ηλεκτρονική ψηφοφορία χρησιμοποιείται για να δηλώσει μια διαδικασία ψηφοφορίας, η οποία επιτρέπει στους ψηφοφόρους να κάνουν μια ασφαλή και μυστική ψηφοφορία μέσω ενός δικτύου και ο ψηφοφόρος που ψηφίζει δεν παρακολουθείται κατά τη διάρκεια της ψηφοφορίας. Η εγγραφή μπορεί να είναι είτε φυσική ή να πραγματοποιείται ηλεκτρονικά. Η ηλεκτρονική ψηφοφορία θεωρείται μέσω για την περαιτέρω ενίσχυση των δημοκρατικών διαδικασιών στις σύγχρονες κοινωνίες των πληροφοριών. Μετά τη διαμάχη για την ψηφοφορία στη Φλόριντα κατά τις προεδρικές εκλογές του 2000, οι κυβερνήσεις ανέθεσαν την πίστη τους στην τεχνολογία, υιοθετώντας μηχανές ηλεκτρονικής ψηφοφορίας που προσφέρουν ευκολότερη πρόσβαση στους ψηφοφόρους και εξαλείφουν τις υποψίες για υποκειμενικές ή μεροληπτικές αντιδράσεις. Επιπλέον, η ηλεκτρονική ψηφοφορία μπορεί να αποτελέσει έναν αποτελεσματικό και οικονομικά αποδοτικό τρόπο για τη διεξαγωγή της διαδικασίας της ψηφοφορίας, όπως κι έναν αποτελεσματικό τρόπο για την προσέλκυση συγκεκριμένων ομάδων ατόμων (π.χ. νέων, αναπήρων, κλπ). Ιδιαίτερα, οι κυβερνητικές υπηρεσίες αν τονίσουν τα οφέλη της ηλεκτρονικής υπηρεσίας σε νέους ψηφοφόρους, η ευκολία και η συμβατότητα της δύναται να έχει αρκετή επιρροή για να παρακινήσει αυτόν τον απαθή πληθυσμό των νέων ατόμων για να συμμετάσχει στην εκλογική διαδικασία. Η καθιέρωση της ηλεκτρονικής ψηφοφορίας, και μάλιστα της ψηφοφορίας μέσω διαδικτύου αναμένεται να απλοποιήσει και να περιορίσει τα λάθη κατά τη διαδικασία υποβολής και καταμέτρησης των ψήφων (Mohen,2001)

Το βασικό όμως είναι η ηλεκτρονική ψηφοφορία πρώτα να συμμορφώνεται με το υφιστάμενο νομικό και κανονιστικό πλαίσιο του κράτους. Στη συνέχεια, η ηλεκτρονική ψηφοφορία θα πρέπει να υλοποιείται τεχνικά κατά τρόπο που να διασφαλίζει επαρκής πρόσβαση των χρηστών [2].



Εικόνα 1 Απεικόνιση της ηλεκτρονικής ψηφοφορίας (πηγή https://www.researchgate.net/profile/Vehbi_Neziri/publication/236693845/figure/fig2/AS:299395879850006@1448392948517/General-architecture-of-e-Voting-system.png)

1.2 Αποσαφήνιση όρων

Ηλεκτρονική ψηφοφορία νοείται το δικαίωμα άσκησης του εκλογικού δικαιώματος ενός πολίτη με την χρήση ηλεκτρονικών μεθόδων. Τα δύο θεμελιώδη στοιχεία που αποτελούν την ηλεκτρονική ψηφοφορία είναι η δυνατότητα άσκησης του εκλογικού δικαιώματος απομακρυσμένα με την χρήση υπολογιστικού συστήματος και η διεξαγωγή της εκλογικής διαδικασίας με τη χρήση ηλεκτρονικών συστημάτων. Επίσης, πρέπει να σημειωθεί ότι η ηλεκτρονική ψηφοφορία αναφέρεται σε ηλεκτρονικές μηχανές ψηφοφορίας που χρησιμοποιούν ηλεκτρονικά ψηφοδέλτια και όχι σε έγγραφα που αναφέρονται σε μηχανογραφικά μηχανήματα ψηφοφορίας και είναι επίσης γνωστά ως ηλεκτρονικές μηχανές άμεσης καταγραφής ή DREs (direct-recording electronic).

1.3 Ηλεκτρονικό σύστημα ψηφοφορίας

Ένα ηλεκτρονικό σύστημα ψηφοφορίας περιλαμβάνει ένα πλήθος μονάδων ασύρματης απόκρισης, κάθε μονάδα απόκρισης είναι ικανή να μεταδίδει πολλά διαφορετικά ψηφιακά κωδικοποιημένα σήματα. Κάθε ένα από αυτά τα ψηφιακά κωδικοποιημένα σήματα αντιστοιχεί στην απόκριση ενός ατόμου που ανταποκρίνεται σε ένα δεδομένο ερέθισμα. Κάθε μονάδα απόκρισης μεταδίδει μια επιλεγμένη ψηφιακά κωδικοποιημένη απόκριση μέσω ενός σήματος ραδιοσυχνότητας κατά τη διάρκεια μιας σειράς χρονικών διαστημάτων, διαφορετικό χρονικό διάστημα που αντιστοιχεί σε κάθε μια από τις μονάδες απόκρισης. Μία μονάδα επεξεργασίας σηματοδοτεί τις μονάδες απόκρισης να αρχίσουν τη μετάδοση απόκρισης ώστε να ξεκινήσει να λαμβάνει, να επεξεργάζεται και να εμφανίζει τις μεταδιδόμενες αποκρίσεις για παρατήρηση από επιλεγμένα πρόσωπα.

1.4 Στάδια ηλεκτρονικής ψηφοφορίας

Η ηλεκτρονική ψηφοφορία δεν είναι μια απλή διαδικασία, κι όπως η παραδοσιακή ψηφοφορία προϋποθέτει ορισμένα στάδια για τη διεξαγωγή της. Σε σύγκριση με την παραδοσιακή ψηφοφορία, τα στάδια της ηλεκτρονικής ψηφοφορίας είναι απλούστερα και φιλικότερα στη χρήση για τους ψηφοφόρους.
Αν επιχειρήσουμε να περιγράψουμε τα στάδια της ηλεκτρονικής ψηφοφορίας, πρώτα θα χωρίζαμε τη διαδικασία αυτή με βάση τα βήματα που ακολουθούν οι ψηφοφόροι.

i. Το πρώτο στάδιο είναι αυτό κατά το οποίο οι ψηφοφόροι αποδεικνύουν την αληθινή τους ταυτότητα και τη νομιμότητα του δικαιώματος τους να ψηφίσουν, όπως το όριο ηλικίας ή η κατοχή των εκλογικών δικαιωμάτων κλπ. Σε αυτό το στάδιο οι εγγραφόμενοι χρήστες προστίθενται στον εκλογικό κατάλογο.
ii. Το δεύτερο στάδιο είναι το στάδιο της επικύρωσης. Το στάδιο αυτό αποτελεί το στάδιο της επιβεβαίωσης της ταυτότητας του ψηφοφόρου. Κατά την ηλεκτρονική ψηφοφορία, όπως ακριβώς και στην παραδοσιακή, οι ψηφοφόροι εγγράφονται σε καταλόγους και πριν υποβάλλουν τη ψήφο τους, οι ψηφοφόροι

ταυτοποιούνται (identification), επιβεβαιώνεται δηλαδή η ταυτότητα τους τη δεδομένη χρονική στιγμή.

iii. Το τρίτο στάδιο είναι το στάδιο κατά το οποίο υποβάλλεται η ψήφος από τους ψηφοφόρους. Συναφές με τη διαδικασία, ονομάζεται το στάδιο της υποβολής της ψήφου. Κάθε ψηφοφόρος έχει δικαίωμα να υποβάλλει μόνο μια φορά την οριστική/τελική του ψήφο. Αυτό είναι το κυριότερο στάδιο που ενδιαφέρει τον ψηφοφόρο καθώς για τον ψηφοφόρο εκλογές σημαίνουν την υποβολή της ψήφου επιλογής του.

iv. Το τέταρτο στάδιο είναι η καταμέτρηση ψήφων. Πρόκειται για το τελευταίο στάδιο της ηλεκτρονικής ψηφοφορίας, το οποίο ξεκινά μόλις εκπνεύσει η προθεσμία υποβολής ψήφων. Οι ψήφοι καταμετρούνται– με τρόπο που περιγράφεται στη συνέχεια της παρούσας εργασίας – ενώ μετά την ολοκλήρωση αυτού του σταδίου ανακοινώνεται το αποτέλεσμα των εκλογών.

Η διαδικασία της ηλεκτρονικής ψηφοφορίας αποτελείται, όπως περιεγράφηκε παραπάνω, από τέσσερα στάδια. Αυτά τα στάδια είναι δυνατόν να πραγματοποιηθούν είτε με διαδικασίες όπου υπάρχει φυσική παρουσία του ψηφοφόρου είτε με ηλεκτρονικές διαδικασίας οπότε δεν απαιτείται φυσική παρουσία του ψηφοφόρου.

1.5 Τύποι ηλεκτρονικής ψηφοφορίας

Οι τύποι της ηλεκτρονικής ψηφοφορίας είναι δυο. Ο πρώτος τύπος είναι η ηλεκτρονική ψηφοφορία σε εκλογικά σημεία (Polling Place E-Voting) και ο δεύτερος τύπος είναι η ηλεκτρονική ψηφοφορία μέσω διαδικτύου (Internet Voting).

1.5.1 Ψηφοφορία μέσω διαδικτύου

Σε αυτόν τον τύπο της ηλεκτρονικής ψηφοφορίας, η ψήφος υποβάλλεται από τον ψηφοφόρο μέσω διαδικτύου και τα συστήματα-πελάτες βρίσκονται υπό ελλιπής είτε μηδαμινή επιτήρηση. Ελλιπής ή μηδαμινή επιτήρηση σημαίνει ότι οι ψηφοφόροι βρίσκονται σε χώρο όπου δεν υπάρχει κάποιος αρμόδιος (υπεύθυνος, υπάλληλος, κλπ) των εκλογών, π.χ. ο ψηφοφόρος βρίσκεται στο σπίτι, στον χώρο εργασίας, σε

εστιατόριο, στο δρόμο, σε σχολεία κλπ – οπουδήποτε μπορεί να συνδεθεί στο διαδίκτυο.

Στην ψηφοφορία μέσω του διαδικτύου το πρώτο στάδιο, δηλαδή η εγγραφή μπορεί να γίνει είτε με φυσικές είτε με ηλεκτρονικές διαδικασίες. Οι φυσικές διαδικασίες εγγραφής περιλαμβάνουν την παρουσία σε εκλογικά γραφεία, ενώ οι ηλεκτρονικές διαδικασίες εγγραφής περιλαμβάνουν την ψηφιακή υπογραφή και τις μεθόδους βιομετρικής. Αμέσως μετά ακολουθεί το στάδιο της επικύρωσης η οποία πραγματοποιείται αποκλειστικά ηλεκτρονικά. Στη συνέχεια, μόνο μέσω ηλεκτρονικών διαδικασιών πραγματοποιείται και το στάδιο της υποβολής. Τέλος, όπως τα προηγούμενα στάδια έτσι και το τελευταίο στάδιο της καταμέτρησης στην περίπτωση της ψηφοφορίας μέσω διαδικτύου φέρεται εις πέρας ηλεκτρονικά.

Σε σύγκρισή με άλλες διαδικασίες που γίνονται αποκλειστικά με ηλεκτρονικό τρόπο, για παράδειγμα το ηλεκτρονικό εμπόριο, η ψηφοφορία μέσω διαδικτύου απαιτεί ένα μεγαλύτερο επίπεδο ασφάλειας. Η ψηφοφορία μέσω διαδικτύου απαιτεί ένα πολύπλοκο μοντέλο ασφάλειας επειδή είναι απαραίτητη η μυστικότητα και η ανωνυμία της ψήφου, η οικουμενική επαληθευσιμότητα, καθώς και η προστασία από καταναγκασμό. Αυτά απαιτούν περαιτέρω εξέλιξη και βελτίωση. Ταυτόχρονα, όμως η ταυτοποίηση των ψηφοφόρων και η εξασφάλιση της μοναδικότητας της ψήφου ανά ψηφοφόρο αποτελούν πτυχές που μπορούν να αντιμετωπιστούν με τεχνικές που ήδη χρησιμοποιούνται σε εφαρμογές ηλεκτρονικών συστημάτων πληρωμών όπως οι ψηφιακές υπογραφές και τα ψηφιακά πιστοποιητικά. Δεν είναι λίγοι εκείνοι που θεωρούν πως τα συστήματα και οι υπάρχουσες τεχνολογίες δεν είναι επαρκείς για την αποτελεσματική διεξαγωγή της ηλεκτρονικής ψηφοφορίας, όπως επίσης ότι τα σύγχρονα κράτη δεν είναι σε θέση να αντιμετωπίσουν τα προβλήματα ασφάλειας που προκύπτουν. Επιπρόσθετα, αυτή τη μερίδα ειδημόνων οι οποίοι δεν συμφωνούν με τη χρήση της ψηφοφορίας μέσω διαδικτύου, υπερασπίζονται ότι η υιοθέτηση ενός τέτοιου τύπου ψηφοφορίας θα οδηγούσε στον κοινωνικό αποκλεισμό των λεγόμενων «ψηφιακά αναλφάβητων» πολιτών (Dictson,2000, Philips,2001). Βέβαια, αυτό είναι ένα πρόβλημα το οποίο μπορεί εύκολα να λυθεί με την επιμόρφωση των πολιτών στη χρήση ηλεκτρονικών μέσων και διαδικτύου με έμφαση στην ηλεκτρονική ψηφοφορία. Ωστόσο, η προσφορά της διαδικτυακής ψηφοφορίας προσφέρει πρόσβαση επιτιθέμενους (χάκερ) σε όλο τον πλανήτη. Οι επιτιθέμενοι θα μπορούσαν εύκολα να

παραβιάσουν την ιερότητα του μυστικού ψηφοδελτίου, να τροποποιήσουν τις ψήφους ή ακόμα και να καταστήσουν τη διαδικτυακή εφαρμογή μη διαθέσιμη σε ορισμένους ψηφοφόρους την ημέρα των εκλογών.

1.5.2 Αυτοματοποιημένο σύστημα ψηφοφορίας

Όπως είναι γνωστό και έχει εκφραστεί τόσο από τους πολιτικούς ειδήμονες όσο και από το εκλογικό σώμα, το ιδιωτικό απόρρητο και η απαίτηση ασφάλειας, όλες οι ψηφοφορίες πρέπει να επαληθευτούν και να μετρηθούν με ακρίβεια χωρίς να συμπεριλαμβάνονται στην καταμέτρηση τα ψηφοδέλτια που δεν έχουν συμπληρωθεί σωστά (άκυρα ψηφοδέλτια). Μια μέθοδος είναι η παροχή ασφάλειας στον τόπο ψηφοφορίας με παρατηρητές ψηφοφορίας, δηλαδή η παραδοσιακή καταμέτρηση ψήφων από ανθρώπους. Η παραδοσιακή μέθοδος καταμέτρησης ψήφων αποσκοπεί στην εξασφάλιση της ακρίβειας και της αυθεντικότητας της ψηφοφορίας και των αποτελεσμάτων της ψηφοφορίας. Ωστόσο, αυτή η διαδικασία είναι αργή για τα σημερινά δεδομένα και υπάρχει η πιθανότητα για ανακριβή καταμέτρηση ή και διαφθορά π.χ. με την εγγραφή των ψηφοδελτίων που δεν έχουν συμπληρωθεί σωστά. Το αυτοματοποιημένο σύστημα ψηφοφορίας είναι μια εφεύρεση η οποία αναφέρεται σε συστήματα αυτοματοποιημένων ψηφοφοριών και ειδικότερα σε ένα σύστημα για την επαλήθευση εγγεγραμμένων ψηφοφόρων και τη συλλογή και την ταξινόμηση των ψήφων από μία ή περισσότερες μηχανές ψηφοφορίας. Αυτό το αυτοματοποιημένο σύστημα ψηφοφορίας ξεπερνά πολλά από τα προβλήματα που συσχετίζονται με τις παραδοσιακές μεθόδους ψηφοφορίας, συμπεριλαμβανομένων των προηγούμενων ηλεκτρονικών συστημάτων ψηφοφορίας διατηρώντας παράλληλα όλα τα πλεονεκτήματα των προηγουμένων συστημάτων.

Το αυτοματοποιημένο σύστημα ψηφοφορίας περιλαμβάνει έναν σταθμό εισόδου ψηφοφορίας, ο οποίος ενσωματώνει ένα πρόγραμμα υπολογιστή με ενσωματωμένη συσκευή κατάδειξης με γραφική διεπαφή για τον χρήστη για την εμφάνιση των ψηφοδελτίων ή των προβλημάτων σε μια οθόνη. Ο σταθμός εισόδου στην ψηφοφορία ενσωματώνει όλες τις απαιτούμενες λειτουργίες. Ο προγραμματισμένος σταθμός εισόδου ψηφοφορίας έχει ένα ηλεκτρονικό πληκτρολόγιο ή ένα απλό πληκτρολόγιο για την εμφάνιση και εισαγωγή των υποψηφίων. Επιτρέπει, επίσης την ψηφοφορία για

περισσότερους από έναν υποψήφιους. Επιπλέον, το πρόγραμμα επιτρέπει στους ψηφοφόρους να αλλάξουν την ψήφο τους πριν από τη μετάδοσή της. Το πρόγραμμα που περιέχεται στη συσκευή ψηφοφορίας επιτρέπει την παρακολούθηση του αριθμού των ψήφων που εκπέμπεται από κάθε μονάδα και ο σταθμός εισόδου εμφανίζει την καταμέτρηση.

Το αυτοματοποιημένο σύστημα ψηφοφορίας έχει να παρουσιάσει ποικίλα πλεονεκτήματα. Στα πλεονεκτήματα αυτού του συστήματος περιλαμβάνεται πρώτα, το γεγονός ότι οι σταθμοί εισόδου των ψηφοφοριών μπορούν να προγραμματιστούν από έναν ή περισσότερους εκλογικούς υπαλλήλους ώστε να παρέχουν σε όλους τους σταθμούς με πολλαπλές οθόνες το ίδιο στυλ ψηφοφορίας. Ακόμη, ο ψηφοφόρος μπορεί να επιλέξει τη γλώσσα που επιθυμεί. Ο σταθμός εισόδου ψηφοφορίας ενεργοποιείται με τουλάχιστον έναν κωδικό ενεργοποίησης που εισάγουν οι εκλογικοί εργαζόμενοι για την πρόληψη της απάτης. Μπορεί επίσης να υπάρχει μια μονάδα εκλογών σε επικοινωνία με τον σταθμό ψηφοφορίας για την παροχή πληροφοριών και επαλήθευσης τέτοιων πράξεων, όπως ο κωδικός εξουσιοδότησης ψηφοφόρου και επαλήθευση των δεδομένων εγγραφής των ψηφοφόρων. Αυτή η μονάδα μπορεί επίσης να προγραμματιστεί για να επαληθεύσει την υπογραφή ψηφοφόρων, τα δακτυλικά αποτυπώματα των ψηφοφόρων και μπορεί επίσης να ενημερώνει το ιστορικό των ψηφοφόρων.

Το αυτοματοποιημένο σύστημα ψηφοφορίας έχει την δυνατότητα να περιλαμβάνει είτε μία μόνο συσκευή ψηφοφορίας, η οποία θα εκτελέσει όλες τις λειτουργίες που περιγράφονται παραπάνω είτε να χρησιμοποιεί την ίδια συσκευή ψηφοφορίας ως μονάδα υποδοχής ή ελέγχου έτσι ώστε να μπορούν να ελέγχονται διάφοροι σταθμοί ψηφοφορίας από μία μονάδα. Το σύστημα ψηφοφορίας ελέγχεται από κωδικούς εξουσιοδότησης, οι οποίοι επαληθεύουν την έγκριση των ψηφοφόρων. Ακόμα χρησιμοποιούν εκλογικές κάρτες ασφαλείας για την επαλήθευση και ενεργοποίηση της λειτουργίας του εξοπλισμού του συστήματος. Ο εξοπλισμός δεν μπορεί να λειτουργήσει χωρίς τη χρήση της σωστής κάρτας ασφαλείας η οποία συνήθως παρέχεται σε σφραγισμένους φακέλους από την εκλογική αρχή.

Ένα άλλο πολύ σημαντικό πλεονέκτημα του αυτοματοποιημένου συστήματος ψηφοφορίας έγκειται στο ότι αυτό περιλαμβάνει έναν ή περισσότερους σταθμούς ψηφοφορίας για έλεγχο και ταυτόχρονα σταθμό ψηφοφορίας. Το σύστημα

ψηφοφορίας περιλαμβάνει μια ενσωματωμένη συσκευή με γραφικό περιβάλλον για τον χρήστη με στόχο την εμφάνιση των ψηφοδελτίων. Οι σταθμοί ψηφοφορίας μπορούν να αλληλοσυνδέονται και μάλιστα να λειτουργούν ως ενιαία μονάδα ως πλήρες εκλογικό τμήμα. Το σύστημα ψηφοφορίας παρακολουθεί τον αριθμό των ψήφων και τον εμφανίζει συνεχώς σε ένα σύστημα καταμέτρησης, καθώς εμφανίζει και την πρόθεση του ψηφοφόρου.

Το αυτοματοποιημένο σύστημα ψηφοφορίας παρέχει επίσης ασφάλεια για τον ψηφοφόρο και το σύστημα τόσο εσωτερικά όσο και εξωτερικά. Το εξωτερικό σύστημα ασφαλείας μπορεί να ελέγχεται από τις αρχές ψηφοφορίας ενώ το σύστημα εσωτερικής ασφάλειας λειτουργεί ανεξάρτητα.

Επιπρόσθετα, ένα πλεονέκτημα του αυτοματοποιημένου σύστημα ψηφοφορίας είναι ότι παρέχει πολλαπλές επιλογές ψηφοφορίας σε μία ή περισσότερες μονάδες ψηφοφορίας και παρέχει ένα ηλεκτρονικό πληκτρολόγιο αφής για τους ψηφοφόρους. Το αυτοματοποιημένο σύστημα ψηφοφορίας εκτυπώνει επίσης σε ξεχωριστούς εκτυπωτές τα αποτελέσματα στο χώρο ψηφοφορίας και μεταδίδει το μήνυμα σε μια κεντρική μονάδα συλλογής.

Ένα τελευταίο πλεονέκτημα αυτού του συστήματος που αξίζει να σημειωθεί είναι ότι επιτρέπει στον ψηφοφόρο να ακυρώσει την ψηφοφορία όσες φορές επιθυμεί πριν από τη μετάδοση της στα αποτελέσματα.

Αναφέροντας την ηλεκτρονική ψηφοφορία ας δούμε συνοπτικά την διαδικασία που ακολουθεί ένα τέτοιο σύστημα. Πρώτα είναι ορθό να επισημανθεί ότι, όπως γίνεται αντιληπτό και από τα παραπάνω, πραγματοποιείται σε ένα εκλογικό σημείο για παράδειγμα στο εκλογικό κέντρο(California Internet Voting Task Force,2000). Το επόμενο που πρέπει να αναφερθεί είναι ότι τόσο τα συστήματα - πελάτες (voting system (server)- clients) που χρησιμοποιούν οι ψηφοφόροι για να υποβάλλουν ηλεκτρονικά την ψήφο τους, όσο και το φυσικό περιβάλλον στο οποίο διεξάγεται η ψηφοφορία, επιβλέπονται από εξουσιοδοτημένες οντότητες (π.χ. εκλογικοί αντιπρόσωποι, αστυνομία). Αφού πραγματοποιείται το πρώτο στάδιο, ανάλογα με το είδος του εκλογικού σημείου, ακολουθεί το στάδιο της επικύρωσης – επιβεβαίωσης. Το στάδιο της επικύρωσης είναι δυνατόν να πραγματοποιηθεί είτε με φυσικές διαδικασίες, δηλαδή με έλεγχο απ’ ευθείας από τους εκλογικούς αντιπροσώπους, είτε με ηλεκτρονικές διαδικασίες όπως χρήση κωδικού PIN. Αφού διεκπεραιωθεί το στάδιο

της επικύρωσης (επιβεβαίωσης της ταυτότητας του ψηφοφόρου), ακολουθεί το στάδιο της υποβολής της ψήφου. Η υποβολή της ψήφου πραγματοποιείται από τον κάθε ψηφοφόρο ηλεκτρονικά είτε σε προσωπικούς υπολογιστές είτε σε ειδικές συσκευές με οθόνες αφής (όπως οι συσκευές άμεσης καταμέτρησης – DRE, που χρησιμοποιούνται ευρέως στις Η.Π.Α) (Caltec/Mit,2001). Μετά την υποβολή της ψήφου από τον ψηφοφόρο, οι ψήφοι αποθηκεύονται τοπικά σε αποσπώμενες περιφερειακές μονάδες, έτοιμοι για το επόμενο στάδιο.

Όπως έχει αναφερθεί παραπάνω, το επόμενο στάδιο είναι το στάδιο της καταμέτρησης, το οποίο αποτελεί και το τελικό στάδιο της ηλεκτρονικής ψηφοφορίας. Στην ηλεκτρονική ψηφοφορία το τελευταίο στάδιο δηλαδή η καταμέτρηση των ψήφων γίνεται ηλεκτρονικά. Εξάλλου, ένας από τους βασικούς πυλώνες της φιλοσοφίας της ηλεκτρονικής ψηφοφορίας είναι η καταμέτρηση των ψήφων χωρίς ανθρώπινη παρέμβαση. Η ηλεκτρονική καταμέτρηση των ψήφων πραγματοποιείται τοπικά στο εκλογικό κέντρο ή αποστέλλονται στον κεντρικό εξυπηρετητή (server) των εκλογών για τον υπολογισμό των συγκεντρωτικών αποτελεσμάτων. Η μεταφορά στον κεντρικό server μπορεί να γίνει επίσης ηλεκτρονικά, με «ασφαλείς» συνδέσεις. Οι εν λόγω ασφαλείς συνδέσεις μπορούν να πραγματοποιηθούν με γραμμές οπτικών ινών ή μέσω Internet με τεχνικές IPSEC - Εικονικά Ιδιωτικά Δίκτυα VPNs. Επίσης, για την ασφαλή μεταφορά έχει προταθεί η χρήση των δικτύων ATM την ημέρα των εκλογών διότι τα δίκτυα αυτά έχουν ορισμένα επιθυμητά χαρακτηριστικά ασφάλειας όπως η μυστικότητα του καναλιού επικοινωνίας, ο αξιόπιστος εξοπλισμός, τα ανθεκτικά τερματικά και το υψηλό ποσοστό διείσδυσης. Όμως, δεν λείπει ο διχασμός των απόψεων όσον αφορά την καταλληλόλητα τους για τη διενέργεια ηλεκτρονικών εκλογών (Jefferson,2000).

Παρακάτω δίνονται ορισμένα σχέδια του αυτοματοποιημένου συστήματος ψηφοφορίας. Επάνω στα σχέδια δίνονται επεξηγήσεις του συστήματος με απλά λόγια, ώστε να γίνεται εύκολα αντιληπτή η λειτουργία του.

Η χρήση των συστημάτων ψηφοφορίας εισάχθηκε για πρώτη φορά το 1960 όταν κυκλοφόρησαν οι punched card. Πρόκειται για ένα κομμάτι άκαμπτου χαρτιού το οποίο μπορεί να χρησιμοποιηθεί για τη συγκράτηση ψηφιακών δεδομένων που αντιπροσωπεύονται από την παρουσία ή την απουσία οπών σε προκαθορισμένες

θέσεις. Το 1964 έγινε η πρώτη διαδεδομένη χρήση τους στις προεδρικές εκλογές των ΗΠΑ, όπου 7 κομητείες χρησιμοποίησαν αυτή τη μέθοδο.

Σήμερα, σε πολλές χώρες προτιμάται η ηλεκτρονική ψηφοφορία η οποία διεξάγεται με μηχανήματα. Επομένως, τα μηχανήματα και τα ηλεκτρονικά συστήματα ψηφοφορίας και καταμέτρησης ψήφων θα πρέπει να εξασφαλίζουν την ίδια αυθεντικότητα και ακρίβεια.

Έχουν αναπτυχθεί πολλά συστήματα για ηλεκτρονική ψηφοφορία. Όλα τα συστήματα έχουν καταφέρει τους επιστήμονες να επικεντρωθούν σε 2 ερωτήματα : 1) είναι αρκετά ασφαλείς; 2) προσφέρουν ιδιωτικότητα – εμπιστευτικότητα. Τέλος ένα e-voting σύστημα είναι πολύ σημαντικό να είναι πλήρως λειτουργικό και να γίνει αποδεκτό από την κοινωνία.

1.5.3 DS200

Ένα δημοφιλές μηχάνημα ψηφοφορίας είναι το DS200 το οποίο επεξεργάζεται τους ψήφους οι οποίοι είναι σε χάρτινη μορφή μονής ή διπλής όψεως. Το μηχάνημα αυτό έχει τη δυνατότητα καταμέτρησης ψήφων. Αφού ολοκληρώσει την καταμέτρηση ψήφων προχωρά στη διεξαγωγή αποτελεσμάτων.

Το DS200 δεν έχει σύνδεση με το διαδίκτυο, αλλά μπορεί να μεταδώσει τα αποτελέσματα μέσω ενός modem. Διαθέτει μια οθόνη αφής LCD 12 ιντσών, η οποία χρησιμοποιείται για να ενημερώνει τους χρήστες για την κατάσταση του μηχανήματος και της ψηφοφορίας, όπως μια προειδοποίηση υπερτιμήσεων.

Εικόνα 2 Μηχάνημα ψηφοφορίας DS200

Με το τέλος της ψηφοφορίας, δηλαδή των εκλογών, το DS200 εκτυπώνει τα αρχεία καταγραφής ψηφοφόρων. Το DS200 αποθηκεύει ψηφιοποιημένες εικόνες όλων των ψηφοδελτίων που σαρώθηκαν. Αυτό επιτρέπει την επεξεργασία των ψηφοδελτίων που είχαν κάποιο πρόβλημα κατά την συμπλήρωση τους με αποτέλεσμα όλα τα ψηφοδέλτια να μην χρήζουν επανεξέτασης παρά μόνο σε περιπτώσεις καταγραφής ή ελέγχου. Το χαρτί με τα αποτελέσματα λαμβάνεται από την εφορευτική επιτροπή. Δεν υπάρχει καμία ανθρώπινη παρέμβαση στη διαδικασία καταμέτρησης ψήφων.
Το DS200 παρουσιάζει ορισμένα μειονεκτήματα. Ένα μειονέκτημα είναι πως σε περίπτωση κακοπροαίρετων ή διεφθαρμένων υπαλλήλων, οι εργαζόμενοι μπορούν να στείλουν μέσω του μόντεμ το πρωτότυπο ψηφοδέλτιο χωρίς να αποθηκευτεί. Η πληροφορία που ανταλλάσσεται είναι κρυπτογραφημένη και από τον αποστολέα αλλά και από τον παραλήπτη, παρόλα αυτά ένας κακόβουλος που διαθέτει ένα Stingray θα μπορούσε να παρακολουθεί και να υποκλέπτει την ανταλλαγή των δεδομένων. Αν και οι κατασκευαστές υποστηρίζουν ότι αυτό είναι εξαιρετικά σπάνιο να συμβεί. Ωστόσο, η Νέα Υόρκη, το Μέριλαντ, η Βιρτζίνια και η Αλαμπάμα απαγόρευσαν τη χρήση μόντεμ για τη μετάδοση των αποτελεσμάτων των εκλογών.

1.5.4 Ballots

Στις ΗΠΑ υπάρχουν 13 πολιτείες που περιέχουν κομητείες όπου τα μηχανήματα ψηφοφορίας που χρησιμοποιούν δεν κάνουν χρήση ψηφοδέλτια χάρτινης μορφής, αλλά κάποιες μηχανές ψηφοφορίας με οθόνη αφής, τα γνωστά ως Ballots. Αυτά είναι τα πιο ευπαθή μηχανήματα, καθώς οι μηχανές αφής χωρίς χαρτί είναι ανασφαλείς. Σε αυτά τα μηχανήματα ο ψηφοφόρος μπορεί να αγγίξει το όνομα ενός υποψηφίου. Όμως λόγω διάφορων ανωμαλιών το μηχάνημα μπορεί να καταγράψει διαφορετική ψήφο. Επομένως, δεν είναι σίγουρο αν το μηχάνημα παράγει έγκυρο αντίγραφο και δεν είναι εφικτό να αποκλειστεί η πιθανότητα ότι δεν γίνονται λάθη ή δεν ψηφίζονται κατά λάθος διαφορετικοί υποψήφιοι από αυτούς που στην πραγματικότητα ψηφίζουν οι ψηφοφόροι. Τέτοιου είδους λάθη ενδέχεται να συμβούν από το μηχάνημα ή με την εισαγωγή κακόβουλου λογισμικού. Ένα γνωστό παράδειγμα στην ιστορία της ηλεκτρονικής ψηφοφορίας αποτελεί το μηχάνημα ψηφοφορίας της περιφέρειας Venango της Πενσυλβάνια όπου το μηχάνημα αντικατέστησε τον υποψήφιο τον οποίο ψήφισε ο ψηφοφόρος με έναν άλλο υποψήφιο.

Εικόνα 3 Ballot

Γεγονός που χρήζει ανησυχίας είναι ότι δεν υπάρχει κανένας τρόπος να επιβεβαιωθεί αν η ψηφοφορία ήταν έγκυρη ή όχι. Χωρίς έντυπη μορφή της ψήφου, ώστε να υπάρχει η επιβεβαίωση της, το μηχάνημα θα μπορούσε να διαγράψει μέρος ή και ολόκληρο το ψηφοδέλτιο ενώ ταυτόχρονα θα ενημερώνει τον ψηφοφόρο πως η ψήφος του καταχωρήθηκε επιτυχώς. Μετά την διαρροή αυτών των πληροφοριών το 2017, 22 σταθμοί ψηφοφορίας στην Βιρτζίνια απέσυραν τις μηχανές με τις οθόνες αφής και

προχώρησαν στην εισαγωγή των χάρτινων ψηφοδελτίων, γιατί θεώρησαν ότι αν και είναι πιο χρονοβόρα, είναι η πιο ασφαλής μορφή ψηφοφορίας.

2

Ασφάλεια στην ηλεκτρονική ψηφοφορία

2.1 Γιατί διαφέρει η ηλεκτρονική Ψηφοφορία

Η διεξαγωγή ηλεκτρονικής εκλογής μέσω συστήματος REV είναι ένα πολύπλοκο ζήτημα που θέτει πολλές απαιτήσεις ασφαλείας εξαιρώντας εκείνες που είναι κοινές σε πολλές άλλες διαδικτυακές εφαρμογές. Οι απαιτήσεις ασφαλείας ειδικά για την ηλεκτρονική ψηφοφορία (π.χ. το απόρρητο των ψηφοφόρων) δεν μπορούν να διασφαλιστούν μέσω γενικών μέτρων ασφαλείας, αλλά χρειάζονται ειδικά μέτρα. Επιπλέον, δεδομένης της ευαίσθητης φύσης της ψηφοφορίας (δηλαδή εκείνοι που είναι υπεύθυνοι για τη λειτουργία του συστήματος είναι επίσης ψηφοφόροι ή / και υποψήφιοι και έχουν συμφέρον για το αποτέλεσμα των εκλογών), το σύστημα πρέπει να προστατεύεται τόσο από εξωτερικές όσο και από εσωτερικές επιθέσεις. Συνοπτικά, οι κύριες πτυχές που διαφοροποιούν την ασφάλεια της ηλεκτρονικής ψηφοφορίας από εκείνες άλλων κοινών διαδικτυακών εφαρμογών είναι:

- Η ηλεκτρονική ψηφοφορία απαιτεί ένα σύνολο προηγμένων απαιτήσεων ασφαλείας
- Οποιοδήποτε σύστημα ηλεκτρονικής ψηφοφορίας πρέπει να προστατεύεται τόσο από επιθέσεις εξωτερικού παράγοντα όσο και εσωτερικού

2.2 Πρωτόκολλα κρυπτογραφίας στο επίπεδο της εφαρμογής

Λόγω των παραπάνω προβλημάτων, ένα σύστημα REV θα ήταν συνετό να αποτελείται από μία εφαρμογή που να περιέχει ένα πρωτόκολλο κρυπτογραφικής ψηφοφορίας. Ένα τέτοιο πρωτόκολλο λειτουργεί ως κεντρικός άξονας για τα μέτρα ασφαλείας που εστιάζουν ειδικά στην ηλεκτρονική ψηφοφορία. Επειδή το πρωτόκολλο βρίσκεται στο επίπεδο της εφαρμογής, μπορεί να κατανοήσει πλήρως και να καλύψει τις ανάγκες της εφαρμογής της ηλεκτρονικής ψηφοφορίας. Οποιοδήποτε μέτρο ασφαλείας κάτω από το επίπεδο εφαρμογής, όπως κρυπτογραφία σε transport-level, δεν θα μπορούσε να επιλύσει τα προβλήματα ασφαλείας που αφορούν ειδικά την ηλεκτρονική ψηφοφορία. Ένα πρωτόκολλο κρυπτογραφικής ψηφοφορίας στο επίπεδο της εφαρμογής των συστημάτων, έχει σχεδιαστεί για να προστατεύει τα συμφέροντα όλων των κομμάτων που εμπλέκονται στις εκλογές, ακόμη και όταν έρχονται αντιμέτωποι με τις κακόβουλες πράξεις άλλων κομμάτων ή από εσωτερικές επιθέσεις. Επίσης καθορίζει τα βήματα και

τις ενέργειες που πρέπει να ακολουθούνται για την ηλεκτρονική ψηφοφορία, τόσο από τη συσκευή του ψηφοφόρου όσο και από τον αντίστοιχο διακομιστή ψήφων. Καθορίζει ακόμη, τις κρυπτογραφικές ενέργειες που πρέπει να γίνουν για να ανοίξει μία ψηφιακή κάλπη για να καταγράψουν τα ψηφοδέλτια και επίσης για να επαληθεύσουν τα αποτελέσματα των εκλογών. Φυσικά, ένα κρυπτογραφικό πρωτόκολλο ψηφοφορίας θα πρέπει να συμπληρώνεται με ψηφιακά μέτρα ασφαλείας όπως τείχη προστασίας, κρυπτογράφηση δεδομένων, προστασία από επιθέσεις DDoS κ.λπ.
Παρ 'όλα αυτά, το πρωτόκολλο ψηφοφορίας είναι αναμφισβήτητα το πιο ουσιαστικό τεχνολογικό στοιχείο που επιτρέπει στην ψηφοφορία μέσω ενός δικτύου επικοινωνιών να επιτύχει τα ίδια επίπεδα προστασίας με τα συμβατικά συστήματα ψηφοφορίας. Ένα πρωτόκολλο κρυπτογραφικής ψηφοφορίας είναι επομένως ουσιαστικό μέρος οποιουδήποτε συστήματος REV.

2.3 Απαιτήσεις ασφάλειας που αντιμετωπίζονται με τα πρωτόκολλα ψηφοφορίας

Έχουν γίνει πολλές έρευνες για πρωτόκολλα κρυπτογραφικής ψηφοφορίας τις τελευταίες δεκαετίες, με αποτέλεσμα να υπάρχουν πολλές παραλλαγές των πρωτοκόλλων ψηφοφορίας. Παρά την ποικιλία, τα περισσότερα από τα πρωτόκολλα τείνουν να πληρούν το ίδιο σύνολο απαιτήσεων ασφαλείας. Η ιδιωτικότητα των ψηφοφόρων θεωρείται συχνά ως η κεντρική απαίτηση ασφάλειας. Κανένας (ούτε καν οι εκλογικές αρχές ή οι διαχειριστές συστήματος που είναι υπεύθυνοι για τους διακομιστές) δεν πρέπει να είναι σε θέση υπό κανονικές συνθήκες να συσχετίσουν τις ψήφους με τους ψηφοφόρους. Ωστόσο, αυτό έρχεται σε αντίθεση με την υποχρέωση επαρκούς ταυτοποίησης των ψηφοφόρων χρησιμοποιώντας ισχυρά μέσα ελέγχου ταυτοποίησης προκειμένου να μην επιτρέπεται η ψήφος των μη αυθεντικοποιημένων ψηφοφόρων και να αποτραπεί η ψήφος των έγκυρων ψηφοφόρων να προβεί σε οριστική υποβολή περισσότερες από μία φορές. Η ακρίβεια των εκλογικών αποτελεσμάτων είναι επίσης απαραίτητη. Πρέπει να είναι αδύνατο να προστεθούν άκυρα ψηφοδέλτια (π.χ. ψευδείς ψήφους αντί της αποχής ψηφοφόρων) ή να διαγραφούν ή να τροποποιηθούν έγκυρα ψηφοδέλτια. Μια άλλη απαίτηση που αντιμετωπίζεται από τα πρωτόκολλα ψηφοφορίας είναι να διατηρούνται μυστικά τα αποτελέσματα μέχρι την ολοκλήρωση των εκλογών (εκτός εάν απαιτείται από τη συγκεκριμένη φύση των εκλογών). Ο στόχος αυτού του απορρήτου είναι να αποφευχθεί η διαρροή εκλογικών αποτελεσμάτων πριν την ολοκλήρωση της ψηφοφορίας.
Επίσης, μια άλλη σημαντική απαίτηση ασφάλειας που λαμβάνεται υπόψιν από τα πρωτόκολλα ψηφοφορίας είναι η δυνατότητα επαλήθευσης. Για να αποκτήσουν την εμπιστοσύνη των ψηφοφόρων στο σύστημα, είναι σημαντικό να τους δοθεί η δυνατότητα να επαληθεύουν ότι οι ψήφοι τους έχουν αντιμετωπιστεί σωστά. Η μέθοδος επαλήθευσης δεν πρέπει να αφήνει περιθώρια για αμφιβολίες ως προς τη μεταχείριση της ψηφοφορίας. Επιπλέον, σε περίπτωση εντοπισμού οποιουδήποτε

προβλήματος, ένας ψηφοφόρος πρέπει να είναι σε θέση να αποδείξει, χωρίς φόβο να διακυβεύσει το απόρρητό του, ότι η ψήφος του δεν αντιμετωπίστηκε σωστά. Ταυτόχρονα, ένα πρωτόκολλο ψηφοφορίας πρέπει να διασφαλίσει ότι η ικανότητα επαλήθευσης της ψηφοφορίας κάποιου δεν εκθέτει τους ψηφοφόρους στον εξαναγκασμό τρίτων και δεν τους επιτρέπει να πουλήσουν τις ψήφους τους.
Οι απαιτήσεις ασφάλειας:

- Απόρρητο: Αδύνατο να συσχετιστούν οι ψήφοι με τους αντίστοιχους ψηφοφόρους.
- Ταυτοποίηση : Για να διασφαλιστεί ότι μόνο οι ψηφοφόροι που έχουν ταυτοποιηθεί μπορούν να ψηφίσουν και προσμετράτε μόνο μία ψήφος ανά ψηφοφόρο (οριστική υποβολή)
- Ακρίβεια: Οι έγκυρες ψήφοι δεν μπορούν να αφαιρεθούν ή να τροποποιηθούν. Δεν μπορούν να προστεθούν άκυρες ψήφοι.
- Απόρρητο των αποτελεσμάτων: Όλα τα αποτελέσματα διατηρούνται μυστικά μέχρι την ολοκλήρωση των εκλογών.
- Το σύστημα δεν πρέπει να επιτρέπει την πώληση ψήφων ή τον εξαναγκασμό ψηφοφόρων.
- Επαληθευσιμότητα: Οι ψηφοφόροι πρέπει να είναι σίγουροι για τη σωστή μεταχείριση των ψήφων τους και να διαθέτουν μέσα για να αποδείξουν αδιαμφισβήτητα οποιαδήποτε απάτη.

2.4 Πρωτόκολλα κρυπτογραφίας για την ηλεκτρονική Ψηφοφορία

Mix-Net:

Ένα σύνολο διακομιστών που συνεργάζονται για να παρέχουν ανωνυμία στις επικοινωνίες. Κάθε διακομιστής στο mix-net λαμβάνει ένα σύνολο μηνυμάτων και τα προωθεί με μυστική τυχαία σειρά στον επόμενο διακομιστή mix. Στην ηλεκτρονική ψηφοφορία, τα mix nets χρησιμοποιούνται συνήθως για να παρέχουν ανωνυμία κατά την υποβολή ψήφων ή τη διαδικασία αποκρυπτογράφησης. Ο David Chaum ήταν ο πρώτος που δημοσίευσε την ιδέα των mixnets το 1979 [3]

Homomorphic Encryption:

Το 1986 ο Benaloh ξεκίνησε μια δεύτερη ομάδα πρωτοκόλλων κρυπτογραφικής ψηφοφορίας με βάση τεχνικές ομομορφικής κρυπτογράφησης[4]. Αυτά τα πρωτόκολλα ψηφοφορίας απέφυγαν τη χρήση καναλιών ανωνυμοποίησης χωρίζοντας τα ψηφοδέλτια σε διάφορα κομμάτια και ρίχνοντας κάθε κομμάτι σε ξεχωριστή κάλπη.

Μετά το τέλος της ψηφοφορίας μαζεύονται όλοι οι ψήφοι για την διεξαγωγή των αποτελεσμάτων (υπήρχαν κρυπτογραφικοί μηχανισμοί για τη διασφάλιση της ακρίβειας του τελικού αποτελέσματος). Αντιπροσωπευτικά πρωτόκολλα ψηφοφορίας με βάση τα ομομορφικά έχουν προταθεί από τους Sako και Kilian[5], και από τους Cramer. [6,7]

Τα πρωτόκολλα ψηφοφορίας που βασίζονται σε ομομορφική κρυπτογραφία απαιτούν πολύ μεγαλύτερη υπολογιστική ισχύ από τα πρωτόκολλα ψηφοφορίας με mixnets(τόσο στον πελάτη όσο και στην πλευρά του διακομιστή). Αυτή η ανάγκη αποτρέπει αποτελεσματικά την κατασκευή ομοφορικών συστημάτων ψηφοφορίας για την ψηφοφορία.

Untappable Κανάλια

Μια φυσική συσκευή με την οποία μια οντότητα Α μπορεί να στείλει ένα μήνυμα σε άλλη οντότητα Β, διατηρώντας το μήνυμα απόλυτα μυστικό σε όλες τις άλλες οντότητες

Άλλα πρωτόκολλα

Υπάρχουν ορισμένα πρωτόκολλα ψηφοφορίας που χρησιμοποιούν απλούστερες μεθόδους για να διασφαλίσουν τις επιθυμητές απαιτήσεις ασφαλείας. Αυτά τα πρωτόκολλα, όμως στις επιθέσεις είναι περισσότερο ευάλωτα και οι επιτιθέμενοι ολοκληρώνουν την διαδικασία με επιτυχία με λιγότερη προσπάθεια ή καταφέρνουν να αποκτήσουν μειωμένα δικαιώματα συγκριτικά με τα άλλα πρωτόκολλα.

Μεταξύ των μεθόδων που χρησιμοποιούνται για την ασφάλεια των εφαρμογών της ηλεκτρονικής ψηφοφορίας μία σημαντική μέθοδος είναι και ο διαχωρισμός της επαλήθευσης της ταυτότητας και αυθεντικοποίησης των ψηφοφόρων από την καταμέτρηση των ψηφοδελτίων ως δυο διαφορετικές διαδικασίες. Τα πρωτόκολλα που βασίζονται στην συγκεκριμένη λογική καλύπτουν ορισμένες από τις απαιτήσεις ασφάλειας της ηλεκτρονικής ψηφοφορίας με την προϋπόθεση πως δύο υπηρεσίες δεν συνεργάζονται, και ότι ορισμένα μέρη του συστήματος είναι απολύτως αξιόπιστα.[8] Σε αυτού του είδους τα πρωτόκολλα η ακρίβεια των εκλογικών αποτελεσμάτων μπορεί να διασφαλιστεί μόνο αν έχουμε εμπιστοσύνη στον οργανισμό που είναι υπεύθυνος για την καταμέτρηση των ψηφοδελτίων. Δυστυχώς δεν διασφαλίζονται περαιτέρω απαιτήσεις ασφαλείας, όπως η ικανότητα των ψηφοφόρων να επαληθεύουν τα αποτελέσματα και να αντιτίθενται δημόσια στο αποτέλεσμα

2.4 Κρυπτοσυστήματα για την ηλεκτρονική Ψηφοφορία

Threshold (κατώφλι) Cryptosystem

Η κρυπτογραφία threshold (t, n) είναι ένα σύστημα για τη διανομή μυστικών κλειδιών ή λειτουργιών ενός κρυπτοσυστήματος μεταξύ n συμβαλλομένων μερών, προκειμένου να αφαιρεθεί ένα μόνο σημείο αποτυχίας. Η απαιτούμενη εμπιστοσύνη στην κρυπτογραφική υπηρεσία κατανέμεται μεταξύ της ομάδας αρχών.
Ο στόχος είναι να επιτρέψουμε σε οποιοδήποτε υποσύνολο περισσότερων από t συμβαλλόμενων μερών να ανακατασκευάσουν από κοινού ένα μυστικό και να εκτελέσουν τον υπολογισμό διατηρώντας παράλληλα την ασφάλεια ακόμη και παρουσία ενός ενεργού

Homomorphic Cryptosystem:

Ένα σύστημα όπου είναι δυνατό να δημιουργηθεί μια σχέση μεταξύ μιας συνάρτησης των κρυπτογραφημένων κειμένων δύο μηνυμάτων m1, m2 και του κρυπτογραφήματος μιας άλλης λειτουργίας των καθαρών μηνυμάτων. Για την ηλεκτρονική ψηφοφορία η πιο ενδιαφέρουσα ομομορφική ιδιότητα είναι η ιδιότητα πρόσθετου: υπάρχει μια συνάρτηση f που εφαρμόζεται στα κρυπτογραφήματα των μηνυμάτων m1, m2 έχει ως αποτέλεσμα το κρυπτογραφημένο άθροισμα των μηνυμάτων m1 και m2, f (C (m1) C (m2) = C (m1 + m2) Τα ομόμορφα κρυπτοσυστήματα, με την πρόσθετη ομομορφική ιδιότητα, μπορούν να χρησιμοποιηθούν για την αποκρυπτογράφηση του τελικού αριθμού χωρίς να αποκρυπτογραφήσουν τις ψήφους, παρέχοντας έτσι περισσότερες εγγυήσεις ανωνυμίας ψήφων.

3.

Ευπάθειες

Καθώς τα συστήματα της ηλεκτρονικής ψηφοφορίας αποτελούν ηλεκτρονικά συστήματα είναι λογικό και επόμενο από την φύση τους να έχουν «κενά ασφαλείας» τα οποία μπορούν να χρησιμοποιηθούν είτε κατά λάθος κάποιες φορές είτε σκόπιμα κάποιες άλλες, με αποτέλεσμα προκαλέσουν μεγάλες ζημιές στο σύστημα.
Αυτά τα κενά θα μπορούσαν να είναι:

1. Η διαφορά μεταξύ των προσδοκιών για το υλικό και το λογισμικό και ποια απόδοση μπορεί να επιτευχθεί.
2. Η διαφορά μεταξύ των κοινωνικών πολιτικών (νόμοι, κώδικες δεοντολογίας) και των πολιτικών υπολογιστών (διαδικασίες, λειτουργικότητα).
3. Η πιθανότητα κατάχρησης, λόγω του χάσματος μεταξύ των κοινωνικο-πολιτικών και της ανθρώπινης συμπεριφοράς.

3.1 Κριτήρια Σχεδιασμού

Τα πλήρως μηχανογραφημένα συστήματα ψηφοφορίας χρησιμοποιούν συνήθως επεξεργαστές για όλες τις πτυχές των εκλογών, όπως: προετοιμασία ψηφοφορίας, ψηφοφορία και καταγραφή, πίνακα για την απεικόνιση των αποτελεσμάτων και αναφορά αποτελεσμάτων. Τα υβριδικά συστήματα μπορεί να περιλαμβάνουν μη μηχανογραφημένα εξαρτήματα, όπως τα ψηφοδέλτια που παρασκευάζονται με την χρήση ενός εκτυπωτή.
Οι σχεδιαστικές σκέψεις πρέπει να εστιάζονται στην εξάλειψη ή τον περιορισμό των τεχνολογικών κενών ασφαλείας. Τα γενικά κριτήρια για τις ηλεκτρονικές πτυχές των εκλογικών συστημάτων θα μπορούσαν να είναι τα παρακάτω:

- Ακεραιότητα συστήματος: Στην ιδανική περίπτωση, οι αλλαγές συστήματος πρέπει να απαγορεύονται σε όλα τα ενεργά στάδια της εκλογικής διαδικασίας, ακόμα και από διαδικασίες που τρέχουν αυτόματα από το σύστημα, όπως ένα cron job. Το βασικότερο στοιχείο όμως είναι το σύστημα να παράγει σωστά αποτελέσματα μετά το πέρας της καταμέτρησης
- Ακεραιότητα και αξιοπιστία δεδομένων: Όλα τα δεδομένα που εμπλέκονται στην εισαγωγή και κατάθεση ψήφων πρέπει να είναι αμετάβλητα. Οι ψήφοι πρέπει να καταγράφονται σωστά
- Ανωνυμία ψηφοφορίας και εμπιστευτικότητα δεδομένων: Οι μετρήσεις των ψήφων πρέπει να προστατεύονται από την ανάγνωση εξωτερικών παραγόντων κατά τη διαδικασία ψηφοφορίας. Οποιαδήποτε σχέση μεταξύ των καταγεγραμμένων ψήφων και της ταυτότητας του ψηφοφόρου πρέπει να είναι εντελώς άγνωστη στα συστήματα ψηφοφορίας

- Έλεγχος ταυτότητας χειριστή: Όλα τα άτομα που έχουν εξουσιοδότηση για τη διεξαγωγή εκλογών, λογικό και επόμενο είναι να κατέχουν πρόσβαση στους μηχανισμούς ελέγχου ταυτότητας. Επομένως, συνετό και κάθε τι άλλο από πρέπον είναι να μην μένουν σταθεροί οι κωδικοί ασφαλείας και να αλλάζουν το λιγότερο κάθε 3 μήνες
- Εμπιστοσύνη στο Σύστημα: Όλες οι εσωτερικές λειτουργίες πρέπει να παρακολουθούνται, χωρίς να παραβιάζεται η εμπιστευτικότητα των ψηφοφόρων. Οποιαδήποτε απόπειρα και επιτυχημένες αλλαγές στην κατάσταση διαμόρφωσης πρέπει να γίνονται γνωστές. Η παρακολούθηση των κινήσεων στο σύστημα δεν πρέπει να αμελείται. Όλες οι κινήσεις των χρηστών πρέπει να καταγράφονται και να μένουν για μεγάλο χρονικό διάστημα στα αρχεία καταγραφής του συστήματος και τα αρχεία αυτά να κρατούνται χωρίς να διαγράφονται για λόγους ασφάλειας και επαληθευσιμότητας
- Ελεύθερο Λογισμικό: Το λογισμικό, το υλικό και οτιδήποτε χρησιμοποιεί το σύστημα ψηφοφορίας πρέπει να είναι διαθέσιμο στο κοινό
- Λειτουργικότητα: Το σύστημα πρέπει να είναι διαθέσιμο για χρήση όποτε αναμένεται να είναι λειτουργικό και πρέπει να προστατεύεται από τυχαίες και κακόβουλες DoS επιθέσεις.

Τα παραπάνω κριτήρια είναι ορισμένα από τα σημαντικά κριτήρια που θα έπρεπε να τηρεί ένα ηλεκτρονικό σύστημα και κατ' επέκταση ένα σύστημα ηλεκτρονικής ψηφοφορίας

3.2 Ευπάθειες συστημάτων ηλεκτρονικής ψηφοφορίας

Η ψηφοφορία μέσω διαδικτύου θέτει πολλούς κινδύνους. Όπως η εγκυρότητα της ψήφου του ψηφοφόρου, η αυθεντικοποίηση του ψηφοφόρου στο σύστημα και οι απειλές που υπονομεύουν στο διαδίκτυο όπως «virus(Ιοι)» ή «Trojan». Μερικά προβλήματα της διαδικτυακής ψηφοφορίας είναι :

- Η εγκυρότητα του ψηφοφόρου(Αυθεντικοποίηση)
- Η ακεραιότητα της ψήφου (Integrity)
- Αξιοπιστία αποθήκευσης και μετάδοσης ψήφου.
- Πρόληψη διπλασιασμού της ψήφου.

Βάσεις Δεδομένων

Μια ευπάθεια είναι οι κακόβουλοι να αποκτούν πρόσβαση στις βάσεις δεδομένων των συστημάτων ηλεκτρονικής ψηφοφορίας, όπως έγινε και στο Ιλινόις. Θεωρητικά, η πληροφορία που αποθηκεύεται στην βάση δεδομένων μπορεί να τροποποιηθεί ή και

να κλαπεί. Για να αποφευχθεί αυτό πρέπει η πρόσβαση στην βάση δεδομένων να είναι περιορισμένη, αλλά και οι κωδικοί πρέπει να είναι ασφαλείς (πάνω από 8 χαρακτήρες , να περιέχουν αριθμούς ,κεφαλαία και σύμβολα) και να αλλάζουν συχνά , ώστε να μπερδεύουν τους επιτιθέμενους.

Μηχανήματα Ψηφοφορίας

Stingrays

Μετά τις βάσεις δεδομένων το επόμενο ευπαθές σύστημα είναι τα μηχανήματα ηλεκτρονικής και διαδικτυακής ψηφοφορίας. Τα δεδομένα των ψήφων στέλνονται από το μηχάνημα ψηφοφορίας σε έναν κεντρικό υπολογιστή.

Επομένως, οι κακόβουλοι που βρίσκονται κοντά σε εκλογικά κέντρα και γραφεία εκλογών θα μπορούσαν ενδεχομένως να εισέλθουν στις μηχανές, προκαλώντας τη σύνδεση των μόντεμ της μηχανής ψηφοφορίας με τις κακόβουλες συσκευές που ελέγχουν. Αυτές οι συσκευές, γνωστές ως stingrays, μιμούνται ένα νόμιμο πύργο κινητής τηλεφωνίας (που επικοινωνούν τα μηχανήματα ψηφοφορίας για να επικοινωνήσουν τα αποτελέσματα) για να αναγκάσουν τις συσκευές στην περιοχή να συνδεθούν με αυτές. Αφού συνδεθεί με μια μηχανή ψηφοφορίας που μεταδίδει τα αποτελέσματα ή με τη μηχανή τυποποίησης που τις λαμβάνει, ένας εξειδικευμένος κακόβουλος θα μπορούσε ενδεχομένως να μεταβάλει το λογισμικό ψηφοφορίας και το λογισμικό καταγραφής ή να τροποποιήσει τα επίσημα αποτελέσματα. Έχοντας ταυτόχρονα την δυνατότητα να διαγράψει αποδεικτικά στοιχεία αυτής της δραστηριότητας ώστε να μην τον αναγνωρίσουν.

Στην Ουάσιγκτον , το Τμήμα Εσωτερικής Ασφάλειας αποκάλυψε ότι ανακαλύφθηκαν αρκετές Stingrays συσκευές, χωρίς να γνωρίζουν ποιος τις χειρίζεται.

4

Επιθέσεις σε συστήματα ηλεκτρονικής ψηφοφορίας

4.1 Πιθανές Επιθέσεις σε μηχανήματα του E-Voting

4.1.1 Συστήματα εγγραφής ψηφοφόρων

Τα μηχανήματα ψηφοφορίας δεν είναι συνδεδεμένα στο Διαδίκτυο και επομένως δεν είναι προσβάσιμα από εξωτερικούς εισβολείς σε απόσταση στις περισσότερες περιπτώσεις. Αλλά το ίδιο δεν ισχύει για τα συστήματα που χρησιμοποιούν οι πολίτες για να εγγραφούν για την ψηφοφορία στο Διαδίκτυο.

Οι ευπάθειες ασφαλείας που έχουν τέτοια συστήματα μπορούν να παρέχουν πρόσβαση και την δυνατότητα να αξιοποιηθούν εξ αποστάσεως μέσω του Διαδικτύου. Ωστόσο, οι πιθανότητες τέτοιων παρεμβολών να επηρεάσουν κατά κάποιο τρόπο τα εκλογικά αποτελέσματα είναι ελάχιστες.

4.1.2 Εγκατάσταση κακόβουλου λογισμικού

Παρόλο που τα μηχανήματα ψηφοφορίας δεν είναι σχεδόν ποτέ άμεσα συνδεδεμένα στο Διαδίκτυο, πρέπει να μπορούν να λαμβάνουν ηλεκτρονικά αρχεία ώστε να μπορούν να γνωρίζουν ποιοι υποψήφιοι συμμετέχουν στην ψηφοφορία. Συνήθως, οι αξιωματούχοι των εκλογών το κάνουν προετοιμάζοντας τα κατάλληλα αρχεία ψηφοφορίας σε ξεχωριστό σύστημα και στη συνέχεια τα μεταφέρουν στο σύστημα ψηφοφορίας μέσω κάρτας μνήμης ή κάποιου είδους flash drive.

Πολλά μηχανήματα ψηφοφορίας χρησιμοποιούν μνήμη flash για να αποθηκεύουν και να ενημερώνονται . Πολλά από αυτά τα συστήματα έχουν τη δυνατότητα να λαμβάνουν ενημερώσεις λογισμικού με τον ίδιο τρόπο (flash drive,CD , κλπ). Αυτό δίνει την ευκαιρία σε έναν εισβολέα να εισάγει ένα κακόβουλο πρόγραμμα σε ένα μηχάνημα ψηφοφορίας προκαλώντας το να υπολογίσει εσφαλμένα τις ψήφους.
Ένας εισβολέας θα μπορούσε να το κάνει αυτό μέσω του Διαδικτύου, εισβάλλοντας στον υπολογιστή που χρησιμοποιείται για τη δημιουργία αρχείων της ψηφοφορίας ή κάποιος με πρόσβαση στον υπολογιστή θα μπορούσε να εισάγει τον κακόβουλο κώδικα κατά τη δημιουργία του αρχείου ψηφοφορίας.

Η εγκατάσταση κακόβουλου λογισμικού θα μπορούσε να πραγματοποιηθεί και κατά την διάρκεια ενημέρωσης του συστήματος είτε του μηχανήματος ψηφοφορίας είτε στον υπολογιστή που χρησιμοποιείται για την δημιουργία των κατάλληλων αρχείων. Είναι πιθανό, κάποιοι πάροχοι των μηχανημάτων αυτών να ανακοινώνουν ενημερώσεις του λογισμικού μέρες ή ώρες πριν την διεξαγωγή των εκλογών ,με αποτέλεσμα να μην προλαβαίνει η επιτροπή να το ελέγξει.

4.1.3 Επίθεση από έναν ψηφοφόρο

Τα μηχανήματα αυτά είναι ευάλωτα κατά την διάρκεια της ψηφοφορίας. Ένας εξειδικευμένος κακόβουλος θα μπορούσε κατά την διάρκεια της ψηφοφορίας να επηρεάσει το μηχάνημα είτε με την εισαγωγή λογισμικού από κάποια θύρα USB, είτε από την αλλαγή κάποιον τσιπ μέσα σε μικρό χρονικό διάστημα στο μηχάνημα. Αυτές οι αλλαγές θα μπορούσαν να επηρεάσουν το αποτέλεσμα των εκλογών.

4.1.4 Clash Attack

Τα περισσότερα μηχανήματα ψηφοφορίας εκτυπώνουν απλά τον ίδιο σειριακό αριθμό στα ψηφοδέλτια που έχουν το ίδιο μοτίβο, δηλαδή, όπου σημειώνονται οι ίδιοι υποψήφιοι, ώστε να πραγματοποιείται η καταμέτρηση των ψήφων. Αξίζει να σημειωθεί ότι δεν είναι σε όλα τα ψηφοδέλτια η ίδια λογική και δεν το πράττουν όλα τα μηχανήματα.
Ο πίνακας ανακοινώσεων μπορεί να αντικαταστήσει με ασφάλεια όλα τα ψηφοδέλτια εκτός από ένα με τον ίδιο σειριακό αριθμό με νέους σειριακούς αριθμούς. Ο πίνακας ανακοινώσεων πρέπει μόνο να διασφαλίσει ότι το σύνολο των ψηφοδελτίων παραμένει ακριβής και ίσος με τους ψηφοφόρους που παραβρέθηκαν στην ψηφοφορία.
Αυτού του είδους η επίθεση θα μπορούσε να πραγματοποιηθεί είτε από κάποιο malware που θα είχε τοποθετήσει κάποιος κακόβουλος είτε από κατασκευαστικό λάθος που δεν είχε ανακαλυφθεί κατά τις δοκιμές

4.2 Επιθέσεις σε ηλεκτρονική ψηφοφορία

4.2.1. Επιθέσεις

Τα τρέχοντα συστήματα παραδοσιακής ψηφοφορίας έχουν λίγες πιθανότητες απάτης σχετικά με την ψήφο, ενώ με την ηλεκτρονική ψηφοφορία, η πιθανότητα απάτης μεγαλώνει υπερβολικά, λόγω της αυτοματοποίησης και της σύνδεσης στο δίκτυο.

Τα ηλεκτρονικά δεδομένα είναι πιθανό να τροποποιηθούν ή να καταστραφούν πιο εύκολα από ό, τι στις φυσικές ψηφοφορίες. Επιπλέον, όλα τα είδη συστημάτων ηλεκτρονικής ψηφοφορίας είναι επιρρεπή σε κάποιο βαθμό σε εσωτερικές επιθέσεις(από το προσωπικό) και επιθέσεις άρνησης υπηρεσίας (DOS attacks). Αν και υπάρχουν ισχυροί κρυπτογραφικοί αλγόριθμοι, δεν έχουμε συστήματα (π.χ. πλατφόρμες, λειτουργικά συστήματα) με επαρκή ασφάλεια στα οποία μπορεί να ενσωματωθεί η κρυπτογραφία. [9] Τα συστήματα ψηφιακής ψηφοφορίας μπορούν να έχουν υψηλό κόστος όσον αφορά την αγορά και τη διατήρηση διακομιστών ψηφοφορίας, τυποποιημένων βάσεων δεδομένων και συστημάτων δρομολόγησης (router). Τα συστήματα αυτά είναι πιο ευαίσθητα σε επιθέσεις μέσω διαδικτύου, όπως coercion attacks. Μπορεί να απαιτείται από τους ψηφοφόρους να ασφαλίζουν τα δικά τους μηχανήματα πριν ψηφίσουν, για να εγγυηθούν την ακρίβεια των εκλογικών αποτελεσμάτων. Ο έλεγχος και η πιστοποίηση των συστημάτων φαίνεται να είναι δύσκολο, καθώς τέτοια συστήματα πιθανώς θα βασίζονται σε εφαρμογές άλλων εταιριών, όπως λειτουργικά συστήματα και προγράμματα περιήγησης.

Η ηλεκτρονική ψηφοφορία είναι πιο ευάλωτη σε επιθέσεις από την παραδοσιακή ψηφοφορία:

- Από την μεριά του ψηφοφόρου: Οι ιοί σκουλήκια (Worm-like) ή οι Δούρειοι ίπποι(Trojan horses) ενδέχεται να αλλάξουν την ψήφο προτού εφαρμοστεί οποιαδήποτε κρυπτογράφηση ή έλεγχος ταυτότητας στα δεδομένα. Ένας εισβολέας μπορεί να εκμεταλλευτεί κενά ασφαλείας στο λειτουργικό σύστημα ή στο πρόγραμμα περιήγησης.[10] Μια ακόμα επίθεση που είναι επιρρεπής τα συστήματα και ο ψηφοφόρος είναι και η επίθεση phishing, όπου ο επιτιθέμενος υποδύεται μία έγκυρη ιστοσελίδα με αποτέλεσμα να κλέβει τα στοιχεία σύνδεσης του ψηφοφόρου
- Στην επικοινωνία: Κατά τη διάρκεια μιας spoofing επίθεσης, ένας εισβολέας θα μπορούσε να τροφοδοτήσει έναν ψηφοφόρο με μια φαινομενικά νόμιμη ιστοσελίδα. Αυτό μπορεί να είναι αρκετό για να αλλάξει την ψήφο του ψηφοφόρου. Η επικοινωνία μπορεί επίσης να απειλείται από άλλες επιθέσεις που βασίζονται στο δίκτυο (π.χ. πλαστογράφηση TCP SYN, κατακερματισμός IP κ.λπ.).

- Στο server : Οι επιθέσεις σε αυτό το επίπεδο είναι παρόμοιες με τις επιθέσεις στον ψηφοφόρο και επιπλέον την DoS επίθεση

Brute Force Επίθεση

Οι ψήφοι αποστέλλονται και αποθηκεύονται στον διακομιστή. Κρυπτογραφούνται από ένα συμμετρικό κλειδί που προστατεύεται μόνο από ένα κλειδί που προέρχεται από το ID και το PIN του ψηφοφόρου. Αυτό οδηγεί στη δυνατότητα ανάκτησης ψήφων μέσω μιας brute force επίθεσης του ID ή του PIN.

Ο κατακερματισμός (Hash) που χρησιμοποιείται από το πρωτόκολλο της διαδικτυακής ψηφοφορίας για την προστασία του ζεύγους ID / PIN μπορεί να δεχτεί επίθεση brute force από έναν επιτιθέμενο που παρακολουθεί την ροή της ανταλλαγής μηνυμάτων μεταξύ ενός ψηφοφόρου και του διακομιστή.

Όταν οι αρχές χρησιμοποιούν τον ίδιο TLS proxy server για την εγγραφή των ψηφοφόρων αλλά και για την πραγματοποίηση της ψηφοφορίας αυτό δίνει την δυνατότητα στον επιτιθέμενο να έχει πρόσβαση στα περισσότερα δεδομένα.

Ενώ η ασφάλεια επιπέδου μεταφοράς (TLS) προστατεύει το δίκτυο από επιθέσεις Man-in-the-middle, η εταιρίες που παρέχονται για την προστασία DDoS επιθέσεων αποδυναμώνουν το πρωτόκολλο TLS

Timing attack:

Στην κρυπτογραφία, μια επίθεση χρονισμού είναι μια επίθεση πλευρικού καναλιού στην οποία ο εισβολέας προσπαθεί να θέσει σε κίνδυνο ένα κρυπτοσύστημα αναλύοντας τον χρόνο που απαιτείται για την εκτέλεση κρυπτογραφικών αλγορίθμων. Κάθε λογική λειτουργία σε έναν υπολογιστή χρειάζεται χρόνο για να εκτελεστεί και ο χρόνος μπορεί να διαφέρει ανάλογα με την είσοδο. Με ακριβείς μετρήσεις του χρόνου για κάθε μέθοδο/συνάρτηση , ένας εισβολέας μπορεί να λειτουργήσει προς την είσοδο.

DDOS επιθεση

Ο φθηνότερος και ευκολότερος τρόπος επίθεσης σε ένα ηλεκτρονικό σύστημα ψηφοφορίας είναι η DDoS επίθεση. Οποιοδήποτε script από έναν κακόβουλο θα μπορούσε με κάποιο Bitcoin να ενοικιάσει έναν στρατό από botnets, ώστε να επιτεθεί στον διακομιστή(server) ψηφοφορίας την ημέρα των εκλογών. Προκειμένου να

αποφευχθούν τέτοιες επιθέσεις, οι εταιρείες συνήθως χρησιμοποιούν τεχνικές για άμυνα όπως Cloudflare ή Incapsula Imperva και άλλες.

Τέτοιες υπηρεσίες είναι κατάλληλες για πολλές εφαρμογές, αλλά δεν είναι κατάλληλες για την εξασφάλιση ελεύθερων και ανοιχτών δημοκρατικών εκλογών. Μια υπηρεσία άμυνας στην DDoS πρέπει να κατασκοπεύει την κυκλοφορία των πακέτων για να σταματήσει τις επιθέσεις DDoS. Αυτό έχει ως βασική προϋπόθεση ότι πρέπει να αποκρυπτογραφήσει όλη την κίνηση μεταξύ του χρήστη και του διακομιστή για να προσδιορίσει ποια πακέτα είναι έγκυρα και ποια πακέτα είναι κακόβουλα. Για να το πραγματοποιήσει αυτό ενεργεί ως ένας TLS διακομιστής (proxy) πραγματοποιώντας μια Man in the middle επίθεση(με την ανάλογη εξουσιοδοτημένη άδεια) εναντίων όλων των πακέτων προς την υπηρεσία της ψηφοφορίας

Το TLS είναι η τεχνολογία κρυπτογράφησης που κάνει το HTTPS να λειτουργεί, το οποίο, υπό κανονικές συνθήκες, θα διασφάλιζε την εμπιστευτικότητα της κυκλοφορίας από το συνομιλητή στον κεντρικό υπολογιστή. Ωστόσο, για να λειτουργήσει μια υπηρεσία αντιμετώπισης της DDoS επίθεσης η οποία βασίζεται στην τεχνολογία του cloud, το κλειδί κρυπτογράφησης TLS της βρίσκεται σε servers σε όλο τον κόσμο. Αυτό έχει ως συνέπεια, οποιοσδήποτε κακόβουλος που θα μπορούσε να εισβάλει σε έναν από αυτούς τους servers, να λάβει το κλειδί αυτό και να επεξεργαστεί την ψηφοφορία. Οποιοσδήποτε επιτιθέμενος θα μπορούσε εύκολα να θέσει σε κίνδυνο έναν από τους servers. Επομένως , κάθε χώρα θα μπορούσε να αποκτήσει τους απαραίτητους κωδικούς πρόσβασης και να επηρεάσει τις εκλογές προς όφελός της.

Η μυστική ψηφοφορία αποτελεί θεμέλιο της δημοκρατίας από την αρχαία Αθήνα είναι ουσιαστικής σημασίας για την αποτροπή της πώλησης ψήφων ή του εξαναγκασμού των ψηφοφόρων. Κανένας δεν πρέπει να ξέρει πως ένας ψηφοφόρος εκλέγει έναν υποψήφιο. Η χρήση μιας υπηρεσίας για την παροχή άμυνας στην DDoS επίθεση σε ένα ψηφιακό σύστημα ψηφοφορίας μπορεί να αποτρέψει την DDoS επίθεση, αλλά δημιουργεί παράλληλα έναν γιγαντιαίο στόχο για οποιοδήποτε έθνος που επιθυμεί να κατασκοπεύσει τους ψηφοφόρους ή να επεξεργαστεί τους ψήφους τους.

4.2.2 Προτάσεις Προστασίας

Υπάρχουν πολλά ζητήματα, τόσο τεχνικά όσο και πολιτικά, τα οποία πρέπει να επιλυθούν προτού η ηλεκτρονική ψηφοφορία γίνει δημόσια αποδεκτή. Πρέπει να χρησιμοποιηθούν ισχυρές κρυπτογραφικές μέθοδοι για να υπάρξει η δυνατότητα ελέγχου και επομένως η εμπιστοσύνη του κοινού στα συστήματα ηλεκτρονικής ψηφοφορίας και οι ψηφοφόροι πρέπει να εκπαιδευτούν σχετικά με την ίδια τη φύση των κρυπτογραφικών εγγυήσεων. Έχει παρατηρηθεί ότι εάν οι ψηφοφόροι και το περιβάλλον τους παρακολουθούνται προσεκτικά, όπως με την παραδοσιακή ψηφοφορία, τότε η ηλεκτρονική ψηφοφορία μπορεί να είναι εφικτή[11,12,13] ακόμη και με σύνδεση στο Διαδίκτυο μεταξύ ψηφοφόρων και server.

Η ηλεκτρονική ψηφοφορία θα γίνει πλήρως ηλεκτρονική μόνο όταν διατίθεται μια ασφαλής και ομοιόμορφη υποδομή δημόσιου κλειδιού για ψηφιακές υπογραφές. Η ακρίβεια και το απόρρητο μέσω του Διαδικτύου πρέπει να προστατεύονται με ισχυρές ψηφιακές υπογραφές και τεχνικές κρυπτογράφησης. Πρέπει να σχεδιαστούν προγράμματα περιήγησης που επιτρέπουν τόσο την κρυπτογράφηση όσο και την ψηφιακή υπογραφή. Επιπλέον, απαιτείται έρευνα σχετικά με την ασφαλή εφαρμογή τεχνολογιών όπως SSL / TLS και SSH για την αντιμετώπιση επιθέσεων πλαστογράφησης [14]. Θα πρέπει να χρησιμοποιούνται ισχυρές διαδικασίες αρίθμησης και ελέγχου, συστήματα προστασίας από ιούς στην πλευρά του κεντρικού υπολογιστή, τείχη προστασίας και συστήματα εντοπισμού εισβολών (IDS) στην πλευρά του διακομιστή. Τέλος, πρέπον θα ήταν να πραγματοποιηθεί μία ανάλυση ρίσκου για ευπάθειες που δεν αναφέρθηκαν όπως η τοποθεσία του server, η ποιότητα του κλπ. Πρέπει να διεξαχθεί μία ισχυρή πολιτική ασφάλειας και να σχεδιαστεί προσεκτικά για να αντιμετωπίσει όλες τις πιθανές επιθέσεις και απειλές. Πρέπει να θεσπιστούν νέοι νόμοι για την προστασία του δικαιώματος της μυστικής ψήφου και για την ποινικοποίηση συμπεριφορών.

5

Διαμόρφωση νομοθεσίας σχετικά με την ηλεκτρονική ψηφοφορία

5.1 Το επίπεδο της Νομοθεσίας

Στις περισσότερες χώρες, θα υπάρξουν ορισμένοι συνταγματικοί κανόνες για τις εκλογές. Γενικά, θα ισχύει ότι οι εκλογές πρέπει να είναι γενικές, άμεσες, ανοικτές και ίσες προς όλους[15]. Αυτά τα δικαιώματα αναφέρονται επίσης στο άρθρο 25 του καταστατικού χάρτη των Ηνωμένων Εθνών για τα Ανθρώπινα Δικαιώματα και στο άρθρο 3 του Πρώτου πρωτόκολλου της Ευρωπαϊκής Σύμβασης για τα Ανθρώπινα Δικαιώματα. Στις περισσότερες περιπτώσεις πιθανότατα, για την εισαγωγή της ηλεκτρονικής ψηφοφορίας να μην είναι απαραίτητο να τροποποιηθούν αυτά τα άρθρα στο σύνταγμα. Ωστόσο, πιθανότατα θα χρειαστεί ο υφιστάμενος εκλογικός νόμος και η χαμηλότερη νομοθεσία να αλλάξει. Το ερώτημα που πρέπει να αντιμετωπίσει ο νομοθέτης σχετικά με αυτές τις αλλαγές είναι ποια στοιχεία πρέπει να ρυθμίζονται από το Κοινοβούλιο και ποια μέρη μπορούν να ανατίθενται σε χαμηλότερα επίπεδα νομοθεσίας. Στα περισσότερα νομοθετικά συστήματα, οι γενικοί και αφηρημένοι κανόνες θεσπίζονται από το Κοινοβούλιο, και τα διοικητικά και τα τεχνικά θέματα μπορούν να ανατεθούν σε χαμηλότερα επίπεδα νομοθεσίας. Όσον αφορά την ηλεκτρονική ψηφοφορία, ορισμένοι συγγραφείς τείνουν να έχουν τη ίδια άποψη[16,17]. Ωστόσο, όπως αναφέρθηκε προηγουμένως, η εκλογική διαδικασία είναι πολύ πολιτικοποιημένη. Αυτό σημαίνει ότι όσον αφορά τη νομοθεσία σχετικά με τις εκλογές, ενδέχεται να είναι απαραίτητο να εμπλακεί το Κοινοβούλιο σε περισσότερα στοιχεία του νομοθετικού συστήματος προκειμένου να διασφαλιστεί ότι ένα κυβερνών κόμμα δεν είναι σε θέση να αλλάξει ορισμένα νομοθετικά στοιχεία της εκλογικής διαδικασίας προς το δικό του συμφέρον.

Ελάττωμα της διαδικασίας των εκλογών είναι ότι οι λεπτομέρειες που μπορεί να φαίνονται αρκετά τεχνικές και όχι απαραίτητα πολιτικές θα μπορούσαν τελικά να χρησιμοποιηθούν με πολιτικό τρόπο[16]. Για παράδειγμα, το χρονικό πλαίσιο στο οποίο οι ψηφοφόροι μπορούν να υποβάλουν αίτηση για βιομετρική εγγραφή ψηφοφόρων μπορεί να χρησιμοποιηθεί για τον αποκλεισμό ορισμένων ομάδων ψηφοφόρων, όπως τα άτομα που ζουν στο εξωτερικό και κάνουν χρήση αυτού του τρόπου εγγραφής. Εάν είναι γνωστό ότι αυτές οι ομάδες ψηφοφόρων τείνουν να ψηφίζουν ένα συγκεκριμένο κόμμα/ κόμματα, μπορεί να είναι επωφελές για το κυβερνών κόμμα να ορίσει το χρονικό πλαίσιο με τέτοιο τρόπο ώστε να αποκλειστούν αυτοί οι ψηφοφόροι, εάν αυτό σημαίνει αποδυνάμωση της αντιπολίτευσης, ή να συμπεριληφθούν στην περίπτωση που είναι δικοί τους ψηφοφόροι [18]. Αυτό θα σήμαινε ότι διοικητικές και τεχνικές λεπτομέρειες που κανονικά θα ρυθμιζόντουσαν από χαμηλότερη νομοθεσία ενδέχεται να πρέπει να εμπλακεί το Κοινοβούλιο όταν πρόκειται για εκλογές. Ωστόσο, στις περισσότερες χώρες, η αλλαγή των πράξεων του Κοινοβουλίου με σκοπό να εμπλακεί απαιτεί περισσότερο χρόνο από οποιαδήποτε άλλη αλλαγή της χαμηλότερης νομοθεσίας. Δεδομένου ότι η νομοθεσία για την ηλεκτρονική ψηφοφορία πιθανότατα να περιλαμβάνει τεχνικές προδιαγραφές που μπορεί να αλλάξουν αρκετά γρήγορα λόγω των νέων τεχνολογικών βελτιώσεων. Με αποτέλεσμα την νομιμοποίηση ολόκληρης της διαδικασίας της ηλεκτρονικής ψηφοφορίας μέσω του Κοινοβουλίου που θα μπορούσε να παρεμποδίσει τη νομοθετική διαδικασία[19].

5.2 Η νομοθεσία

5.2.1 Διαχωρισμός Αρμοδιοτήτων

Σε χώρες που διαθέτουν ένα πολύ αποκεντρωμένο σύστημα για τη διεξαγωγή εκλογών, όπως το Ηνωμένο Βασίλειο και η Ολλανδία, οι παραδοσιακές εκλογές που πραγματοποιούνται μπορούν πολύ εύκολα να διεξαχθούν από αυτό το τοπικό επίπεδο εκλογικής διοίκησης. Αν και είναι απαραίτητη η λεπτομερής γνώση των διαδικασιών ψηφοφορίας, οι εκλογές με χάρτινα ψηφοδέλτια δεν απαιτούν πολύ συγκεκριμένες

τεχνικές γνώσεις. Επίσης, η αλυσίδα διοίκησης δεν είναι πραγματικό ζήτημα στις απλές εκλογές, καθώς το εκλογικό υλικό είναι άχρηστο μεταξύ των τωρινών εκλογών και των επομένων. Αυτό σημαίνει ότι δεν έχει σημασία εάν οι δήμοι και οι τοπικοί φορείς διαχείρισης εκλογών έχουν ελαφρώς διαφορετικές διαδικασίες για την αποθήκευση υλικού. Ωστόσο, κατά την εισαγωγή μορφών ηλεκτρονικής ψηφοφορίας ή ηλεκτρονικής καταμέτρησης, αυτό αλλάζει. Πρώτον, απαιτείται μεγαλύτερη τεχνική γνώση για τη διεξαγωγή εκλογών[20]. Όσον αφορά τα EMB πρέπει να υπάρχει η κατάλληλη γνώση για την επίλυση πιθανών τεχνικών προβλημάτων και τρόπων αντιμετώπισής τους. Αυτό σημαίνει ότι η εκπαίδευση δεν θα μπορούσε σε όλες τις περιπτώσεις να αφεθεί στους τοπικούς φορείς, αλλά πρέπει να γίνει σε κεντρικό επίπεδο. Επίσης, ένας υπολογιστής ψηφοφορίας ή ένας σαρωτής ψηφοφορίας μεταξύ των εκλογών πρέπει να αποθηκευτεί με ασφάλεια για να αποφευχθεί η αλλαγή λογισμικού ή άλλων σχετικών μερών του εξοπλισμού από τρίτους. Δεδομένου ότι αυτή η αλυσίδα επιμέλειας είναι ύψιστης σημασίας για τη διασφάλιση της ακεραιότητας των εκλογών[21], ίσως δεν είναι πρέπον να αφήσουμε τις τοπικές αρχές να αποφασίσουν πώς θα το αντιμετωπίσουν, αλλά να έχουν ομοιόμορφους κανονισμούς για ολόκληρη τη χώρα. Αυτό σημαίνει ότι θα πρέπει να επανεξεταστεί ο καταμερισμός αρμοδιοτήτων μεταξύ των εθνικών και των τοπικών αρχών που λειτουργούν στην εκλογική διαδικασία[22].

5.2.2 Ποινικό δίκαιο

Ένα πράγμα που πρέπει να ληφθεί υπόψη κατά την εισαγωγή της ηλεκτρονικής ψηφοφορίας ή άλλων μορφών ηλεκτρονικής χρήσης κατά την εκλογική διαδικασία είναι, εάν τα άρθρα είτε στον εκλογικό νόμο είτε στον Ποινικό Κώδικα που ασχολούνται με εκλογικά εγκλήματα είναι κατάλληλα για αδικήματα που διαπράττονται κατά τη χρήση ηλεκτρονικών ψηφοφοριών[23,24]. Για παράδειγμα, η Ολλανδία χρησιμοποίει DREs στις εκλογές, αλλά όταν ένας υποψήφιος και ένας εργαζόμενος στις δημοσκοπήσεις χρησιμοποίησαν το DRE για να διαπράξουν εκλογική απάτη, ήταν δύσκολο να καταδικαστούν για αυτό το έγκλημα. Αυτό οφείλεται στο γεγονός ότι τα άρθρα του νόμου για τις εκλογές, γράφτηκαν για εκλογές βασισμένες στην

παραδοσιακή ψηφοφορία και δεν ξαναγράφτηκαν κατά την εισαγωγή των DRE. Επειδή υπήρχε ένας γενικός νόμο στον Ποινικό Κώδικα σχετικά με την απάτη με υπολογιστή, ήταν δυνατόν να καταδικαστεί αυτό το άτομο, αλλά αυτό δεν συμβαίνει πάντα. Επίσης, σε ορισμένες χώρες απαιτείται καταδίκη για εκλογικά αδικήματα με ποινή την αφαίρεση των εκλογικών δικαιωμάτων ενός ατόμου. Εάν η εκλογή ή το ποινικό δίκαιο δεν είναι προσαρμοσμένα για ηλεκτρονική ψηφοφορία, τέτοια συγκεκριμένα μέτρα ενδέχεται να μην είναι διαθέσιμα .

Μια άλλη πτυχή που πρέπει να ληφθεί υπόψη είναι η συλλογή αποδεικτικών στοιχείων κατά την αντιμετώπιση των εκλογικών εγκλημάτων. Με τις παραδοσιακές εκλογές είναι απόλυτα σαφές ποια υλικά μπορούν να εξεταστούν για να διαπιστωθεί εάν διαπράχθηκε έγκλημα. Με την ηλεκτρονική ψηφοφορία αυτό μπορεί να είναι πιο δύσκολο και σε ορισμένες περιπτώσεις μπορεί να εξαρτάται από τον πωλητή ή τον ιδιοκτήτη του εξοπλισμού που χρησιμοποιείται για τη συνεργασία με τη συλλογή αποδεικτικών στοιχείων. Συνιστάται λοιπόν ο νομοθέτης να λαμβάνει υπόψη εάν είναι απαραίτητη η συμπερίληψη ορισμένων άρθρων που αφορούν την υποχρέωση συνεργασίας. Τέλος, η κλίμακα πιθανής απάτης στις εκλογές μπορεί να είναι μεγαλύτερη στην ηλεκτρονική ψηφοφορία παρά στην παραδοσιακή ψηφοφορία. Για να διαπραχθεί έγκλημα στην απλή ψηφοφορία, ίσως χρειαστεί συνωμότης σε σχεδόν κάθε εκλογικό κέντρο. Με την ηλεκτρονική ψηφοφορία, κάποιος ξένος μπορεί να μπει στο λογισμικό που χρησιμοποιείται και αυτό θα μπορούσε να γίνει με λιγότερα άτομα ή και μόνος του[25]. Αυτό κάνει διαφορετική την ανάλυση κινδύνου για τον πιθανό δράστη. Προκειμένου να αντιμετωπιστεί αυτό, οι πιθανές ποινές πρέπει να είναι μεγαλύτερες.

5.3 Τεχνικά Προβλήματα

Οι νομοθέτες που εξετάζουν την εισαγωγή της ηλεκτρονικής ψηφοφορίας θα πρέπει να αντιμετωπίσουν διάφορα τεχνικά ζητήματα. Ζητήματα που έχουν ερευνηθεί καλά είναι οι διαδικασίες πιστοποίησης και διαδικασίες προμηθειών. Υπάρχουν, ωστόσο, ορισμένα άλλα ζητήματα που δεν έχουν εξεταστεί ακόμη καλά.

5.3.1 Νομοθεσία για καταστάσεις έκτακτης ανάγκης

Όταν χρησιμοποιούνται χάρτινα ψηφοδέλτια, ενδέχεται να απαιτούνται μέτρα έκτακτης ανάγκης την ημέρα των Εκλογών, αλλά συνήθως σε μικρή κλίμακα. Αυτό θα ισχύει για παράδειγμα εάν τα ψηφοδέλτια δεν παραδίδονται στο εκλογικό τμήμα ή εάν υπάρχει τυπωμένη περίπτωση λανθασμένων πληροφοριών. Ωστόσο, στις περισσότερες από αυτές τις περιπτώσεις, αυτά θα είναι τοπικά προβλήματα που μπορούν εύκολα να επιλυθούν χωρίς να διαταραχθεί υπερβολικά η εκλογική διαδικασία. Όμως, με την ηλεκτρονική ψηφοφορία αυτό μπορεί να είναι πολύ διαφορετικό, εάν μια χώρα χρησιμοποιεί μηχανήματα και λογισμικό κατασκευασμένο από ένα συμβαλλόμενο μέρος, δημόσιο ή ιδιωτικό, ένα πρόβλημα με αυτό το μηχάνημα ή λογισμικό μπορεί να υπάρξει σε όλο τον εξοπλισμό. Αυτό σημαίνει ότι ολόκληρες οι εκλογές ενδέχεται να τεθούν σε κίνδυνο. Εάν χρησιμοποιείται ένα σύστημα ηλεκτρονικής ψηφοφορίας και υπάρχουν προβλήματα με το Διαδίκτυο την ημέρα των εκλογών, θα μπορούσαν επίσης να έχουν μεγάλες συνέπειες για την εγκυρότητα των εκλογών. Το κύριο πρόβλημα με τις εκλογές είναι ότι πρέπει να συμβούν σε πολύ σύντομο χρονικό διάστημα, ως επί το πλείστων σε μια μέρα και ότι υπάρχει πολύ λίγος χώρος για επαναλήψεις. Η νομοθεσία για τέτοιου είδους καταστάσεις έκτακτης ανάγκης είναι πολύ δύσκολη, λόγω του πολιτικού χαρακτήρα των εκλογών. Ωστόσο, δεν είναι καλή ιδέα να μην υπάρχουν σχέδια έκτακτης ανάγκης και να λαμβάνονται οι αποφάσεις κατά την εμφάνιση προβλημάτων. Αυτό θα μπορούσε ενδεχομένως να δώσει στο στέλεχος πολύ χώρο για να λάβει πολιτικά μεροληπτικές αποφάσεις[26]. Ο νομοθέτης πρέπει να γνωρίζει αυτό το δίλημμα κατά τη νομοθεσία για την ηλεκτρονική ψηφοφορία, προκειμένου να προσπαθήσει να βρει μια ισορροπία μεταξύ της παροχής επαρκούς καθοδήγησης για το πώς να λειτουργεί όταν προκύπτουν προβλήματα, και της προσπάθειας του να μην νομοθετήσει για κάθε πρόβλημα που μπορεί να προκύψει[20].

5.3.2 Διπλά συστήματα

Μετά τη συζήτηση σε διάφορες χώρες σχετικά με το πρόβλημα των υπολογιστών ψηφοφορίας οι οποίοι αποτελούν άγνωστο πεδίο για αυτές, έχουν δημιουργηθεί

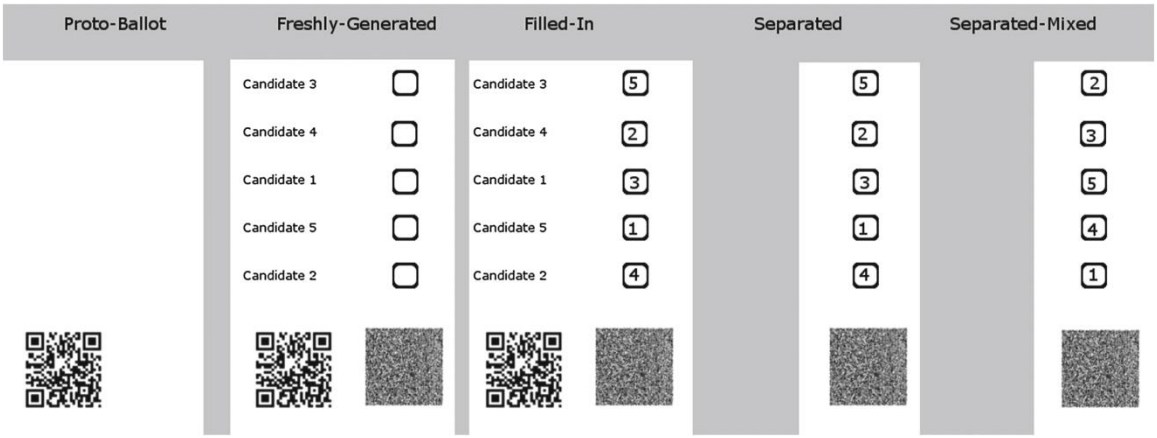
συστήματα που έχουν προσθέσει ένα είδος χάρτινου ψηφοδελτίου στον υπολογιστή. Αυτό σημαίνει ότι είναι δυνατή η σύγκριση των αποτελεσμάτων που δίνονται από τον υπολογιστή με χάρτινο ψηφοδέλτιο. Αυτό ακούγεται πολύ καλό όσον αφορά τη διαφάνεια και την ακεραιότητα. Ωστόσο, έθεσε επίσης δύσκολες ερωτήσεις στον νομοθέτη, οι οποίες θα πρέπει να επιλυθούν βάσει νόμου πριν από κάθε εκλογή. Το κύριο ερώτημα είναι ποιο από τα συστήματα υπερτερεί, τα αποτελέσματα του υπολογιστή ή του χάρτινου ψηφοδελτίου. Αν το χάρτινο ψηφοδέλτιο υπερτερεί, αυτό σημαίνει ότι στην πραγματικότητα σε όλες τις περιπτώσεις, όλες οι εκτυπώσεις χαρτιού πρέπει να μετρηθούν. Αυτό όμως σημαίνει ότι ένα από τα οφέλη της ηλεκτρονικής ψηφοφορίας, η ακρίβεια και η ταχύτητα της καταμέτρησης των ψήφων ακυρώνονται. Ωστόσο, εάν οι νομοθέτες επιλέξουν να βασίζονται στα αποτελέσματα του υπολογιστή, η προσθήκη χαρτιού είναι χρήσιμη μόνο όταν μετράτε ένα ορισμένο ποσοστό εκτυπώσεων και σε σύγκριση με τα αποτελέσματα του υπολογιστή. Σε αυτήν την περίπτωση, ο νομοθέτης όχι μόνο πρέπει να θεσπίσει κανόνες σχετικά με αυτό το ποσοστό, αλλά και για τον τρόπο με τον οποίο καταλογίζονται τα εκλογικά κέντρα ή τα μέρη καταμέτρησης [27]. Το πιο σημαντικό όμως είναι ότι ο νόμος πρέπει να είναι σαφής σχετικά με το τι πρέπει να συμβεί σε περίπτωση που υπάρχουν διαφορές μεταξύ του αριθμού του υπολογιστή και του μη αυτόματου αριθμού[23] .

6.

Προτάσεις επιστημόνων για την ενίσχυση των REV

Prêt à Voter

Το Prêt à Voter είναι ένα σύστημα ψηφοφορίας E2E που παρουσιάστηκε από τον Peter Ryan του Πανεπιστημίου του Λουξεμβούργου[28] με βάση την « Οπτική Κρυπτογραφία » του Chaum[29] . Στόχος του είναι να παρέχει εγγυήσεις για την ακρίβεια της καταμέτρησης και του απορρήτου των ψηφοφοριών που είναι ανεξάρτητες από λογισμικό, υλικό κ.λπ. Η βασική καινοτομία, η οποία βρίσκεται στο επίκεντρο του Prêt à Voter, είναι να διαφοροποιηθεί η υποψήφια σειρά. Το Prêt à Voter παρέχει προστασία απορρήτου ισοδύναμο με το κρυπτοσύστημα, που χρησιμοποιείται για την κρυπτογράφηση της υποψήφιας παραγγελίας, εκτός εάν οι αξιόπιστες συσκευές είναι κατεστραμμένες.



Εικόνα 4 Σύστημα ψηφοφορίας Pret a Voter, Πηγή:

https://images.app.goo.gl/MDgSf2J4z4NFCXmP8

Μια ψήφος Prêt à Voter, έτοιμη να συμπληρωθεί, φαίνεται στο Σχ. 1. Αποτελείται από μια αριστερή πλευρά και μια δεξιά πλευρά. Η αριστερή πλευρά περιέχει τη λίστα των υποψηφίων σε μια συγκεκριμένη κατάταξη τόσο σε μορφές αναγνώσιμες από τον άνθρωπο όσο και από τον υπολογιστή. Η δεξιά πλευρά περιέχει πλαίσια όπου μπορεί

να σημειωθεί η επιθυμητή σειρά τον υποψηφίων και στην συνέχεια να κρυπτογραφηθεί από ένα κλειδί που κατέχουν οι ψηφοφόροι.

Ένα συμβατικό ψηφοδέλτιο του Prêt à Voter μπορεί να είναι ως εξής:

Προκειμένου ο Prêt à Voter να είναι χωρίς απόδειξη της ψήφου, είναι σαφές ότι οι χωριστές ψηφοφορίες δεν πρέπει να αποκαλύπτουν τις ψήφους. Επιπλέον, είναι σαφές ότι τα συμπληρωμένα ψηφοδέλτια είναι αυτά που θα αποκαλύπτουν τους ψήφους. Τα νέα ψηφοδέλτια δεν αποκαλύπτουν τους ψήφους, ωστόσο, περιέχουν τη σχέση μεταξύ της αναδιάταξης και του ciphertext . Δεδομένου ότι αυτό το ciphertext θα εμφανιστεί αργότερα στο Bulletin Board δίπλα σε μια κατάταξη, τα πρόσφατα δημιουργημένα ψηφοδέλτια αποκαλύπτουν τους ψήφους, όπως σημείωσε ο Ryan[30].

6.1 Η Λυση των Thomas Haines and Xavier Boyen: Truly Multi-authority Prêt à Voter

Οι Thomas Haines and Xavier Boyen εφαρμόζουν την λύση τους στο Prêt à Voter, ένα υπερσύγχρονο ηλεκτρονικό σύστημα ψηφοφορίας. Προτείνουν δύο προσεγγίσεις: μία με υψηλότερη ασφάλεια και μια άλλη με αυστηρότερους περιορισμούς χρηστικότητας. Το πρωταρχικό όφελος είναι ότι τα ψηφοδέλτια δεν αποτελούν πλέον κίνδυνο ιδιωτικότητας. Δώσανε την λύση για την σύγκρουση μεταξύ της δυνατότητας ελέγχου και του εμπιστευτικού απορρήτου των εκτυπωτών. Τα πρόσθετα οφέλη περιλαμβάνουν την πρακτική προστασία της ιδιωτικότητας από παραβιασμένες συσκευές ψηφοφορίας. Παρόλο που δεν παρέχουν προστασία της ιδιωτικότητας ενάντια σε μια πλήρως παραβιασμένη αρχή, ένας ψηφοφόρος χρειάζεται ειλικρίνεια από ένα μόνο από τα μηχανήματα στον εκλογικό χώρο για μυστικότητα.

Τα κρυπτογραφικά σχήματα ψηφοφορίας μπορούν να κατηγοριοποιηθούν ως εξής:

- Αυτά που χρησιμοποιούν mixnets.[31-36] Τα συστήματα αυτά επιτρέπουν την αυθαίρετη και εκφραστική ψηφοφορία σε σχετικά σταθερό κόστος, καθώς ο υπολογισμός του γίνεται στους αποκρυπτογραφημένους και ανακατεμένους ψήφους. Ωστόσο υπάρχει

καθυστέρηση στον υπολογισμό λόγω της ανάγκης για επαλήθευση των ψήφων μετά τις εκλογές.

- Αυτά που χρησιμοποιούν homomorphic κρυπτογραφία[37-40]. Τα συστήματα αυτά υπόσχονται ένα υψηλότερο επίπεδο ιδιωτικότητας και ασφάλειας καθώς οι ψήφοι δεν αποκαλύπτονται και εμφανίζεται μόνο το τελικό αποτέλεσμα με τις κατάλληλες αποδείξεις. Όμως ο υπολογισμός των ψήφων είναι μια δαπανηρή διαδικασία.
- Αυτά που χρησιμοποιούν την blind υπογραφή.[41-44] Τα σχήματα αυτά απαιτούν διαφορετικές υλοποιήσεις ανώνυμων καναλιών από τα σχήματα που βασίζονται σε mixnet και μετατοπίζουν μεγάλο μέρος της κρυπτογραφικής διαδικασίας από την αρχή στον ψηφοφόρο, κάτι που μπορεί να είναι πιο αποτελεσματικό.

Παρουσιάζουν δύο νέες παραλλαγές του Prêt à Voter,[53] με βάση την εκ νέου κρυπτογράφηση. Οι παραλλαγές τους επιτυγχάνουν την διαφύλαξη του απορρήτου της συσκευής χωρίς να βασίζονται σε προηγούμενα μυστικά κλειδιά.

Στο Prêt à Voter, ο ψηφοφόρος απαιτείται να λάβει κάποιες μυστικές πληροφορίες για να συμπληρώσει και να ψηφίσει. Ομοίως, στο Scantegrity II (ένα άλλο σημαντικό ηλεκτρονικό σύστημα ψηφοφορίας),[45] ο ψηφοφόρος πρέπει να λάβει μυστικούς κωδικούς επιβεβαίωσης. Η απαίτηση ότι αυτές οι πληροφορίες πρέπει να διατηρούνται μυστικές δημιουργεί δυσκολίες στη δημιουργία και μεταφορά ψηφοδελτίων.

Οι προφανείς παραβιάσεις των ψηφοδελτίων του Scantegrity II πρέπει να παρέχουν ισχυρές αποδείξεις στον ψηφοφόρο ότι οι πληροφορίες έχουν μεταφερθεί με ασφάλεια, αλλά δεν παρέχει καμία εγγύηση σχετικά με το απόρρητο κατά της αρχής της εκτύπωσης. Έχουν γίνει εργασίες για την ασφαλή εκτύπωση[46], ωστόσο, σε αυτήν την περίπτωση, ο ψηφοφόρος που λαμβάνει το ψηφοδέλτιο δεν μπορεί να επαληθεύσει εύκολα το απόρρητο της ψηφοφορίας του.

Το κυρίαρχο ζήτημα στην ασφάλεια της ψηφοφορίας είναι πώς θα επιτευχθεί, ταυτόχρονα, η ακεραιότητα και η ιδιωτικότητα. Ένα untappable κανάλι επικοινωνίας σε τουλάχιστον μια κατεύθυνση , μεταξύ ψηφοφόρου και της αρμόδιας υπηρεσίας για την ψηφοφορία, φαίνεται απαραίτητο για την απόδειξη παραλαβής της ψήφου. Τα παραβάν είναι σχεδιασμένα από την κυβέρνηση ώστε να υλοποιείται αυτός ο

περιορισμός. Ένα μεγάλο πρόβλημα για την ιδιωτικότητα που αντιμετωπίζουμε είναι το γεγονός πως θεωρούμε την εκλογική αρχή ως αντίπαλο. Για τον μετριασμό και τον έλεγχο αυτού του ζητήματος, ο ρόλος της εκλογικής αρχής διαιρείται συχνά σε μια συλλογή κομμάτων των οποίων τα συμφέροντα βρίσκονται σε διένεξη. Ο προτιμώμενος μηχανισμός για αυτό είναι η threshold κρυπτογραφία. Ωστόσο, αυτό δεν υπερασπίζει το απόρρητο από το μηχάνημα που κρυπτογραφεί (όπως το Wombat[47], το StarVote[48] ή το Moran-Naor[49]) ή εκτυπώνει την ψηφοφορία (όπως στο Prêt à Voter and Scantegrity) II).

Ο διαχωρισμός της «εμπιστοσύνης» μεταξύ πολλών οντοτήτων δημιουργεί μια ισχυρή διαφορά μεταξύ της ιδιωτικής ζωής έναντι των χρηστών των εκλογών και της ιδιωτικής ζωής έναντι των μηχανών ή των εκτυπωτών. Προσπαθούν να δείξουν πως να υπερασπιστούν την ιδιωτικότητα σε ένα μηχάνημα στο οποίο χρησιμοποιεί ένας ψηφοφόρος σε ένα εκλογικό κέντρο και όχι σε όλα τα μηχανήματα. Αυτό δεν είναι δυνατόν να προστατεύσει από μια εντελώς διεφθαρμένη εκλογική αρχή που δημιουργεί τον εκλογικό θάλαμο και επομένως ελέγχει όλες τις υπολογιστικές συσκευές της. Ωστόσο, προστατεύει από ad hoc συμβιβασμούς μεμονωμένων συσκευών δημοσκόπησης.

Τρία από τα εξέχοντα συστήματα ψηφοφορίας στον εκλογικό θάλαμο είναι τα Prˆet a Voter [53], Scantegrity II[50] και STAR-Vote[48]. Το καθένα αντιπροσωπεύει μια πολύ διαφορετική προσέγγιση για την ψηφοφορία με ηλεκτρονικό υπολογιστή. Κάθε μία από αυτές τις προσεγγίσεις έχει ένα ευρέως διαχωρισμένο σύνολο πιθανών λύσεων για την επίτευξη απορρήτου ενάντια σε διεφθαρμένες συσκευές. Τα εξετάζουμε εν συντομία.

- **STAR-Vote:** Χρησιμοποιεί μια συσκευή για την κρυπτογράφηση ψήφων απευθείας από την είσοδο της ψήφου. Μια τέτοια συσκευή μαθαίνει απαραιτήτως τις ψήφους, οπότε οποιαδήποτε λύση που προσπαθεί να επιτύχει το απόρρητο κατά των διεφθαρμένων συσκευών στο STAR-Vote φαίνεται να απαιτεί τη χρήση πολλαπλών συσκευών για την κρυπτογράφηση των ψήφων.
- **Scantegrity II:** βασίζεται σε οπτικά συστήματα σάρωσης και παρέχει επαλήθευση από άκρο σε άκρο των εκλογικών αποτελεσμάτων. Αυτό

το επιτυγχάνει μέσω της εκτύπωσης κωδικών επιβεβαίωσης στην ψηφοφορία που ο ψηφοφόρος αποκαλύπτει ως μέρος της ψηφοφορίας. Αυτοί οι κωδικοί επιβεβαίωσης εμφανίζονται αργότερα στον πίνακα ανακοινώσεων που επιτρέπει στους ψηφοφόρους να επιβεβαιώσουν την ψήφο τους. Η χρήση στατικών (μη τυχαιοποιημένων) κωδικών επιβεβαίωσης αποτρέπει την εκ νέου κρυπτογράφηση. Δεδομένου ότι η εκ νέου κρυπτογράφηση δεν είναι δυνατή, οι ψήφοι δεν μπορούν να ανωνυμοποιηθούν περαιτέρω.

- **Prêt à Voter:** χρησιμοποιεί υβριδική κρυπτογραφία ανθρώπου-υπολογιστή για να επιτύχει υψηλό επίπεδο πρακτικότητας και απορρήτου. Το ζήτημα της ιδιωτικότητας εναντίων των διεφθαρμένων μηχανών ψηφοφορίας αντιμετωπίζεται κυρίως με τον τρόπο δημιουργίας ψηφοδελτίων. Τα ψηφοδέλτια δεν μπορούν να δημιουργηθούν άμεσα λόγω των ζητημάτων παραβίασης της ιδιωτικότητας και για την αποφυγή επιθέσεων κλεπτογραφίας[51]. Το κλεπτογραφικό πρόβλημα επιλύεται με τη διανομή πληροφοριών δημιουργίας της ψηφοφορίας σε ένα σύνολο ατόμων[52]. Ωστόσο, λύσεις αυτού του είδους εξακολουθούν να χρησιμοποιούν έναν φυσικό εκτυπωτή που πρέπει να είναι αξιόπιστος ώστε να προστατεύει το απόρρητο.

Έτσι, ενώ είναι δυνατόν να διαιρέσουμε την εξουσία μεταξύ των χρηστών και να προτείνουμε κατασκευές ασφαλών καναλιών, όλες αυτές οι λύσεις απαιτούν επί του παρόντος κάποια αξιόπιστη συσκευή (εκτυπωτής ή ψηφοδέλτιο). Αυτή η συσκευή παρουσιάζει επαρκείς πληροφορίες στον ψηφοφόρο για να του δώσει τη δυνατότητα να ψηφίσει και, με αυτόν τον τρόπο, η συσκευή μαθαίνει επαρκείς πληροφορίες για να ανακτήσει την επιλογή του ψηφοφόρου (τουλάχιστον μέχρι να εμφανιστούν οι πληροφορίες επαλήθευσης στον πίνακα ανακοινώσεων). Στο πλαίσιο του Prêt à Voter, προτάθηκε μια λύση[46] για χρήση οπτικής κρυπτογραφίας ώστε να επιτρέπεται σε πολλούς εκτυπωτές να κατασκευάζουν ψηφοδέλτιο. Στην συνέχεια προτάθηκε μια άλλη προσέγγιση που αφορούσε τη πρόσληψη πολλών υπαλλήλων για επανακρυπτογράφηση των ψηφοδελτίων[53], αλλά αυτό αργότερα αποδείχθηκε ότι

«έσπασε»[54] επειδή οι μεγάλες παραλλαγές που διέρρευσαν είναι πιθανό να μην είναι μοναδικές.

Η βασική ιδέα τους είναι να επιτρέψουν την προαιρετική εκ νέου κρυπτογράφηση σε χωριστά ψηφοδέλτια για την παροχή απορρήτου έναντι διεφθαρμένων συσκευών. Οι παραλλαγές τους είναι παρόμοιες με το θεωρητικό σύστημα ψηφοφορίας των Hirt και Sako[40]. Ωστόσο, οι Hirt και Sako δεν κάνουν τη διάκριση μεταξύ του ψηφοφόρου και της υπολογιστικής τους συσκευής. Αυτή όμως είναι η πρόκληση της πρακτικής λύσης του τρόπου επίτευξης ασφάλειας στον ψηφοφόρο, χωρίς την εμπιστοσύνη στη συσκευή, η οποία είναι η κύρια συμβολή τους. Και στις δύο παραλλαγές τους κατασκευάζουν ένα ανώνυμο κανάλι χρησιμοποιώντας ένα σύνολο αποστολέων και δεκτών , σαν ένα mixnet. Ωστόσο, σε αντίθεση με τα mixnets, η εκ νέου κρυπτογράφηση πραγματοποιείται σε μεμονωμένα ψηφοδέλτια και καθοδηγείται από τη δράση των ψηφοφόρων. Το σχήμα που ανέπτυξαν, έχει ορισμένα κοινά χαρακτηριστικά με τους αξιόπιστους τυχαιοποιητές(μηχανισμοί που παράγουν τυχαίους αριθμούς) των Lee[54] και Aditya[55], αλλά δεν έχουν χρησιμοποιήσει αξιόπιστα στοιχεία για την τυχαιοποίηση και διατηρούν την επαλήθευση που προορίζεται για τη μετάδοση.

Η πιο σημαντική ιδιότητα είναι να επιτύχουν με τα συστήματα τους να μην απαιτούν προηγούμενα μυστικά κλειδιά. Στόχος τους είναι να αφαιρεθεί η δύναμη του αντιπάλου να ελέγχει όλα τα στοιχεία και τα δεδομένα που ο ψηφοφόρος φέρνει στο εκλογικό θάλαμο.

6.1.1 Χωρίς την χρήση προηγούμενων μυστικών κλειδιών

Ο αντίπαλος έχει πλήρη γνώση και έλεγχο επί όλων των πληροφοριών που παραδίδονται στον ψηφοφόρο πριν εισέλθει στον εκλογικό θάλαμο.

Πρέπει να σημειωθεί ότι άλλα σχήματα από άκρο σε άκρο, όπως το STAR-Vote, και το Prêt à Voter, όπως εφαρμόζονται στη Βικτώρια της Αυστραλίας, δεν απαιτούν την διαβίβαση προηγούμενων μυστικών κλειδιών στον ψηφοφόρο. Αντ 'αυτού, περιέχουν μεμονωμένες συσκευές που εμποδίζονται μόνο διαδικαστικά να παραβιάσουν το

απόρρητο. Ορίζουν την πλήρη ιδιότητα του απορρήτου συσκευής για να αντικατοπτρίζει ένα σχήμα που διατηρεί τις επιθέσεις μιας συσκευής.

6.1.2 Ιδιωτικό απόρρητο συσκευής

Ένα σύστημα ψηφοφορίας έχει πλήρη προστασία του απόρρητου της συσκευής, υπό την προϋπόθεση ότι τουλάχιστον μία συσκευή είναι ειλικρινής, έτσι διασφαλίζεται το απόρρητο του ψηφοφόρου.
Προσθέτουν επίσης τον πρόσθετο περιορισμό ότι οι συσκευές δεν πρέπει να συνδεθούν με το διαδίκτυο. Ο περιορισμός αυτός διευκολύνει την εφαρμογή των διαδικαστικών μέτρων κατά των κλεπτογραφικών και άλλων επιθέσεων που στοχεύουν και προέρχονται από τις συσκευές.

6.1.3 Χωρίς σύνδεση σε δίκτυο

Καμία συσκευή μέσα στον εκλογικό θάλαμο δεν απαιτεί πρόσβαση στο δίκτυο ώστε να συνδεθεί με οποιαδήποτε άλλη συσκευή, τοπική ή απομακρυσμένη, για να λειτουργεί κατά τη διάρκεια των εκλογών.
Υποθέτουν ότι οι αποδείξεις που λαμβάνουν οι ψηφοφόροι είναι γνωστές στο κοινό και συνδέονται με αυτές. Δεδομένου ότι οι ψηφοφόροι ενθαρρύνονται στις περισσότερες προτάσεις να κοινοποιήσουν τις αποδείξεις τους σε όσο το δυνατόν περισσότερα ενδιαφερόμενα μέρη, αυτή η υπόθεση φαίνεται λογική.

6.1.4 Δημόσιες αποδείξεις

Οι πληροφορίες που παρέχονται στον πίνακα ανακοινώσεων και στις αποδείξεις με σκοπό την επαλήθευση των ψήφων είναι διαθέσιμες στο κοινό και οι συνδέσεις των ψήφων με τους ψηφοφόρους είναι γνωστοί.

Η πρώτη τους παραλλαγή βασίζεται σε μια υπόθεση ανθρώπινου υπολογισμού πολύ παρόμοιου με αυτόν του Prˆet a Voter. Στο τυπικό Prˆet a Voter, θεωρείται ότι ένας ψηφοφόρος που έχει μια λίστα υποψηφίων μπορεί να δημιουργήσει μία κατάταξη με βάσει τις προτιμήσεις του. Αυτή η λογική υπόθεση είναι ελαφρώς τροποποιημένη για την παραλλαγή τους, υποθέτοντας ότι ο ψηφοφόρος μπορεί να λάβει δύο λίστες και να τις προσαρμόσει ανάλογα με τις προτιμήσεις του.

6.1.5 Συσκευή Anonymous Polling-Booth:

Ο T. Haines και ο X. Boyen ορίζουν επίσης μια δεύτερη παραλλαγή που δεν βασίζεται στην παραδοχή του διανοητικού υπολογισμού, καθιστώντας την πιο κατάλληλη για τους λιγότερο περίπλοκους διαγωνισμούς όπως η STV ή IRV. Για να επιτύχουν το απόρρητο της συσκευής, χωρίς προηγούμενα μυστικά κλειδιά και χωρίς να χρησιμοποιούν τους πνευματικούς υπολογισμούς των ψηφοφόρων, χρειάστηκαν να δημιουργήσουν μια συσκευή η οποία θα είναι ισχυρότερη από τα παραβάν που χρησιμοποιούμε στην παραδοσιακή ψηφοφορία και την ονομάζουν anonymous polling-booth. Αυτή η υπόθεση σημαίνει ότι οι συσκευές δεν έχουν κανένα μέσο για την αναγνώριση του ψηφοφόρου εκτός από τις πληροφορίες που περνούν μεταξύ τους. Ένας ψηφοφόρος ο οποίος αλληλοεπιδρά με τις συσκευές σε έναν εκλογικό θάλαμο το κάνει πάνω από ένα ανώνυμο untappable κανάλι.
Καμία νέα πληροφορία δεν αποκαλύπτεται στους γενικούς αντιπάλους, δεδομένου ότι τα χωριστά ψηφοδέλτια, που τώρα πρέπει να ξανακρυπτογραφηθούν και να ανακατευθούν, ήταν δημόσιες πληροφορίες στο αρχικό Prˆet a Voter. Μια εντελώς διεφθαρμένη αρχή, ή ένας εξωτερικός εισβολέας, μπορεί ακόμα να θέσει σε κίνδυνο το απόρρητο, αλλά μόνο εάν όλα τα μηχανήματα που χρησιμοποιεί ο ψηφοφόρος στο εκλογικό τμήμα είναι κατεστραμμένα

6.2 Μια ολοκληρωμένη εικόνα της λύσης τους

Η πρωταρχική τους τεχνική είναι να κρυπτογραφούν εκ νέου μια ψηφοφορία, είτε πριν είτε μετά τη συμπλήρωσή της, μέσα στο εκλογικό θάλαμο για να αποτρέψουν μεμονωμένα σημεία αποτυχίας για προστασία της ιδιωτικότητας. Μπορούν να το πραγματοποιήσουν αυτό επειδή το Prêt à Voter έχει ένα ψηφοδέλτιο που περιέχει μια λίστα υποψηφίων σε απλό κείμενο, ένα κρυπτογραφημένο στοιχείο και χώρο για να μπορέσουν οι ψηφοφόροι να καταγράψουν την ψήφο τους. Ο λόγος που πρέπει να κρυπτογραφηθεί εκ νέου είναι γιατί ένας επιτιθέμενος, ο οποίος έχει παραποιήσει τον εκτυπωτή, θα μπορούσε να χρησιμοποιήσει το μη αλλαγμένο κρυπτογραφημένο στοιχείο του ψηφοδελτίου και να καταφέρει να συσχετίσει την λίστα των υποψηφίων, η οποία εκτυπώνεται στον εκτυπωτή με την επιλογή των υποψηφίων που θα ανακοινωθούν στο Bulletin Board με αποτέλεσμα να παραβιάζεται η ιδιωτικότητα.

6.3 Προβλήματα και ανησυχίες

Ένα από τα προβλήματα με τη βελτίωση τους είναι η αύξηση του χρόνου και της πολυπλοκότητας της διαδικασίας ψηφοφορίας, η οποία συνάμα έχει και κόστος. Υποστηρίζουν ότι γενικά το κόστος αυτής της βελτίωσης είναι μικρότερο από το ποσό που δαπανήθηκε σε εκτυπωτές, EBM και σε σαρωτές. Δεδομένου ότι υπάρχουν συνήθως μόνο μερικά μεγάλα κόμματα σε μια χώρα και αρκετά μικρότερα κόμματα σε κάθε εκλογικό σώμα, ο χρόνος που αφιερώνεται σε ένα EBM είναι τάξεις μεγέθους υψηλότερες από εκείνες που απαιτούνται για τη σάρωση και ανάμιξη, ακόμη και αν όλα τα μεγάλα κόμματα είναι διατεθειμένα να προσφέρουν ένα μηχάνημα για να ανακατεύει τις ψήφους. Δεδομένου ότι ο αριθμός των μηχανημάτων ανακατέματος είναι μικρός και ο αριθμός των απαιτούμενων EBM είναι υψηλός, το σχετικό κόστος φαίνεται λογικό.

7.

Ηλεκτρονική ψηφοφορία – Παραδείγματα χωρών

Η ηλεκτρονική ψηφοφορία εφαρμόζεται σε διάφορες χώρες ανά τον κόσμο. Ορισμένες από αυτές είναι οι αναπτυγμένες, δηλαδή χώρες του Πρώτου Κόσμου, ενώ άλλες αναπτυσσόμενες δηλαδή χώρες του Δεύτερου Κόσμου. Σε αυτή την ενότητα παρουσιάζονται διάφορα παραδείγματα τόσο αναπτυγμένων όσο και αναπτυσσόμενων χωρών που έχουν υιοθετήσει είτε περιστασιακά είτε σταθερά τη χρήση της ηλεκτρονικής ψηφοφορίας έναντι της παραδοσιακής.

7.1 Αναπτυσσόμενες χώρες

7.1.1 Ηλεκτρονική ψηφοφορία στις αναπτυσσόμενες χώρες

Ο αναπτυσσόμενος κόσμος έχει αναφερθεί ότι έχει σημαντικά συμφέροντα στην τεχνολογία της ψηφοφορίας[56] και ότι ο ρυθμός της εφαρμογής της ηλεκτρονικής ψηφοφορίας είναι ταχύτερος σε αυτό από ό, τι στις ανεπτυγμένες χώρες[57]. Σε χώρες όπως η Νιγηρία, η ηλεκτρονική ψηφοφορία θεωρείται αναγκαιότητα[58] και ως η μόνη λύση για αξιόπιστες εκλογές[59]. Η Νιγηρία ξεκίνησε συζητήσεις για την εφαρμογή της ηλεκτρονικής ψηφοφορίας από το 2011 και αποφάσισε να προχωρήσει με την τεχνολογία[60]. Στη Νιγηρία, το παραδοσιακό σύστημα ψηφοφορίας θεωρήθηκε ότι επέτρεψε σημαντικές παρατυπίες και χαμηλότερο επίπεδο ακεραιότητας, υπευθυνότητας, διαφάνειας και παρακολούθησε διαφθορά, καταπιεστικές πράξεις και διοικητικές αποτυχίες[61]. Παρόμοιος ενθουσιασμός παρουσιάστηκε στην Ινδία, όπου η ηλεκτρονική ψηφοφορία θεωρήθηκε ότι ήταν σημαντικά πιο αξιόπιστη από την ψηφοφορία χαρτιού.

Ταυτόχρονα, υπάρχουν ορισμένα παραδείγματα αναπτυσσόμενων χωρών όπου η ηλεκτρονική ψηφοφορία δεν φαίνεται έγκαιρη στους πολίτες. Για παράδειγμα στη Βραζιλία η ηλεκτρονική ψηφοφορία προκαλεί περισσότερες ανησυχίες στην κοινή γνώμη. Παρόλο που στη Βραζιλία η εφαρμογή της ηλεκτρονικής ψηφοφορίας αποφασίστηκε και ολοκληρώθηκε με επιτυχία το 2000[62] συνεχίζει να υπάρχει έλλειψη εμπιστοσύνης του κοινού στο σύστημα[63]. Στην περίπτωση της Βραζιλίας η ηλεκτρονική ψηφοφορία απέτυχε να βελτιώσει τη συμμετοχή του κοινού παρά τις τεράστιες επενδύσεις που έγιναν στο σύστημα. Έχουν αναφερθεί επίσης κριτικές σχετικά με την απόφαση της κυβέρνησης να χρησιμοποιήσει αυτήν την τεχνολογία, δεδομένου ότι εκατομμύρια Βραζιλιάνοι εξακολουθούν να υποφέρουν από φτώχεια και αναλφαβητισμό[64,65]. Η απόφαση θεωρήθηκε ως καθοδηγούμενη από την αγορά και τα συμφέροντα των ανώτερων κοινωνικών τάξεων αφού η γνώση στη χρήση των ηλεκτρονικών μηχανημάτων ψηφοφορίας και των τεχνολογιών πληροφοριών και επικοινωνιών των πολιτών που ανήκουν στα κατώτερα στρώματα δεν ήταν επαρκής όσον αφορά τη στρατηγική για τις τεχνολογίες πληροφοριών και επικοινωνιών[66].

Ο Khan και οι συνεργάτες[67]του πρότειναν ότι η επιτυχία υλοποίησης ψηφοφορίας με ηλεκτρονικά συστήματα εξαρτάται από την ταυτόχρονη διαμόρφωση των τεχνικών, οργανωτικών και κοινωνικών πτυχών των συστημάτων. Η τεχνική πτυχή αφορά τον τρόπο με τον οποίο η τεχνολογία χρησιμοποιείται για την εγκαθίδρυση των συστημάτων, ενώ το οργανωτικό και κοινωνικό σύστημα δίνει έμφαση στις ανάγκες κατανόησης των νοοτροπιών, δεξιοτήτων και αξιών, καθώς και των σχέσεων μέσα στην οργανωτική δομή της κοινωνίας[68].Αυτή η αντίληψη θεωρεί ότι η τεχνολογία της πληροφορίας δεν είναι απλώς ένα εργαλείο το οποίο είναι άμεσα εφαρμόσιμο σε οποιοδήποτε δεδομένο πλαίσιο για οποιονδήποτε συγκεκριμένο σκοπό. Αλλά θεωρείται ως ένας σύνθετος κοινωνικό - τεχνικός παράγοντας του οποίου οι συσχετιστικές αλληλεπιδράσεις με άλλους κοινωνικούς παράγοντες είναι σημαντικές για την κατανόηση του τρόπου της λειτουργίας αυτής της τεχνολογίας[69].

Η τεχνολογία έχει μικρό μόνο αντίκτυπο στη διαμόρφωση των ανθρώπινων προθέσεων και επιλογών και, ως εκ τούτου, οι επιπτώσεις που συνδέονται με την εφαρμογή ηλεκτρονικής ψηφοφορίας μπορούν να αποδοθούν στην ανθρώπινη υπηρεσία που διαμορφώνεται από το κοινωνικό πλαίσιο[70].

Αυτό δεν σημαίνει ότι μπορούν να αγνοηθούν οι τεχνικές λύσεις για τα συστήματα ηλεκτρονικής ψηφοφορίας. Αλλά η έμφαση δίνεται στον τρόπο με τον οποίο οι κοινωνικές και οργανωτικές πτυχές θα πρέπει να θεωρούνται εξίσου καθοριστικές, για την επιτυχία της ηλεκτρονικής ψηφοφορίας[71]. Στην επιστημονική κοινότητα έχει αναφερθεί ότι η χρήση της τεχνολογίας στις εκλογές ενδέχεται να αποτύχει να βελτιώσει τη συμμετοχή του κοινού λόγω κοινωνικό-τεχνικών κενών. Ο Al Shammari και οι συνεργάτες του[72] επισημαίνουν τρεις διαστάσεις ανισοτήτων σχετικά με τις εφαρμογές της ηλεκτρονικής ψηφοφορίας. Πρώτον, είναι το τεχνολογικό χάσμα που προκαλείται από την ασυμβατότητα μεταξύ των συστημάτων - τόσο του υλικού όσο και του λογισμικού. Ακολουθεί το κοινωνικό χάσμα μεταξύ κοινωνικών πολιτικών και της ανθρώπινης συμπεριφοράς που αντιπροσωπεύει ηθικές αποκλίσεις μεταξύ των χρηστών, μεταξύ των χρηστών και των κοινωνικών αξιών, καθώς και μεταξύ του δημοκρατικού πολιτισμού και των εκλογικών πρωτοκόλλων[73].Η τελευταία διάσταση είναι το κοινωνικό-τεχνικό χάσμα που προκαλείται από τις ανισότητες μεταξύ κοινωνικών πολιτικών και ηλεκτρονικών υπολογιστών. Επομένως, για τα συστήματα ηλεκτρονικής ψηφοφορίας, ο κοινωνικός κόσμος και η τεχνολογία που χρησιμοποιείται σε αυτό δεν μπορούν να θεωρηθούν χωριστά, αλλά είναι συνδεδεμένα μεταξύ τους[74].

Στη συνέχεια, έχει αναφερθεί ότι οι αιτίες των αποτυχιών στην εφαρμογή της εκλογικής τεχνολογίας πληροφοριών συνδέονται όχι μόνο με τις τεχνολογικές πτυχές των συστημάτων αλλά και με το οργανωτικό πλαίσιο στο οποίο χρησιμοποιούνται[75,76]. Μολονότι ένας από τους κύριους στόχους της χρήσης της τεχνολογίας στις εκλογές είναι η βελτίωση της δημοκρατίας μέσω της αύξησης της συμμετοχής των ψηφοφόρων[77]. Στην πράξη η ηλεκτρονική ψηφοφορία σπάνια φαίνεται να έχει κοινωνική χρησιμότητα. Πρέπει να σημειωθεί ότι η ηλεκτρονική ψηφοφορία υιοθετείται συχνά για να αποφευχθεί η γραφειοκρατία[78].

Όταν αποτυγχάνει η ηλεκτρονική ψηφοφορία, αυτό ενδέχεται να οφείλεται σε διάφορους λόγους. Συχνά οι αποτυχίες προέρχονται από την έλλειψη πόρων[79,80] ή την υπερβολική εξάρτηση των κυβερνήσεων από τον ιδιωτικό τομέα[81,82]. Ένας λόγος μπορεί να είναι εξαιτίας της έλλειψης τεχνογνωσίας στον τομέα των τεχνολογιών της πληροφορικής. Η απόφαση για το κατά πόσον μια χώρα πρέπει να εφαρμόσει ή όχι μια ηλεκτρονική ψηφοφορία δεν είναι ανεξάρτητη από τις πολιτικές συνέπειες και το

ερώτημα πρέπει να είναι για ποιον λόγο οι κυβερνήσεις των χωρών αυτών θέλουν να χρησιμοποιήσουν την ηλεκτρονική ψηφοφορία[83].

7.1.2 Προτάσεις για τις αναπτυσσόμενες χώρες

Μελέτες σχετικές με την κοινωνία της ηλεκτρονικής ψηφοφορίας στις αναπτυσσόμενες χώρες έδωσαν μεγαλύτερη έμφαση στην εξέταση της αποδοχής των πολιτών και της στάσης τους απέναντι στην τεχνολογία.
Οι ερευνητές προσπαθούν να εντοπίσουν τη δυνατότητα εφαρμογής των εννοιών της ηλεκτρονικής ψηφοφορίας και των θεωρητικών δομών στα διάφορα πλαίσια των αναπτυσσόμενων δημοκρατιών. Αυτές οι έρευνες μπορούν να θεωρηθούν ως μια προσπάθεια να απαντηθούν οι προκλήσεις που προκύπτουν κατά τη διάρκεια αρκετών περιπτώσεων εφαρμογής της ηλεκτρονικής ψηφοφορίας, κυρίως στη Λατινική Αμερική, όπου η εκλογική τεχνολογία θεωρείται ως κοινωνικός πράκτορας που αλληλοεπιδρά και τροποποιεί αμοιβαία τους πολιτικούς, οικονομικούς και άλλους κοινωνικούς παράγοντες. Οι ανησυχίες για τη διαδικασία λήψης αποφάσεων και την εμπιστοσύνη του κοινού, έχουν επισημανθεί τονίζοντας τους συσχετισμούς μεταξύ της ηλεκτρονικής ψηφοφορίας και των πολιτών. Υπήρχε μια υπόθεση ότι η εκλογική τεχνολογία συμβάλλει σε αλλαγές στις κοινωνικές, οικονομικές και πολιτικές δομές, είτε θετικές είτε αρνητικές, οι οποίες πρέπει να αντιμετωπιστούν σωστά για να διασφαλιστούν ομαλές μεταβάσεις ως συνέπεια των πρωτοβουλιών υιοθέτησης της ηλεκτρονικής ψηφοφορίας
Πρέπει να δοθεί έμφαση σε συγκεκριμένες μελέτες σχετικά με το πώς οι υγιείς βιομηχανίες της κάθε χώρας θα διέθεταν τις υποδομές για την ηλεκτρονική ψηφοφορία των αναπτυσσόμενων χωρών για να εξαλείψουν τις τεχνολογικές και πολιτικές τους εξάρσεις από την ξένη δύναμη και να διατηρήσουν τον έλεγχό τους στη δημοκρατία. Η ηλεκτρονική ψηφοφορία, ως εκ τούτου, δεν πρέπει να θεωρείται απλό τεχνολογικό μέσο, αλλά ένας σύνθετος κοινωνικό-τεχνικός παράγοντας που συμβάλλει στις κοινωνικές και πολιτικές μεταρρυθμίσεις. Επιπλέον, πρέπει να γίνουν περισσότερες έρευνες που να επισημαίνουν τη δημόσια εκπαίδευση για τη βελτίωση των ηλεκτρονικών δεξιοτήτων των ψηφοφόρων και να προσκαλέσουν ουσιαστικά

σχόλια για ρυθμίσεις ηλεκτρονικής ψηφοφορίας που ταιριάζουν περισσότερο στα δημογραφικά χαρακτηριστικά των ψηφοφόρων.

Μια τέτοια υπόθεση, ότι οι τεχνολογίες διαδραματίζουν σημαντικό ρόλο στις αναπτυσσόμενες χώρες, ήταν ακόμη πιο εμφανής σε τεχνολογικές μελέτες. Οι αδυναμίες που σημειώθηκαν κατά τη διάρκεια προηγούμενων δημοκρατικών πρακτικών θα μπορούσαν να είχαν οδηγήσει σε τεχνολογικό ντετερμινισμό από χώρες όπως η Νιγηρία και η Ινδία. Μία λύση για αυτό το θέμα θα μπορούσε να είναι ο εξοπλισμός της δημοκρατίας με την τεχνολογική πρόοδο, αλλά θα παρουσίαζε ένα σημαντικό κενό στην αντιμετώπιση ζητημάτων που σχετίζονται με τις αυξανόμενες τεχνολογικές περιπλοκές. Ενώ θέματα ψηφοφορίας μέσω κινητής τηλεφωνίας και της ασφάλειας πληροφοριών ήταν δημοφιλή μεταξύ των ερευνητών, υπήρχε απουσία μελετών σχετικά με τα πρότυπα τεχνολογίας ηλεκτρονικής ψηφοφορίας, τη συμμόρφωση και τη διακυβέρνηση, για παράδειγμα, που μπορεί αργότερα να προκαλέσουν οπισθοδρόμηση στην πρόοδο της ανάπτυξης της ηλεκτρονικής ψηφοφορίας. Επιπλέον, ο τεχνολογικός κεντρισμός θα πρέπει να περιορίζεται ώστε να επιτρέπει μια κατάσταση ισοτιμίας μεταξύ των θεμάτων. Τα ζητήματα που σχετίζονται με την οργάνωση έχουν παραμεληθεί σε μεγάλο βαθμό, γεγονός που μπορεί να έχει ως αποτέλεσμα η κυβέρνηση να δυσκολεύεται να προσδιορίσει τη συνάφεια της θέσπισης τεχνολογικών πλεονεκτημάτων έναντι των αναμενόμενων κενών πραγματικού μοντέλου εφαρμογής. Οι μελλοντικές έρευνες σχετικά με την ηλεκτρονική ψηφοφορία στις αναπτυσσόμενες χώρες, πιστεύεται αλλά και αναμένεται να εξετάσουν περαιτέρω τον περίπλοκο χαρακτήρα των εφαρμογών ηλεκτρονικής ψηφοφορίας και τις επιπτώσεις τους στους οργανισμούς του δημόσιου τομέα. Πρέπον θα ήταν να εξετάσουν προσεκτικά τα κίνητρα πίσω από τις πρωτοβουλίες της ηλεκτρονικής ψηφοφορίας, να ορίσουν με σαφήνεια την ιδιοκτησία του συστήματος και να προσδιορίσουν χωρίς ασάφεια όλες τις απαραίτητες θεσμικές ρυθμίσεις. Υπάρχουν επίσης ζητήματα μεταρρυθμίσεων του δημόσιου τομέα και κατάρτισης δημοσίων υπαλλήλων που πρέπει να αντιμετωπιστούν προκειμένου να διασφαλιστεί ότι δεν θα υπάρξουν προβλήματα ασυνέχειας, ασάφειας και άλλων προβλημάτων.

Η αποτυχία εκτέλεσης έργων ηλεκτρονικής ψηφοφορίας στις περισσότερες αναπτυσσόμενες χώρες οφείλεται κυρίως στην έλλειψη πολιτικής δέσμευσης και στο χαμηλότερο επίπεδο διαθέσιμων πόρων. Τέτοιες καταστάσεις πιθανότατα θα

προκαλέσουν αλλαγές στις πολιτικές και στρατηγικές ατζέντες των χωρών, δημιουργώντας μια κατάσταση ακατάλληλη για μεγάλες και μακροπρόθεσμες επενδύσεις στην ανάπτυξη της τεχνολογίας των πληροφοριών και επικοινωνιών (ΤΠΕ / ICT). Οι ερευνητές της ηλεκτρονικής ψηφοφορίας ενδέχεται να δυσκολεύονται περαιτέρω να διατηρήσουν τα ενδιαφέροντά τους στον τομέα, καθώς η έρευνά τους θα έχει στο τέλος λίγο πρακτικό αντίκτυπο. Αυτό είναι εμφανές από τον μικρό αριθμό ερευνών που έχουν διεξαχθεί όλα αυτά τα χρόνια και από το μικρό πλήθος των άρθρων που αποτελούνται. Οι κυβερνήσεις των αναπτυσσόμενων χωρών και ο ακαδημαϊκός κόσμος, πρέπει να εργαστούν για έναν κοινό στόχο και να ενσωματώσουν μια ολοκληρωμένη άποψη καθώς και οι δυο πλευρές αντιλαμβάνονται την ανάπτυξη της ηλεκτρονικής ψηφοφορίας προκειμένου να επωφεληθούν από την τεχνολογία.

7.2. Ηλεκτρονική ψηφοφορία στον Καναδά

Οι ομοσπονδιακές και επαρχιακές εκλογές στον Καναδά διεξάγονται με την παραδοσιακή ψηφοφορία, αλλά η ηλεκτρονική ψηφοφορία χρησιμοποιείται τουλάχιστον από τη δεκαετία του 1990 σε μερικούς δήμους της χώρας. Σήμερα τα συστήματα ψηφοφορίας με οπτική σάρωση είναι κοινά στις δημοτικές εκλογές στον Καναδά[84]. Οι τοπικές κυβερνήσεις τείνουν να έχουν πιο σύνθετες ψηφοφορίες με μεγαλύτερο αριθμό υποψηφίων, γεγονός που μπορεί να αποτελέσει την διαδικασία καταμέτρησης χρονοβόρα, δύσκολη και δαπανηρή για να πραγματοποιείται με τον παραδοσιακό τρόπο. Από τη δεκαετία του 1990, η τεχνολογία καταμέτρησης των ψηφοφοριών έχει βελτιώσει την ταχύτητα και την ακρίβεια των μετρήσεων και έχει προσφέρει την εξοικονόμηση κόστους εργασίας σε πολλές τοπικές δικαιοδοσίες. Δεν προκαλεί έκπληξη το γεγονός ότι οι καναδικοί δήμοι ήταν ηγέτες στην εισαγωγή της ηλεκτρονικής ψηφοφορίας. Η ψηφοφορία μέσω διαδικτύου δοκιμάστηκε για πρώτη φορά από επιλεγμένους δήμους του Οντάριο το 2003 , με αποτέλεσμα 44 δήμοι του Οντάριο να χρησιμοποιούν σήμερα την τεχνολογία αυτή. Το Χάλιφαξ και τρεις πόλεις της Νέας Σκωτίας δοκίμασαν έναν συνδυασμό ψηφοφορίας μέσω διαδικτύου και τηλεφώνου στις εκλογές του δημοτικού και του σχολικού συμβουλίου του 2008,

επίσης το Χάλιφαξ χρησιμοποίησε ξανά την ψηφοφορία μέσω διαδικτύου σε εκλογές του 2009[85].

Δεν λείπουν οι αντιρρήσεις για την ηλεκτρονική ψηφοφορία στις εθνικές εκλογές. Ορισμένοι δήμοι στο Οντάριο και στη Νέα Σκοτία εφαρμόζουν την ηλεκτρονική ψηφοφορία και πρέπει να επισημανθεί ότι δεν υπάρχουν καναδικά πρότυπα ηλεκτρονικής ψηφοφορίας[86]. Οι εκθέσεις και οι αναλύσεις των επιτροπών από τη Νέα Σκωτία, το Νέο Brunswick, το Κεμπέκ, το Οντάριο και τη Βρετανική Κολούμπια συνιστούσαν όλες να μην προχωρήσουν σε επαρχιακές εκλογές με ηλεκτρονική ψηφοφορία.

Παρόλες τις προειδοποιήσεις από τους ερευνητές της ασφάλειας της ηλεκτρονικής πλατφόρμας ψηφοφορία, το Οντάριο ασκεί πίεση στους δήμους του να ενσωματώσουν την ηλεκτρονική ψηφοφορία. Η επαρχία απαιτούσε, οι δήμοι της να ψηφίσουν ένα νόμο που θα επιτρέπει την ηλεκτρονική ψηφοφορία μέχρι την 1η Μαΐου 2017, ώστε να επιτρέπεται η ηλεκτρονική ψηφοφορία στις δημοτικές εκλογές του 2018, σύμφωνα με την CBC.

Το Οντάριο έχει πάνω από 400 δήμους. Επομένως έχει και προσεγγιστικά 400 διαφορετικά συμβόλαια και διαφορετικά διαδικτυακά συστήματα ψηφοφορίας τα οποία έχουν δημιουργηθεί από διαφορετικούς παρόχους. Η επαρχία του Οντάριο δεν θέτει πρότυπα για την ηλεκτρονική ψηφοφορία και πρότυπα ασφαλείας, ούτε γνωρίζει ποιοι δήμοι χρησιμοποιούν ηλεκτρονική ψηφοφορία και ποιοι όχι.

"Οι δήμοι δεν υποχρεούνται να ενημερώσουν το υπουργείο για τις μεθόδους ψηφοφορίας που θα χρησιμοποιήσουν", έγραψε ένας εκπρόσωπος του Υπουργείου Δημοσίων Υποθέσεων του Οντάριο. Οι δήμοι του Οντάριο έχουν εντάξει την ηλεκτρονική ψηφοφορία από το 2003, σύμφωνα με το υπουργείο, και 98 δήμοι προσέφεραν ηλεκτρονική ψηφοφορία στις εκλογές του 2014.

7.3 Ηλεκτρονική ψηφοφορία στην Αυστραλία

Οι εκλογές του κράτους της Νέας Νότιας Ουαλίας το 2015 πραγματοποιήθηκαν με διαδικτυακή ψηφοφορία, η οποία αποδείχθηκε αρκετά ανασφαλής, σε βαθμό που

γεννά αμφιβολίες για τα αποτελέσματα των εκλογών, έχοντας υποψίες πως μία θέση στο κοινοβούλιο αποφασίστηκε με ψευδείς ψήφους. Η εκλογική επιτροπή προσπάθησε να αποφύγει την ενημέρωση που έγινε από την Dr. Teague και την ομάδα της σχετικά με τα θέματα ασφάλειας της διαδικασίας που ακολουθούν. Ένα χρόνο αργότερα, προχώρησε στην αποκάλυψη του κυριότερου προβλήματος , σχετικά με την θέση στο κοινοβούλιο η οποία είναι αμφίβολη, μετά από στενή διερεύνηση στο κρατικό κοινοβούλιο.

Η ερευνήτρια Teague έχει επιδείξει δύο φορές τις αδυναμίες ασφαλείας στα ηλεκτρονικά συστήματα ψηφοφορίας που χρησιμοποιούνται στις κρατικές εκλογές στην Αυστραλία. Συμπεριλαμβανομένης της δημοκρατικής εκλογής του New South Wales (NSW) , με 280.000 ψήφους να έχουν πραγματοποιηθεί μέσω του διαδικτύου (μιας από τις μεγαλύτερες ηλεκτρονικές ψηφοφορίες).

Πριν από την εκλογή, η κρατική εκλογική επιτροπή δήλωσε στην Αυστραλιανή Ραδιοφωνία (ABC) ότι «η ψήφος των πολιτών είναι απόλυτα μυστική . Είναι κρυπτογραφημένη και προστατευμένη, δεν μπορεί να παραβιαστεί». Ωστόσο, οι ερευνητές χρειάστηκαν μόνο λίγες μέρες για να εντοπίσουν τα ελαττώματα στην ηλεκτρονική εφαρμογή για την διαδικτυακή ψηφοφορία, η οποία θα μπορούσε εύκολα να χρησιμοποιηθεί για την κατασκοπεία και την τροποποίηση κάθε διαδικτυακής ψηφοφορίας και να το κάνει ανυπόστατα.

Όπως αναφέρει η Δρ. Teague «Ο βασικότερος στόχος της ασφάλειας των ηλεκτρονικών συστημάτων ψηφοφορίας είναι να μην υποστεί το σύστημα τροποποίηση ή κατασκοπεία από τρίτους, όμως στην προκυμμένη περίπτωση είναι εύκολό να παρακαμφθεί ο στόχος αυτός. Καθώς δεν υπήρξαν προειδοποιήσεις στον browser και ένας κακόβουλος κατάφερε να συνδεθεί με TLS σύνδεση, με αποτέλεσμα να δείχνει ίδια με μια νόμιμη ψηφοφορία αλλά με την παρέμβασή ενός κακόβουλου με το δικαίωμα παρακολούθησης αλλά και τροποποίησης των ψήφων»

Η Teague και η ομάδα της ανέφεραν στην έρευνά τους στο CERT της Αυστραλίας, πως κατά την διάρκεια της αποκατάστασης του συστήματος και ενίσχυσης της ασφάλειας 66,000 ψηφοφόροι είχαν ολοκληρώσει την διαδικασία. Όπου για την εκλογή ενός ατόμου στο Νομοθετικό Συμβούλιο της Νέας Νότιας Ουαλίας χρειάζονται 3,177 ψήφοι Μετά τις εκλογές, η NSW(Νέας Νότιας Ουαλίας) εκλογική επιτροπή αρχικά δημοσίευσε ότι δεν υπήρξε κανένα τεχνικό πρόβλημα κατά την χρήση της ηλεκτρονικής εκλογικής

πλατφόρμας. Μετά την πάροδο ενός έτους ωστόσο, όταν ερωτήθηκαν στη βουλή, παραδέχτηκαν ότι υπήρξαν πολλές σοβαρές δυσλειτουργίες που αναφέρθηκαν από τους χρήστες/ψηφοφόρους. Περισσότεροι από 600 ψηφοφόροι που προσπάθησαν να επιβεβαιώσουν την ψήφο τους με το τηλεφωνικό σύστημα δεν τα κατάφεραν, γιατί ούτε αυτό λειτούργησε σωστά. Ένα ποσοστό αποτυχούς κατάθεσης ψήφων που αγγίζει το 10% , είναι παραπάνω από αρκετό για να αμφισβητηθεί το τελικό εκλογικό αποτέλεσμα.

Παρόλα αυτά, η κυβέρνηση της NSW συνεχίζει απρόσκοπτα, αγνοώντας τους όποιους κινδύνους έχουν ήδη εμφανιστεί. «Η NSW εκλογική επιτροπή σκόπευε να διαθέσει το iVote ως ηλεκτρονικό εκλογικό σύστημα για τις γενικές NSW βουλευτικές εκλογές 2019.» ανέφερε εκπρόσωπος του σωματείου της NSW. Όπως και έγινε πραγματικότητα σύμφωνα με τον επίσημο ιστότοπο[87] (Commission, 2019). Αδυνατώντας να αντιληφθεί τους κινδύνους που καραδοκούν κατά την χρήση της ηλεκτρονικής ψηφοφορίας, η εκλογική επιτροπή φθάνοντας στα άκρα, αποκάλεσε την Teague και τον συνάδελφό της, Alex Halderman ,από το Πανεπιστήμιο του Μίσιγκαν, «αντί-διαδικτυακούς και πολέμιους της ηλεκτρονικής ψηφοφορίας» ανταπαντώντας στις δηλώσεις τους το 2015, που κατά την έρευνά τους, αμφισβήτησαν την ασφάλεια και την εγκυρότητα των εκλογικών αποτελεσμάτων. Αξίζει να σημειωθεί, ότι νωρίτερα την ίδια εβδομάδα πριν τις δηλώσεις τους, η κυβέρνηση NSW υπέγραψε για δεύτερη φορά συμβόλαιο με την Scytl, την εταιρεία που τους μεταπώλησε το ηλεκτρονικό σύστημα ψηφοφορίας που προκάλεσε το φιάσκο του 2015, σύμφωνα με την Computer world Australia.

Καθώς η ηλεκτρονική αυτή πλατφόρμα ψηφοφορίας, σχεδιασμένη από την ισπανική εταιρεία Scytl, δεν είναι ανοιχτού πηγαίου κώδικα, άρα δεν είναι και διαθέσιμη προς εξέταση, οι τεχνικοί αδυνατούσαν να ελέγξουν την λειτουργικότητα της εφαρμογής πριν τις εκλογές. Αντιθέτως, μόνο μετά την έναρξη των εκλογών και αφότου ξεκίνησε να λειτουργεί το ηλεκτρονικό σύστημα ψηφοφορίας κατάφεραν να εξετάσουν το τμήμα του συστήματος που απευθύνονταν στο κοινό.

7.4 Ηλεκτρονική ψηφοφορία στην Ευρώπη

Οι ευρωπαϊκές χώρες είναι οι πιο προηγμένες στον κόσμο όσον αφορά την ηλεκτρονική ψηφοφορία. Η Εσθονία, η Ελβετία, η Γαλλία, η Γερμανία, η Ισπανία, οι Κάτω Χώρες και το Ηνωμένο Βασίλειο δοκίμασαν την ηλεκτρονική ψηφοφορία μέσω ηλεκτρονικού ταχυδρομείου. Η Νορβηγία πραγματοποίησε τοπικές κυβερνητικές εκλογές σε ορισμένους δήμους με δυνατότητα ηλεκτρονικής ψηφοφορίας για πρώτη φορά τον Σεπτέμβριο του 2011 και πρόσφερε ψηφοφορία σε εθνικό επίπεδο μέσω του διαδικτύου έως το 2017[88].

7.4.1 Ηλεκτρονική ψηφοφορία ανά χώρα

7.4.1.1 Ηλεκτρονική ψηφοφορία στην Ελβετία

Ήδη από το 1982, το ελβετικό Κοινοβούλιο ψήφισε μια νομοθεσία που επιτρέπει πειραματισμό με εναλλακτικές μεθόδους ψηφοφορίας στο καντόνι της Γενεύης. Αργότερα, το 2008, το Κοινοβούλιο ενέκρινε μια συνταγματική τροπολογία που επιτρέπει την ψηφοφορία μέσω του διαδικτύου, η οποία επικυρώθηκε από τους πολίτες το 2009.

Η ηλεκτρονική ψηφοφορία στην Ελβετία ξεκίνησε το 2003 στην Γενεύη, όπου οι κάτοικοι της Ανιέρας ψήφισαν χρησιμοποιώντας το Διαδίκτυο. Αυτή ήταν η πρώτη δοκιμή ηλεκτρονικής ψηφοφορίας στην Ελβετία[89]. Τα επόμενα χρόνια, ο αριθμός των ατόμων που μπορούσαν να χρησιμοποιήσουν την ηλεκτρονική ψηφοφορία αυξήθηκε καθώς όλο και περισσότερες πόλεις άρχισαν να υιοθετούν ένα τέτοιο σύστημα[90].

Η ελβετική κυβέρνηση έχει πολλαπλούς λόγους για τη χρήση ηλεκτρονικής ψηφοφορίας. Μπορεί να μειώσει το κόστος και να αυξήσει την ταχύτητα καταμέτρησης των ψήφων, ο Ελβετός που ζει στο εξωτερικό μπορεί να ψηφίσει πιο αξιόπιστα. Θα μπορούσε επίσης να συμβάλει στην αύξηση της προσέλευσης των ψηφοφόρων (που μειώνεται από τη δεκαετία του 1970[91]), καθώς η ψηφοφορία μέσω του Διαδικτύου θεωρείται από τους περισσότερους ως η πιο βολική[92].

Υπάρχουν πολλά ηλεκτρονικά συστήματα ψηφοφορίας που χρησιμοποιούνται στη χώρα, ιδίως το CHVote (λογισμικό ανοιχτού κώδικα που αναπτύχθηκε από τη Γενεύη) και το sVote (από την Swiss Post, ιδιόκτητο λογισμικό που αναπτύχθηκε από τη Scytl). Το 2019, προέκυψαν ανησυχίες σχετικά με την ασφάλεια της ηλεκτρονικής ψηφοφορίας. Μια επιτροπή πολιτικών και ειδικών σε υπολογιστές ξεκινά μια πρωτοβουλία των πολιτών με στόχο την απαγόρευση της διαδικτυακής ψηφοφορίας για τουλάχιστον πέντε χρόνια έως ότου το σύστημα αποδειχθεί ασφαλές[93]. Η διαμάχη αναπτύχθηκε αφού ερευνητές από το Πανεπιστήμιο της Μελβούρνης ανακάλυψαν ότι το σύστημα της Swiss Post είχε ένα ελάττωμα ασφαλείας.
Οι προϋποθέσεις που άνοιξαν το δρόμο για την ψηφοφορία μέσω διαδικτύου στη Γενεύη υπήρξαν:

- Η έμφαση στην άμεση δημοκρατία που επιτρέπει στους πολίτες να ψηφίζουν τέσσερις έως έξι φορές το χρόνο
- Η επιθυμία για βελτίωση της συμμετοχής
- Η εμπειρία σε εξ ’αποστάσεως ψηφοφορία μέσω ενός καθιερωμένου συστήματος ταχυδρομικής ψηφοφορίας
- Το υψηλό επίπεδο πρόσβασης στο διαδίκτυο
- Η κεντρική λίστα ηλεκτρονικών ψηφοφόρων
- Ο μεγάλος πληθυσμός που ζει στο εξωτερικό
- Η τεχνολογικά προοδευτική κυβέρνηση

Το καντόνι της Γενεύης υιοθέτησε την ηλεκτρονική ψηφοφορία μέσω διαδικτύου το 2001 και στη συνέχεια επεκτάθηκε η ηλεκτρονική ψηφοφορία σε πολλά άλλα καντόνια στην Ελβετία. Η εφαρμογή της ηλεκτρονικής ψηφοφορίας στη Γενεύη αρχικά περιορίζονταν σε δημοψηφίσματα, ενώ στη συνέχεια επεκτάθηκαν στις εκλογές[94].Η Γενεύη διεξήγαγε τον μεγαλύτερο αριθμό εκλογών με ψηφοφορία μέσω του διαδικτύου ως επιλογή στον κόσμο[95].

Χρήση της ηλεκτρονικής ψηφοφορίας

Το επιχείρημα ότι η ψηφοφορία μέσω Διαδικτύου θα αύξανε την προσέλευση των ψηφοφόρων χρησιμοποιήθηκε συχνά στις κοινοβουλευτικές συζητήσεις από τους υποστηρικτές της. Επίσης, η υψηλή χρήση θα δικαιολογούσε το υψηλό χρηματοοικονομικό κόστος και τους κατανεμημένους πόρους που θα

χρησιμοποιούσαν. Για να παρακολουθούν τα ποσοστά χρήσης των ψήφων μέσω Διαδικτύου, δημιουργήθηκε μια βάση δεδομένων που ανέφερε αποτελέσματα λεπτομερώς από την πρώτη ψηφοφορία το 2003[96].

Μελέτες σχετικά με την εξέλιξη των ποσοστών των χρηστών της ηλεκτρονικής ψηφοφορίας στις τρείς πιλοτικές επαρχίες καταγράφουν δύο βασικά κοινωνικά αποτελέσματα που εξηγούν τον τρόπο χρήσης με την πάροδο του χρόνου, την καινοτομία και την παροχή μεγαλύτερης ευκολίας. Η Γενεύη και η Ζυρίχη απεικονίζουν το φαινόμενο της καινοτομίας, όπου παρατηρούνται δραστικές πτώσεις στα ποσοστά χρήσης αμέσως μετά την εφαρμογή της. Αυτή η πτώση μπορεί να οφείλεται σε ορισμένους ψηφοφόρους που δοκιμάζουν το νέο σύστημα ψηφοφορίας λόγω περιέργειας, αλλά στη συνέχεια επιστρέφουν στη παραδοσιακή μέθοδο ψηφοφορίας λόγω των συνηθειών τους. Στην περίπτωση της Γενεύης, απεικονίζεται στα ποσοστά χρήσης η δυσμενής επίδραση της μακροπρόθεσμης διακοπής της ηλεκτρονικής ψηφοφορίας (μεταξύ 2005 και 2009). Πριν από τη διακοπή, το ποσοστό ήταν 20% και στη συνέχεια ήταν μόνο 15%. Γενικά, η ευκολία της ψηφοφορίας μέσω ταχυδρομείου έχει διατηρήσει τα επίπεδα ψηφοφορίας στο Διαδίκτυο χαμηλά. Ωστόσο, εικάζεται ότι θα αυξηθούν τελικά καθώς οι νεότεροι ψηφοφόροι έχουν την τάση να χρησιμοποιούν το Διαδίκτυο. Το γεγονός ότι οι ψηφοφόροι στο Neuchatel πρέπει πρώτα να εγγραφούν στο δήμο για να αποκτήσουν πρόσβαση στην ηλεκτρονική διακυβέρνηση είχε ως αποτέλεσμα την έλλειψη ευκολίας. Ωστόσο, παρατηρείται μικρή αύξηση της ηλεκτρονικής ψηφοφορίας το 2011, η οποία μπορεί να εξηγηθεί με την εισαγωγή της δυνατότητας για ηλεκτρονική υποβολή φόρων μέσω της ηλεκτρονικής διακυβέρνησης, η οποία φαίνεται να προσελκύει ορισμένους πολίτες με σκοπό να προσπαθήσουν να χρησιμοποιήσουν την ψηφοφορία μέσω Διαδικτύου .

Τα ποσοστά χρήσης των ομογενών έχουν ρυθμό ανάπτυξης 2% κάθε χρόνο. Στο Neuchatel, η απαίτηση εγγραφής αυτοπροσώπως για χρήση του συστήματος ηλεκτρονικής διακυβέρνησης στον δήμο είχε ως αποτέλεσμα χαμηλότερα ποσοστά, καθώς αυτό είναι ακόμη δυσκολότερο για όσους ζουν στο εξωτερικό. Μελέτες δείχνουν επίσης ότι η Γενεύη έχει χαμηλότερα ποσοστά από τις υπόλοιπες πόλεις, τα οποία θεωρείται ότι οφείλονται στους «ψεύτικους» ομογενείς που ζουν κοντά στα σύνορα στη Γαλλία για να αποφύγουν τις τιμές των κατοικιών στη Γενεύη.

Τα δύο κύρια συμπεράσματα που μπορούν να εξαχθούν από αυτές τις μελέτες είναι:

- Τα ποσοστά προσέλευσης έχουν μια σχετική άνοδο λόγω τις διευκόλυνσης που προσφέρει η ηλεκτρονική ψηφοφορία
- Με την πάροδο των ετών η διαδικτυακή ψηφοφορία έχει κερδίσει το ενδιαφέρον των Ελβετών ομογενών σε αντίθεση με τους Ελβετούς κατοίκους που τείνουν να εγκαταλείπουν τον νέο τρόπο ψηφοφορίας.

Η ηλεκτρονική ψηφοφορία παρέχει μεγάλη ευκολία καθώς αποτελεί μια διαδικασία ανεξάρτητη από τόπο και χρόνο. Μπορεί δηλαδή ο ψηφοφόρος να υποβάλει την ψήφο του οποιαδήποτε στιγμή από οποιοδήποτε σημείο. Με αυτό το πλεονέκτημα συνάμα γεννιέται και η αύξηση της συμμετοχής καθώς προσφέρει στους ανθρώπους έναν εναλλακτικό τρόπο ψηφοφορίας για εκείνους που μπορεί να μην είναι σε θέση να χρησιμοποιήσουν τον παραδοσιακό τρόπο. Αυτό μπορεί να αφορά κυρίως απόντες, ασθενείς, άτομα με ειδικές ανάγκες ή ηλικιωμένους πολίτες. Επίσης, το άρθρο 6 του ομοσπονδιακού νόμου για τα πολιτικά δικαιώματα ορίζει ότι οι αποικίες πρέπει να βοηθούν τα άτομα με αναπηρία κατά την άσκηση του πολιτικού τους δικαιώματος που θα επιτευχθεί με την ηλεκτρονική ψηφοφορία. Επιπλέον, τα άτομα με αναπηρία μπορεί να προτιμούν τη χρήση των οικιακών υπολογιστών τους όπου παρέχουν ευκολίες σε σχέση με τις παραδοσιακές μορφές γραφής και επικοινωνίας. Επίσης, για παράδειγμα, τα συστήματα ηλεκτρονικής ψηφοφορίας θα μπορούσαν να εξοπλιστούν με πρόσθετα χαρακτηριστικά για να βοηθήσουν εκείνους με προβλήματα όρασης ή ακοής και να προσελκύσουν ένα μεγαλύτερο κοινό[97]. Πρέπει να επισημανθεί ότι η ηλεκτρονική ψηφοφορία μετά την κατασκευή της υποδομής και την αποδοχή του υψηλού κόστους επένδυσης, το κόστος θα εξαργυρωθεί σε λίγα χρόνια και το κόστος της διαδικασίας θα μειωθεί σε σύγκριση με την παραδοσιακή ψηφοφορία. Μπορεί να προκαλέσει αύξηση της αποτελεσματικότητας, καθώς η διαδικασία θα μπορούσε να επιταχυνθεί, να οργανωθεί με μεγαλύτερη ακρίβεια και να αποτραπούν οι άκυρες δημοσκοπήσεις.

Εν αντίθεση όμως, η ανάπτυξη της υποδομής της ηλεκτρονικής ψηφοφορίας είναι δαπανηρή, καθώς περιλαμβάνει υπολογιστές, δημιουργία διακομιστών, πρόσληψη εμπειρογνωμόνων και αγορά του λογισμικού. Για παράδειγμα, το κόστος του πιλοτικού συστήματος που χρησιμοποιήθηκε στη Ζυρίχη κατά την περίοδο 2004-2006 ανήλθε σε 7,9 εκατομμύρια CHF(ελβετικό νόμισμα) για την περιοχή της Ζυρίχης και 0,5 εκατομμύρια CHF για τις κοινότητες που συμμετείχαν στο έργο. Επιπλέον, άλλα 3,2

εκατομμύρια CHF που προέκυψαν από τη δοκιμαστική περίοδο. Όλα αυτά προσθέτουν έως και 11,2 εκατομμύρια CHF. Οι εκτιμήσεις υποθέτουν ότι η εφαρμογή της ηλεκτρονικής ψηφοφορίας σε ολόκληρη τη χώρα θα κόστιζε 400 έως 600 εκατομμύρια CHF. Επιπροσθέτως, η ηλεκτρονική ψηφοφορία είναι μια πολύ περίπλοκη διαδικασία που απαιτεί εξειδίκευση για την πλήρη κατανόηση του. Για το λόγο αυτό, μόνο λίγοι χειρίζονται το σύστημα, από το οποίο κάθε πολίτης εξαρτάται και πρέπει να εμπιστεύεται. Με αποτέλεσμα το σύστημα να είναι άγνωστο προς την κοινότητα, κάτι το οποίο βλάπτει την αξιοπιστία και την εμπιστοσύνη. Ένα σημαντικό μειονέκτημα της ηλεκτρονικής ψηφοφορίας είναι το επίπεδο προστασίας που απαιτείται και το γεγονός ότι δεν θα είναι ποτέ εκατό τοις εκατό ασφαλές, πρέπον είναι να αναφερθεί όμως πώς ούτε η μετάβαση στις κάλπες ούτε η ταχυδρομική ψηφοφορία είναι απολύτως ασφαλής. Αν και δεν υπήρξαν παραβιάσεις ασφάλειας ή προβλήματα σχετικά με την ασφάλεια κατά τη διάρκεια των δοκιμών, αυτό δεν σημαίνει ότι δεν θα υπάρξουν στο μέλλον[98].

Τα πολιτικά κόμματα κάνουν χρήση των νέων δυνατοτήτων διαφήμισης και διάδοσης του μηνύματός τους στο διαδίκτυο με χαμηλό κόστος. Για τους χρήστες, αυτό μπορεί να οδηγήσει σε υπερφόρτωση πληροφοριών και σύγχυση σχετικά με την προέλευση των πληροφοριών, καθώς και μείωση των πολιτικών συζητήσεων και των αλληλεπιδράσεων μεταξύ των ηλεκτρονικών ψηφοφόρων.

Ένα σημαντικό κίνητρο για την ελβετική κυβέρνηση να περάσει την ηλεκτρονική ψηφοφορία είναι οι γρήγορες αλλαγές στις τεχνολογίες της πληροφορίας και των επικοινωνιών και μάλιστα στην πολιτική ζωή. Η Ελβετία θεώρησε ότι η ηλεκτρονική ψηφοφορία διευκολύνει τη συμμετοχή στις εκλογές, προσθέτει νέες και ελκυστικές μορφές συμμετοχής, αυξάνει το ποσοστό της συμμετοχής και προστατεύει τη δημοκρατική αρχή «μία ψήφος ανά άτομο» από την κατάχρηση. Ο Hans-Urs Wili από την Ομοσπονδιακή Καγκελαρία επισημαίνει ότι η εισαγωγή της ηλεκτρονικής ψηφοφορίας είναι απαραίτητη προκειμένου να διατηρηθεί ζωντανή η άμεση δημοκρατία, όπως υπάρχει σήμερα στην Ελβετία. Η ελβετική κυβέρνηση ήθελε να συμβαδίσει με αυτές τις αλλαγές και ξεκίνησαν πιλοτικά σχέδια για την εισαγωγή της ηλεκτρονικής ψηφοφορίας στις αρχές της δεκαετίας του 2000. Η κύρια προσέγγιση που χρησιμοποίησε η ελβετική κυβέρνηση ήταν να δώσει προτεραιότητα στην ασφάλεια αντί της ταχύτητας υιοθέτησης. Για το λόγο αυτό, η Ελβετία ξεκίνησε με τρείς πόλεις, τη

Γενεύη, το Neuchatel και τη Ζυρίχη. Ήταν ένα κοινό σχέδιο της Συνομοσπονδίας και των πόλεων. Η Ελβετική Συνομοσπονδία χρηματοδότησε έως και το 80% των δοκιμών με την προϋπόθεση ότι τα αποτελέσματα των έργων έπρεπε να δημοσιοποιηθούν στις άλλες πόλεις της Ελβετίας. Το 2006 αξιολογήθηκαν τα τρία πιλοτικά έργα και παρατηρήθηκε ότι το σύστημα ψηφοφορίας μέσω Διαδικτύου θα μπορούσε να χρησιμοποιηθεί για περισσότερο από το 20% του εκλογικού καταλόγου των πόλεων και έως και το 10% του ελβετικού εκλογικού καταλόγου[99-101].

Η περίπτωση της Γενεύης

Η Γενεύη ήταν από τις πόλεις που θεωρήθηκε ως «καθορισμένος υποψήφιος» για την εισαγωγή της ηλεκτρονικής ψηφοφορίας για πολλούς διαφορετικούς λόγους. Το ένα είναι το γεγονός ότι υπάρχει ένα κεντρικό ηλεκτρονικό μητρώο ψηφοφοριών. Στη Γενεύη, τα μητρώα των τοπικών ψηφοφόρων έχουν συνδεθεί ηλεκτρονικά από πριν από την έναρξη του προγράμματος ηλεκτρονικής ψηφοφορίας, σε αντίθεση με άλλες πόλεις. Η Γενεύη ήταν επίσης καλά προετοιμασμένη για ένα σχέδιο ηλεκτρονικής ψηφοφορίας, δεδομένου ότι ο νόμος περί κανόνων ψήφου εξουσιοδοτεί τις αρχές να δοκιμάσουν νέες μεθόδους ψηφοφορίας υπό το φως των τεχνολογικών εξελίξεων. Μια άλλη ενδιαφέρουσα πτυχή ήταν το υψηλό ποσοστό των αποδημιών της Γενεύης(https://www.eda.admin.ch/eda/en/home/living-abroad/publications-statistics/statistics.html).

Το σύστημα της Γενεύης βασίστηκε στην ασφάλειά του στη χρήση τυπικών μηχανισμών ασφαλείας, όπως η κρυπτογράφηση των επικοινωνιών με χρήση SSL και η κρυπτογράφηση των ψηφοφόρων στον διακομιστή ψηφοφορίας χρησιμοποιώντας τυπικούς κρυπτογραφικούς αλγόριθμους. Υποδεικνύεται ότι είναι αρκετά ασφαλές και αρκετά χρήσιμο. Ωστόσο, υπάρχουν κυρίως δύο ανησυχίες:

- Εάν ένας υπολογιστής έχει ήδη μολυνθεί από κακόβουλο λογισμικό, δεν είναι εγγυημένο ότι θα εξασφαλίσει τη διαδικασία της ψηφοφορίας
- Πολλά δεδομένα σχετικά με το σύστημα ηλεκτρονικής ψηφοφορίας της Γενεύης παραμένουν μυστικά.

Η κατασκευή του συστήματος ηλεκτρονικής ψηφοφορίας προϋποθέτει ότι ο ψηφοφόρος πρέπει να έχει εμπιστοσύνη και για να δημιουργήσει αυτήν την

εμπιστοσύνη, το Ομοσπονδιακό Συμβούλιο απαιτεί τη δημοσίευση του πηγαίου κώδικα του λογισμικού για την παροχή επαλήθευσης. Επίσης, οι ψηφοφόροι ενθαρρύνονται αν γνωρίζουν πώς λειτουργούν η ηλεκτρονική κάλπη και το μητρώο ψηφοφοριών, πώς παρακολουθούνται οι διακομιστές και τι συμβαίνει εάν εντοπιστεί μια επίθεση[102].

Η περίπτωση της Ζυρίχης

Το έργο ηλεκτρονικής ψηφοφορίας στην Ζυρίχη ξεκίνησε το 2002. Οι πρώτες υλοποιήσεις του συστήματος της Ζυρίχης εισήχθησαν για φοιτητικές εκλογές στο Πανεπιστήμιο της Ζυρίχης το 2004. Μετά την επιτυχία του συστήματος στις φοιτητικές εκλογές, δοκιμάστηκε για δημόσιες εκλογές .

Αξιοσημείωτο είναι το γεγονός ότι το σύστημα ηλεκτρονικής ψηφοφορίας της Ζυρίχης είναι αρκετά παρόμοιο με αυτό της Γενεύης, αλλά έχει επιπλέον χαρακτηριστικά. Εκτός από την ψηφοφορία μέσω Διαδικτύου, το σύστημα της Ζυρίχης επέτρεψε επίσης τη μετάδοση ψήφων μέσω μηνυμάτων κειμένου και διαδραστικών τηλεοπτικών συστημάτων (ITV). Ωστόσο, το 2007, ανακοινώθηκε ότι η ψηφοφορία μέσω SMS θα διακοπεί.

Η Ζυρίχη προσέλαβε την Unisys για να εφαρμόσει και να διαχειριστεί το διαδικτυακό της σύστημα ψηφοφορίας. Κύριο χαρακτηριστικό ασφαλείας του συστήματος της Ζυρίχης ήταν η χρήση διαφορετικών κωδικών για την επιλογή των υποψηφίων. Οι ψηφοφόροι έλαβαν μια ειδική κάρτα ψηφοφορίας με έναν μοναδικό κωδικό ανά υποψήφιο τον οποίο δεν τον επέλεγαν οι ίδιοι αλλά τον παρήγαγε το σύστημα. Αυτός ο μηχανισμός διατηρεί το απόρρητο των ψηφοφόρων ακόμη και αν χρησιμοποιούν ένα ανασφαλές δίαυλο επικοινωνίας όπως το SMS. Αντίθετα με το σύστημα της Γενεύης, η Ζυρίχη δεν διαθέτει κεντρικό μητρώο ψηφοφόρων. Για την επίλυση αυτού του προβλήματος, η ηλεκτρονική ψηφοφορία πραγματοποιείται σε επίπεδο κοινότητας και οι κοινότητες μεταφέρουν τα αποτελέσματα στην πόλη.

Σύστημα Ψηφοφορίας της Ελβετίας – Swiss Post System

Το σύστημα ηλεκτρονικής ψηφοφορίας της Swiss Post έχει σχεδιαστεί από την εταιρεία Scytl που εδρεύει στη Βαρκελώνη της Ισπανίας. Σε αυτό το σύστημα, οι ψηφοφόροι πιστοποιούνται στον ιστότοπο ψηφοφορίας χρησιμοποιώντας την ημερομηνία γέννησής τους και έναν κωδικό αρχικοποίησης που λαμβάνουν από την Swiss Post μέσω ταχυδρομείου. Αφού οι ψηφοφόροι κάνουν τις επιλογές τους, οι ψήφοι κρυπτογραφούνται πριν μεταβούν στους διακομιστές της Swiss Post, όπου ανακατεύονται κρυπτογραφικά για να χάσουν κάθε ίχνος μεταξύ ψήφου και ψηφοφόρου. Οι ψήφοι αποκρυπτογραφούνται μόνο κατά τη διαδικασία καταμέτρησης.

Αυτό το σύστημα δέχεται πολλές κριτικές. Οι ειδικοί βρίσκουν σοβαρά προβλήματα με αυτό το σύστημα, όπως ο κακός σχεδιασμός του, το υψηλό επίπεδο πολυπλοκότητας και η δυνατότητα να αφήσει κάποιον κακόβουλο να επιτεθεί και να αλλάξει τις ψήφους κατά τη φάση του ανακατέματος χωρίς να τον ανιχνεύσουν.

Για να αποδείξει την ασφάλεια του συστήματος έναντι επιθέσεων, η Swiss Post ξεκίνησε ένα δημόσιο τεστ διείσδυσης και ένα πρόγραμμα bug bounty.[103,104]

Μέτρα Ασφαλείας

Η Ελβετία δεν αναμένει ότι η ηλεκτρονική ψηφοφορία θα είναι 100% ασφαλής, αλλά πρέπει να είναι εξίσου ασφαλής και αξιόπιστη με τις παραδοσιακές μεθόδους ψηφοφορίας (δηλαδή ταχυδρομική ψηφοφορία και ψηφοφορία σε εκλογικά κέντρα). Σύμφωνα με τους νόμους της ψηφοφορίας, ένα σύστημα ψηφοφορίας πρέπει να διασφαλίζει ότι όλες οι ληφθείσες ψήφοι είναι ανώνυμες και δεν μπορούν να εντοπιστούν. Πρέπει να είναι αδύνατον να προσδιοριστεί η ψήφος ενός ψηφοφόρου και οι ψήφοι πρέπει να κρυπτογραφούνται μετά την υποβολή τους και να αποκωδικοποιούνται μόνο όταν πρόκειται να μετρηθούν. Η ψηφοφορία πρέπει να παραμείνει απόλυτα ανώνυμη. Επιπλέον, το σύστημα ψηφοφορίας πρέπει να διασφαλίσει ότι έχει ληφθεί η ψηφοφορία, και εάν υπάρχει τροποποιημένη ψηφοφορία, μετράτε μόνο η νεότερη έκδοση. Η διαδικασία δεν πρέπει να ενθαρρύνει τους ψηφοφόρους να ψηφίσουν χωρίς προβληματισμό και οι ψηφοφόροι πρέπει να είναι σε θέση να αλλάξουν την επιλογή τους πριν υποβάλουν την ψήφο τους[105,106].

Επιπλέον, το σύστημα πρέπει να διασφαλίσει ότι μόνο οι δικαιούχοι ψηφοφόροι μπορούν να λάβουν μέρος στην ψηφοφορία, κάθε ψηφοφόρος πρέπει να έχει μία ψήφο και να ψηφίσει μόνο μία φορά. Πρέπει να είναι αδύνατο για οποιοδήποτε τρίτο μέρος να συλλάβει, να τροποποιήσει ή να εκτρέψει ψήφους ή να επηρεάσει το αποτέλεσμα της ψηφοφορίας ή να ανακαλύψει το περιεχόμενο των ψήφων. Όλες οι ψήφοι πρέπει να λαμβάνονται υπόψη κατά τη διάρκεια της καταμέτρησης και ότι κάθε απάτη πρέπει να είναι αδύνατη.

Η ασφάλεια δεν ικανοποιείται μόνο από την κατοχή ενός ασφαλούς λογισμικού. Το σύστημα πρέπει επίσης να διασφαλίσει ότι η διαδικασία ψηφοφορίας δεν μπορεί να επηρεαστεί από το τεχνολογικό περιβάλλον. Σε αυτό το πλαίσιο, το πιο σημαντικό πρόβλημα είναι εάν ένας υπολογιστής, ο οποίος χρησιμοποιείται για την ψηφοφορία, περιέχει οποιοδήποτε κακόβουλο λογισμικό. Σε αυτήν την περίπτωση, ένας εισβολέας μπορεί να έχει πρόσβαση σε όλα τα δεδομένα που είναι αποθηκευμένα στον υπολογιστή, συμπεριλαμβανομένων τυχόν προσωπικών πληροφοριών και να μπορεί να τα χρησιμοποιήσει υπέρ του. Με την ύπαρξη ενός τέτοιου κακόβουλου λογισμικού, οι εκλογές μπορούν να επηρεαστούν από αυτό, αποθηκεύοντας δεδομένα που μεταδίδονται κατά τη διάρκεια της διαδικασίας ψηφοφορίας, προσομοιώνοντας τη διαδικασία κατά την διάρκεια της ψηφοφορίας ή και αργότερα.

Ένα άλλο σημαντικό σημείο είναι ότι ο διακομιστής ηλεκτρονικής ψηφοφορίας όπου αποθηκεύονται όλες οι ψήφοι έως ότου πραγματοποιηθεί η καταμέτρηση πρέπει να είναι απολύτως ασφαλής και άτρωτος σε επιθέσεις. Εάν ένας εισβολέας μπορεί να φτάσει στον κύριο διακομιστή, μπορεί να ανταλλάξει τα ψηφοδέλτια και να επηρεάσει το κύριο αποτέλεσμα των εκλογών. Εάν οι ψήφοι αλλάξουν πριν από τη καταμέτρηση, είναι αδύνατο να ανιχνευτεί αυτή η αλλαγή την ώρα της καταμέτρησης. Εν αντιθέσει η παραδοσιακή κάλπη στο εκλογικό τμήμα δεν είναι δυνατόν να παραβιαστεί με αυτόν τον τρόπο. Είναι ανοιχτό μπροστά στο κοινό και κανείς δεν έχει τη δυνατότητα να αλλάξει κάποιο ψηφοδέλτιο πριν την καταμέτρηση. Ομοίως, το εκλογικό μητρώο πρέπει επίσης να είναι ασφαλές για την αποφυγή επιθέσεων που προσπαθούν να χειραγωγήσουν τις εγγραφές

Η κύρια λειτουργία ενός εκλογικού συστήματος είναι να καθορίσει το σωστό εκλογικό αποτέλεσμα βάσει των ψήφων που υπέβαλαν οι ψηφοφόροι και όλες οι παρατυπίες που προκαλούνται από επιθέσεις ή σφάλματα λογισμικού πρέπει να εντοπιστούν με

αξιόπιστο τρόπο. Για να επαληθευτεί η ασφάλεια ενός συστήματος, πρέπει να γίνουν δοκιμές για να διασφαλιστεί η πληρότητα, η ακεραιότητα, η συνέπεια, τα αποδεικτικά στοιχεία και η αυθεντικότητα της διαδικασίας ψηφοφορίας. Για να βελτιωθεί η εμπιστοσύνη στα συστήματα της ηλεκτρονικής ψηφοφορίας, το Ομοσπονδιακό Συμβούλιο απαιτεί τη δημοσίευση του πηγαίου κώδικα αυτών των συστημάτων και απαιτείται μια δημόσια δοκιμή παραβίασης, η οποία θα επιτρέψει στους ενδιαφερόμενους να προσπαθήσουν να παραβιάσουν τα συστήματα.[107]

7.4.1.2 Ηλεκτρονική ψηφοφορία στην Εσθονία

Η Εσθονία έχει την περισσότερη εμπειρία συγκριτικά με τις άλλες χώρες στον τομέα της διαδικτυακής ψηφοφορίας. Έχει εισάγει την διαδικτυακή ψηφοφορία από το 2005 για τις κυβερνητικές εκλογές

Η Εσθονία παρέχει το μοναδικό παράδειγμα εφαρμογής της ηλεκτρονικής ψηφοφορίας (ψηφοφορίας μέσω διαδικτύου) ως επιλογή για όλους τους ψηφοφόρους σε εθνικό ή υπερεθνικό επίπεδο κυβέρνησης, με βουλευτικές εκλογές το 2007 και το 2011 και εκλογές για το Ευρωπαϊκό Κοινοβούλιο το 2009. Επιπλέον, η Εσθονία προσέφερε την εκλογή μέσω διαδικτύου ως επιλογή στις εκλογές της τοπικής αυτοδιοίκησης το 2005 και το 2009. Στις κοινοβουλευτικές εκλογές του 2011, σχεδόν το ένα τέταρτο των ψήφων, ήταν ψήφοι μέσω του διαδικτύου. Στην Εσθονία, το ποσοστό των ψηφοφόρων που χρησιμοποιούν ηλεκτρονική ψηφοφορία αυξήθηκε σταθερά με κάθε εκλογή από την εισαγωγή της.

Στις τοπικές δημοτικές εκλογές του 2013, 133.808 άτομα ψήφισαν μέσω του Διαδικτύου[108]. Αυτό σημαίνει ότι περίπου 21,2% των συμμετεχόντων ψηφοφόρων ψήφισαν μέσω του Διαδικτύου[108] Ήταν επίσης οι πρώτες εκλογές όπου πραγματοποιήθηκε η επαλήθευση ψήφου με κινητή συσκευή[109].

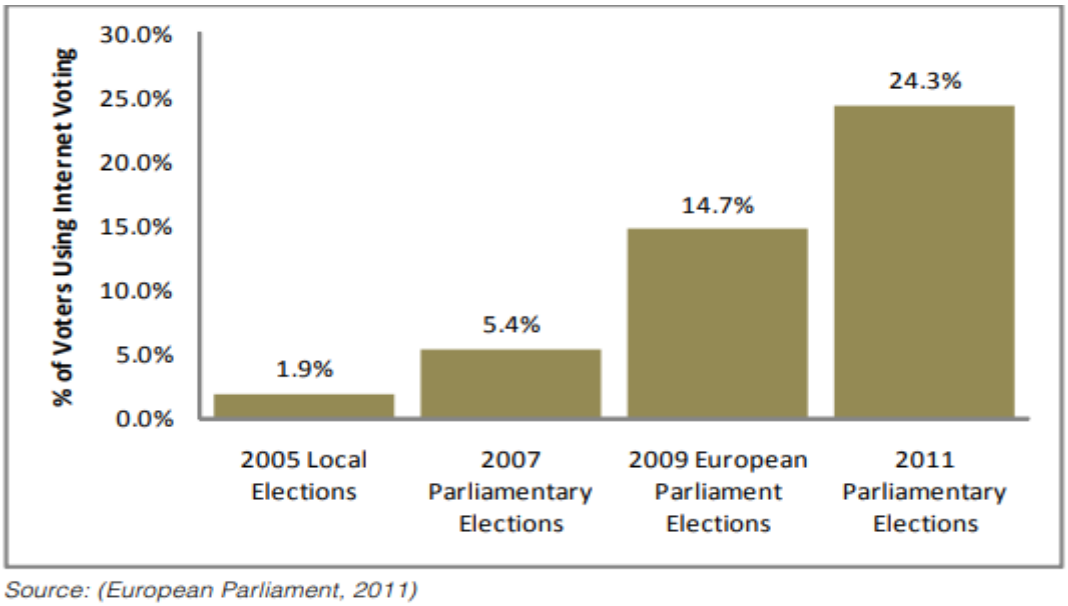
Στις εκλογές του Ευρωπαϊκού Κοινοβουλίου, 103.151 άτομα ψήφισαν μέσω του Διαδικτύου. Αυτό σημαίνει ότι περίπου το 31,3% των συμμετεχόντων ψηφοφόρων ψήφισαν μέσω του Διαδικτύου[108].

Στις κοινοβουλευτικές εκλογές του 2015, 176.491 άτομα, το 30,5% όλων των συμμετεχόντων, ψήφισαν μέσω του Διαδικτύου[108].

Στις τοπικές δημοτικές εκλογές του 2017, 186.034 άτομα ψήφισαν μέσω του Διαδικτύου. Αυτό σημαίνει ότι περίπου το 31,7% των συμμετεχόντων ψηφοφόρων ψήφισαν μέσω του Διαδικτύου[110].

Στις κοινοβουλευτικές εκλογές του 2019, 247.232 άτομα, ή 43,8% όλων των συμμετεχόντων, ψήφισαν μέσω του Διαδικτύου[111].

Αυτή η αύξηση απεικονίζεται στο παρακάτω διάγραμμα. Συγκεκριμένα, παρατηρείται ότι το 2005 που πραγματοποιήθηκε για πρώτη φορά ηλεκτρονική ψηφοφορία στις τοπικές εκλογές η συμμετοχή ήταν σε ποσοστό 1,9%. Στις κοινοβουλευτικές εκλογές μετά από δυο χρόνια (2007) όπου εφαρμόστηκε ξανά η ηλεκτρονική ψηφοφορία το ποσοστό συμμετοχής ήταν 5,4%. Μεγάλη αύξηση σημειώθηκε στις εκλογές για το Ευρωπαϊκό Κοινοβούλιο το 2009 καθώς το ποσοστό προτίμησης της ηλεκτρονικής ψηφοφορίας ήταν 14,7%. Στη συνέχεια, όπως φαίνεται στο διάγραμμα, στις κοινοβουλευτικές εκλογές του 2011 η χρήση της ηλεκτρονικής ψηφοφορίας ανήλθε στο 24,3%.



Source: (European Parliament, 2011)

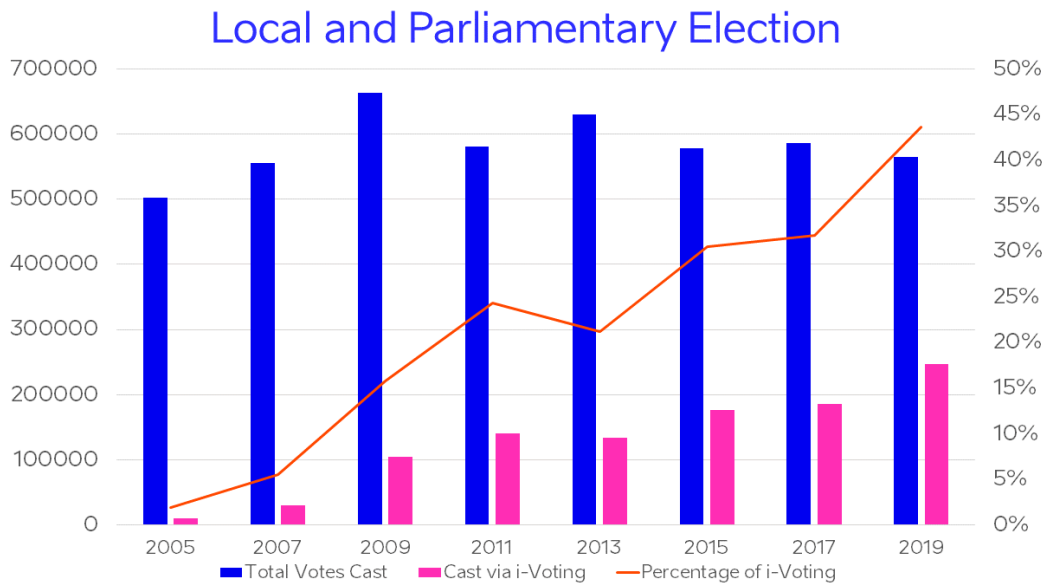
Εικόνα 5 Γραφική απεικόνιση της αύξησης της χρήσης της ηλεκτρονικής ψηφοφορίας στην Ελβετία, 2005-2011

Η Εσθονία έχει πραγματοποιήσει ψηφοφορία μέσω Διαδικτύου σε οκτώ συνεχόμενες εκλογές. Ήταν η πρώτη χώρα, το 2005, που εισήγαγε απομακρυσμένη ηλεκτρονική ψηφοφορία σε πανεθνικές δεσμευτικές εκλογές και ηγήθηκε ενός είδους «αγώνα» στις αρχές της δεκαετίας του 2000 για την εισαγωγή απομακρυσμένων ηλεκτρονικών

μεθόδων στις εκλογές[112,113] . Ο αριθμός των Ψηφοφόρων Διαδικτύου αυξάνεται από την αρχή, φτάνοντας πάνω από 176.000 ψηφοφόρους και αποτελώντας πάνω από το 30% όλων των ψήφων στις κοινοβουλευτικές εκλογές του 2019.

Η ψηφοφορία μέσω Διαδικτύου ξεκίνησε χαμηλά, με μόνο 9.317 ψηφοφόρους, αλλά άρχισε να αυξάνεται στις ακόλουθες εφαρμογές. Το χαμηλό ξεκίνημα και η ακόλουθη βαθμιαία αύξηση των αριθμών θα μπορούσαν να εξηγηθούν από τη θεωρία του Rodgers σχετικά με τη διάδοση της καινοτομίας[114]. Ο αριθμός των επιλέξιμων ψηφοφόρων και οι αριθμοί συμμετοχής διαφέρουν σαφώς ανά τύπο εκλογής. Για παράδειγμα, η προσέλευση των εκλογών στο Ευρωπαϊκό Κοινοβούλιο είναι επίσης χαμηλότερη[115] από ό, τι σε άλλους τύπους εκλογών, όπως οι τοπικές ή εθνικές εκλογές.

Επομένως, οι αριθμοί όπως φαίνεται στο Σχ. 1 έχουν διακυμάνσεις ανά τύπο εκλογής



Εικόνα 6 Ηλεκτρονική ψηφοφορία στην Εσθονία 2005-2019, Πηγή: https://images.app.goo.gl/BH7SYaMsQgvNxBVq6

Ωστόσο, το μερίδιο των ψηφοφόρων στο Διαδίκτυο μεταξύ όλων των ψηφοφόρων έχει δείξει σταθερή αύξηση παρά τις απόλυτες διακυμάνσεις του αριθμού, έχοντας αυξηθεί σε πάνω από 30% στις τελευταίες εκλογές. Επιπλέον, η ψηφοφορία μέσω Διαδικτύου προσφέρεται περίπου επτά ημέρες νωρίτερα, κατά την εκ των προτέρων ψηφοφορία, και από το 2011, υπήρχαν περισσότεροι υποστηριχτές της ηλεκτρονικής ψηφοφορίας από ότι της τυπικής ψηφοφορίας.[116] Αυτή η διαδικασία είχε αντίκτυπο στον

οργανισμό της παραδοσιακής ψηφοφορίας, πιέζοντας τις τοπικές κυβερνήσεις να μειώσουν τον αριθμό των εκλογικών κέντρων, καθώς ο αριθμός των συμμετεχόντων έχει μειωθεί, ειδικά στις αγροτικές περιοχές. Το αποτέλεσμα τονίζεται από τη διαπίστωση ότι η σχετική απόσταση από το εκλογικό τμήμα έχει σαφή συσχέτιση με τη χρήση της ψηφοφορίας μέσω Διαδικτύου[117,118].

Εξετάζοντας την επιρροή των αποτελεσμάτων της ψηφοφορίας μέσω Διαδικτύου, θα μπορούσαν να διακριθούν τουλάχιστον τρεις κατηγορίες:

- πρώτον η επιρροή στην προσέλευση των ψηφοφόρων στα εκλογικά κέντρα, εάν η προσθήκη μιας νέας μεθόδου ψηφοφορίας αυξάνει την προσέλευση
- Δεύτερον, η επίδραση των κοινωνικό-δημογραφικών παραγόντων στη χρήση της ψηφοφορίας μέσω Διαδικτύου
- τρίτον η σχέση της Ψηφοφορίας μέσω Διαδικτύου και των εκλογικών αποτελεσμάτων

Επιστημονικές εκθέσεις για την Εσθονική ψηφοφορία μέσω Διαδικτύου έχουν συγκεντρωθεί[118], και τα αποτελέσματα έχουν συζητηθεί δημόσια και είναι διαθέσιμα στην ιστοσελίδα του EMB.

Η πιο συχνή ερώτηση που γίνεται με οποιαδήποτε νέα εκλογική λύση είναι η επιρροή που έχει στην προσέλευση των ψηφοφόρων. Ωστόσο, είναι δύσκολο να εκτιμηθεί η πραγματική επιρροή της ψηφοφορίας μέσω Διαδικτύου στην προσέλευση, διότι δεν είναι δυνατή η άμεση σύγκριση των ίδιων εκλογών με και χωρίς ψηφοφορία. Ίσως ένα καλύτερο ερώτημα που πρέπει να τεθεί είναι το μερίδιο του εκλογικού σώματος που δεν θα είχε συμμετάσχει στην ψηφοφορία εάν δεν είχε δημιουργηθεί η δυνατότητα της ψηφοφορίας μέσω Διαδικτύου. Δυστυχώς, μόνο τα αποτελέσματα της έρευνας των ψηφοφόρων μπορούν να χρησιμοποιηθούν εδώ. Μία εξαίρεση αποτελεί η περίπτωση που η ψηφοφορία μέσω Διαδικτύου είναι η μόνη επιλογή για τον ψηφοφόρο. Στις τοπικές εκλογές, η Εσθονία δεν προβλέπει ψηφοφορία από το εξωτερικό ταχυδρομικά ή με διπλωματική εκπροσώπηση, επομένως η ψηφοφορία μέσω Διαδικτύου είναι η μόνη μέθοδος ψηφοφορίας για τους ψηφοφόρους του εξωτερικού[119]

Ο αριθμός των ηλεκτρονικών ψηφοφόρων και της γενικής προσέλευσης των ψηφοφόρων δεν ήταν γραμμικός. Επιστημονικές έρευνες έχουν δείξει ότι οι περισσότεροι ψηφοφόροι οι οποίοι επέλεξαν την ψηφοφορία μέσω Διαδικτύου είναι

στην πραγματικότητα οι παραδοσιακοί ψηφοφόροι(με χάρτινα ψηφοδέλτια) που αποφασίζουν να αλλάξουν τη μέθοδο ψηφοφορίας, μόνο ένας σχετικά μικρός αριθμός ψηφοφόρων έχει αρχίσει να ψηφίζει λόγω της ένταξης της ηλεκτρονικής ψηφοφορίας. Το 2005, η ηλεκτρονική ψηφοφορία φαίνεται να είχε μια μικρή επίδραση στην αύξηση της προσέλευσης των ψηφοφόρων που μερικές φορές ψηφίζουν και μερικές φορές δεν ψηφίζουν. Το 2007, ήδη περίπου το 10% των ερωτηθέντων ηλεκτρονικών ψηφοφόρων δήλωσαν ότι πιθανότατα να μην είχαν ψηφίσει αν δεν είχαν τη δυνατότητα να ψηφίσουν μέσω του Διαδικτύου[120]. Οι Trechsel και Vassil δείχνουν[121] (το 2011) ότι το ποσοστό των ψηφοφόρων που ερωτήθηκαν αν δεν θα είχαν ψηφίσει αν δεν είχαν τη δυνατότητα του Διαδικτύου έχει αυξηθεί στο 16,3%, γεγονός που επιτρέπει το συμπέρασμα ότι η συνολική προσέλευση θα μπορούσε να ήταν κατά 2,6% χαμηλότερη εάν δεν υπήρχε τέτοια μέθοδος ψηφοφορίας.

Ένα άλλο ενδιαφέρον ερώτημα είναι εάν η ψηφοφορία μέσω Διαδικτύου δείχνει κάποια διαφορά στην εκπροσώπηση εντός των κοινωνικών ομάδων. Η απομακρυσμένη ηλεκτρονική ψηφοφορία εξαλείφει τα φυσικά εμπόδια που εμποδίζουν τη συμμετοχή στις εκλογές τους ηλικιωμένους, άτομα με ειδικές ανάγκες ή άλλων ομάδων με περιορισμένη, κινητικότητα ή σε ομάδες που δυσκολεύονται να παραβρεθούν στα εκλογικά κέντρα (π.χ. άτομα έχοντας αυστηρά χρονοδιαγράμματα ή εργασία, σπουδές ή ταξίδια στο εξωτερικό, γονείς μικρών παιδιών και άτομα που ζουν σε περιοχές με κακή υποδομή), υποθέτοντας, φυσικά, ότι αυτά τα άτομα έχουν πρόσβαση στο Διαδίκτυο.

Ο Trechsel και αργότερα οι Vassil και Solvak κατέληξαν στο συμπέρασμα, μετά από την εμπειρία τους με την ψηφοφορία μέσω Διαδικτύου από το 2005 έως το 2015, ότι η εκπαίδευση των πολιτών και το εισόδημα, καθώς και ο τύπος διακανονισμού ήταν ασήμαντοι παράγοντες ώστε να εμποδίσουν την στροφή προς αυτήν την κατεύθυνση σε σχέση με άλλες επιλογές[6669]. Ένα από τα πιο σημαντικά ευρήματα των μελετών που ερεύνησαν τους προγνωστικούς παράγοντες της ψηφοφορίας έως τις εκλογές του 2009 ήταν ότι οι ψηφοφόροι δεν είχαν την κατάλληλη γνώση για την χρήση του ηλεκτρονικού υπολογιστή και επίσης δεν χρησιμοποιούσαν τόσο συχνά το διαδίκτυο. Η εμπιστοσύνη στο σύστημα και στη διαδικασία της ηλεκτρονικής ψηφοφορίας υπήρξε ο σημαντικότερος παράγοντας κατά τη διάρκεια των ετών που κατευθύνει την επιλογή των ψηφοφόρων να χρησιμοποιούν την απομακρυσμένη ηλεκτρονική μέθοδο

ψηφοφορίας[122,123]. Ο Vassil[124] ισχυρίστηκε επίσης ότι, βάσει της εμπειρικής ανάλυσης, τουλάχιστον μια περίοδος τριών εκλογών πρέπει να μελετηθεί ώστε να έχει επαρκή αποτελέσματα για την αξιολόγηση της επιρροής των διαφορετικών χαρακτηριστικών της ψηφοφορία μέσω Διαδικτύου.

Το ερώτημα για τα πολιτικά κόμματα είναι εάν η χρήση της ηλεκτρονικής ψηφοφορίας επηρεάζει τα συνολικά εκλογικά αποτελέσματα. Αξιοσημείωτο είναι το γεγονός πως τα κόμματα της Εσθονίας που τάχθηκαν υπέρ της ηλεκτρονικής ψηφοφορίας στις εκστρατείες τους και υποστήριξαν αυτήν τη μέθοδο ψηφοφορίας έλαβαν περισσότερες ηλεκτρονικές ψήφους σε σύγκριση με εκείνα τα κόμματα που δεν υποστηρίζουν τη χρήση της. Ωστόσο, έρευνες έδειξαν πως δεν έχουν σημασία τα πολιτικά πιστεύω για την επιλογή της ψηφοφορίας, επομένως είναι πολιτικά ανεξάρτητη[118,121]. Κλείνοντας, παρατηρήθηκε σταθερή αύξηση της χρήσης της ψηφοφορίας μέσω Διαδικτύου στην Εσθονία έως τις γενικές εκλογές του 2011. Μετά από αυτό, ο αριθμός των ψηφοφόρων δεν ήταν σταθερός λόγω της φύσης των εκλογών στις οποίες χρησιμοποιείται, αλλά το ποσοστό των ηλεκτρονικών ψηφοφόρων συνεχίζει να αυξάνεται. Αξίζει να αναφερθεί πως από το 2011 και μετά η ηλεκτρονική ψηφοφορία είναι πιο δημοφιλές από την παραδοσιακή. Εξετάζοντας την επιρροή της, διαπιστώνουμε πως μόνο ένα μικρό ποσοστό των ψηφοφόρων είναι νέοι, οι υπόλοιποι απλώς εγκαταλείπουν την παραδοσιακή ψηφοφορία και στρέφονται στην ηλεκτρονική. Ένας ισχυρότερος αντίκτυπος θα μπορούσε να γίνει στις τοπικές εκλογές, όπου η ηλεκτρονική ψηφοφορία είναι η μόνη διαθέσιμη μέθοδος από το εξωτερικό. Τέλος, αρκετές μελέτες εξέτασαν την πολιτική επιρροή της ηλεκτρονικής ψήφου και διαπίστωσαν ότι είναι πολιτικά ουδέτερη και δεν επιφέρει προκατειλημμένα αποτελέσματα στις εκλογές.

Τρόπος λειτουργίας

Το σύστημα ψηφοφορίας στο Διαδίκτυο της Εσθονίας βασίζεται στην εσθονική ταυτότητα. Η κάρτα είναι ένα κανονικό και υποχρεωτικό[125] εθνικό έγγραφο ταυτότητας, καθώς και μια έξυπνη κάρτα που επιτρέπει τόσο ασφαλή απομακρυσμένο έλεγχο ταυτότητας όσο και νομικά δεσμευτικές ψηφιακές υπογραφές χρησιμοποιώντας

την υποδομή δημόσιου κλειδιού που υποστηρίζεται από την Εσθονία[126]. Από τον Μάρτιο του 2007 έχουν εκδοθεί πάνω από 1,3 εκατομμύρια κάρτες (από έναν πληθυσμό περίπου 1,32 εκατομμύρια)[127].

Η ψηφοφορία μέσω Διαδικτύου είναι διαθέσιμη για ένα μικρό χρονικό διάστημα πριν την ψηφοφορία (από τέσσερεις έως έξι ημέρες πριν από την Ημέρα των Εκλογών). Οι ψηφοφόροι μπορούν να αλλάξουν τις ηλεκτρονικές ψήφους τους απεριόριστα πολλές φορές, με την τελική ψηφοφορία να καταγράφεται. Είναι επίσης δυνατό για όποιον ψηφίζει χρησιμοποιώντας το Διαδίκτυο να ψηφίσει σε ένα εκλογικό κέντρο κατά την περίοδο πρόωρης ψηφοφορίας, ακυρώνοντας την ψήφο του στο Διαδίκτυο. Δεν είναι δυνατή η αλλαγή ή η ακύρωση της ηλεκτρονικής ψηφοφορίας την Ημέρα των Εκλογών[128]. Μια σύγκριση της αποδοτικότητας κόστους των διαφόρων καναλιών ψηφοφορίας που προσφέρθηκαν στις Εσθονικές Δημοτικές Εκλογές (2017) κατέληξε στο συμπέρασμα ότι η Ψηφοφορία μέσω Διαδικτύου είναι η πιο οικονομικά αποδοτική ψηφοφορία που προσφέρει το Εσθονικό Εκλογικό Σύστημα[129].

Ο θεσμός της ψηφοφορίας ορίζει την αρχή «μία ψήφος ανά άτομο». Στην ηλεκτρονική ψηφοφορία της Εσθονίας η αρχή αυτή διατηρείται καθώς ο ψηφοφόρος μπορεί δυνητικά να ψηφίσει περισσότερες από μία ψήφο, αλλά εξακολουθεί να είναι μόνο μία ψήφος δεδομένου ότι η προηγούμενη απορρίπτεται. Αυτό αμφισβητήθηκε τον Αύγουστο του 2005 από τον Arnold Rüütel, τον Πρόεδρο της Εσθονίας, ο οποίος θεωρεί ότι οι νέες διατάξεις για την ηλεκτρονική ψηφοφορία στον εκλογικό νόμο του Συμβουλίου Τοπικής Αυτοδιοίκησης παραβιάζουν την αρχή της ισότητας των ψήφων. Ο Πρόεδρος άσκησε μια αναφορά κατά των διατάξεων για την ηλεκτρονική ψηφοφορία στο Ανώτατο Δικαστήριο της Εσθονίας, αλλά δεν έγινε αποδεχτή.

Εμπιστευτικότητα και Επαλήθευση

Σύμφωνα με τη σύσταση του 2011 για τους εκλογικούς παρατηρητές του OSCE/ODIHR και λόγω της επίθεσης που πραγματοποιήθηκε στην μεριά του ψηφοφόρου και όχι του server, η οποία έφτασε μέχρι το Ανώτατο Δικαστήριο, η Εσθονία εφάρμοσε την επαλήθευση της ψήφου για κάθε ψηφοφόρο το 2013. Η επαλήθευση γίνεται χρησιμοποιώντας μια εφαρμογή smartphone, η οποία χρησιμοποιεί QR κωδικό, στην συνέχεια αφού πραγματοποιηθεί η ψηφοφορία εμφανίζεται στην οθόνη το όνομα και ο αριθμός του υποψηφίου που ψήφισε ο ψηφοφόρος . Η επαλήθευση εφαρμόζεται για

τον ψηφοφόρο για να επαληθεύσει ότι η ψηφοφορία αποθηκεύτηκε στον server για 30 λεπτά ή μία ώρα, ανάλογα με τις εκλογές. Δυστυχώς, δεν υπάρχει άμεσο μέσο για τον ψηφοφόρο να επαληθεύσει ότι η ψήφος του μετρήθηκε επίσης στην ψηφοφορία
Ο πηγαίος κώδικας του server του συστήματος ψηφοφορίας δημοσιεύθηκε τον Ιούνιο του 2013 λόγω της πίεσης της κοινωνίας των πολιτών που καθοδηγούταν από τον επιστήμονα Tanel Tammet, ένας από τους συγγραφείς ερευνητικών εργασιών σχετικά με τις απαιτήσεις για ηλεκτρονική ψηφοφορία από το 2001. Ο κώδικας δημοσιεύθηκε στο GitHub και ήταν διαθέσιμο για όλες τις επόμενες εκλογές. Ο πηγαίος κώδικας του υποψηφίου δεν έχει δημοσιευτεί καθώς οι εκλογικοί αξιωματούχοι έκριναν ότι αυτό θα διευκόλυνε τους κακόβουλους να δημιουργήσουν ψεύτικους ψηφοφόρους. Το πρωτόκολλο ψηφοφορίας είναι δημόσιο, επομένως ο καθένας θα μπορούσε να δημιουργήσει έναν ψεύτικο ψηφοφόρο.

Επίσης, με αφορμή την αναφορά των εκλογικών παρατηρητών του OSCE/ODIHR το 2015, τις εκτεταμένες αναφορές από μία ανεξάρτητη ομάδα παρατηρητών με ηγέτη τον J Alex Halderman και την δημόσια πίεση από μία τοπικούς ακτιβιστές, καθιερώθηκε η καθολική επαλήθευση της ψηφοφορίας το 2017. Η επαλήθευση της καταμέτρησης γίνεται με mixnet χρησιμοποιώντας τις ομομορφικές ιδιότητες κρυπτογράφησης ElGamal που παρέχεται από τη βιβλιοθήκη του Douglas Wikström. Η καθολική επαλήθευση του αριθμού δεν αποτελεί υποχρεωτικό μέρος της διαδικασίας και πραγματοποιείται από τον ειδικό ελεγκτή δεδομένων. Ο υπολογισμός των ψήφων με το mixnet γίνεται παράλληλα με την εξαγωγή του αποκρυπτογραφημένου κειμένου των ψήφων από τους κρυπτογραφημένους φακέλους, οι οποίοι αποκρυπτογραφούνται χρησιμοποιώντας το μυστικό κλειδί της επιτροπής ψηφοφορίας και των οποίων αφαιρούνται οι ψηφιακές υπογραφές των ψηφοφόρων κατά τη διαδικασία.
Ερευνητές έκαναν κάποιες δοκιμές για την ασφάλεια του συστήματος ψηφοφορίας της Εσθονίας και βρήκαν πολλά προβλήματα ασφαλείας στο λογισμικό αλλά και πολλά προβλήματα στον τρόπο λειτουργίας και διαχείρισης του συστήματος. Όπως για παράδειγμα ένα βίντεο που διέθεταν στο κοινό για την προεκλογική διαδικασία, το οποίο έδειχνε κωδικούς Wi-Fi κολλημένους στον τοίχο, τους διαχειριστές να πληκτρολογούν κωδικούς στο root και ένα λογισμικό το οποίο χρησιμοποιείται για την πλατφόρμα PokerStars.

"Το ηλεκτρονικό σύστημα ψηφοφορίας της Εσθονίας έχει τόσες σοβαρές ευπάθειες στην ασφάλεια, που οι ειδικοί συνιστούν να διακοπεί αμέσως", ανέφεραν οι ερευνητές. Ένας επιτιθέμενος θα μπορούσε πολύ εύκολα να προσπεράσει τους τεχνολογικούς αλλά και τους διαδικαστικούς ελέγχους ώστε να καταφέρει να χειραγωγήσει τα εκλογικά αποτελέσματα.

Η Ρωσία επιτέθηκε στην Εσθονία με massive DDoS επίθεση το 2007 με αφορμή την απόφαση της χώρας να μεταφέρει ένα μνημείο πολέμου της σοβιετικής εποχής. Σύμφωνα με την The Guardian (εφημερίδα), οι κύριοι στόχοι της επίθεσης ήταν κυβερνητικές ιστοσελίδες, πολιτικά κόμματα, μεγάλες ειδησεογραφικές οργανώσεις και δύο από τις μεγαλύτερες τράπεζες της χώρας. Ωστόσο, η εθνική εκλογική επιτροπή της Εσθονίας απέρριψε τα συμπεράσματα των ερευνητών ασφαλείας, λέγοντας σε μια δήλωση την εποχή εκείνη: "Πιστεύουμε ότι η ηλεκτρονική ψηφοφορία μας επιτρέπει να επιτύχουμε ένα επίπεδο ασφάλειας μεγαλύτερο από αυτό που είναι δυνατό με χάρτινες ψηφοφορίες".

7.4.1.3 Ηλεκτρονική ψηφοφορία στη Νορβηγία

Η Νορβηγία, εδραιωμένη δημοκρατία με 3,6 εκατομμύρια εγγεγραμμένους ψηφοφόρους, σχεδίασε να χρησιμοποιήσει την ψηφοφορία μέσω διαδικτύου σε ορισμένους δήμους κατά τις τοπικές εκλογές της στις 12 Σεπτεμβρίου 2011[130]. Οι εκλογές αυτές θα ήταν το πρώτο βήμα σε ένα ευρύτερο σχέδιο για την εφαρμογή της ψηφοφορίας μέσω διαδικτύου ως επιλογή για όλους τους ψηφοφόρους στις κοινοβουλευτικές εκλογές της Νορβηγίας το 2017.

Το Υπουργείο Τοπικής Αυτοδιοίκησης και Περιφερειακής Ανάπτυξης της Νορβηγίας προέβη πιλοτικά στην εφαρμογή της ηλεκτρονικής ψηφοφορίας σε τρεις δήμους, στις τοπικές εκλογές το 2011, χρησιμοποιώντας οθόνες αφής[131] στις μηχανές ψηφοφορίας στα εκλογικά κέντρα.

Η Νορβηγία διεξήγαγε εκλογές χρησιμοποιώντας τη μέθοδο της ηλεκτρονικής ψηφοφορίας και δεν αύξησε την προσέλευση των ψηφοφόρων, ούτε των νέων[132]. Οι Νορβηγοί επιζητούσαν να διασφαλίσουν την εμπιστοσύνη στους ψηφοφόρους, καθώς και την ασφάλεια.

Η νορβηγική κυβέρνηση αναγνωρίζει τη σημασία της οικοδόμησης της εμπιστοσύνης του κοινού σε νέα συστήματα ψηφοφορίας[133]. Η διαφάνεια είναι μια από τις στρατηγικές για την ενίσχυση της εμπιστοσύνης του κοινού στην ψηφοφορία μέσω του διαδικτύου ώστε να επιτευχθεί ένα αξιόπιστο αποτέλεσμα.

Το σύστημα ηλεκτρονικής ψηφοφορίας της Νορβηγίας διαθέτει μια σειρά από καινοτόμα χαρακτηριστικά που επιτρέπουν στους ψηφοφόρους να επαληθεύουν ότι οι ψηφοφορίες τους λαμβάνονται και ότι μειώνουν την εξάρτηση από την ασφάλεια των προσωπικών υπολογιστών των ψηφοφόρων. Αυτό επιτυγχάνεται με τη χρήση δύο ανεξάρτητων καναλιών: το ένα να διαβιβάζει την ψηφοφορία και ένα άλλο για να επιβεβαιώσει ότι η ψηφοφορία ελήφθη. Οι ψηφοφόροι συμπληρώνουν τα ψηφοδέλτια τους χρησιμοποιώντας έναν απομακρυσμένο υπολογιστή και λαμβάνουν επιβεβαίωση για την ολοκλήρωση της ψήφου τους μέσω μηνυμάτων SMS στις κινητές τους συσκευές. Σε περίπτωση που ο υπολογιστής του ψηφοφόρου έχει καταστραφεί, ο ψηφοφόρος είναι σε θέση να προσδιορίσει το ζήτημα και να ψηφίσει ξανά[134].

Συμφώνα με τα αποτελέσματα μιας έρευνας του Ινστιτούτου Κοινωνικών Ερευνών της Νορβηγίας, οι ψηφοφόροι φοβούνται ότι οι ψήφοι τους θα φανούν δημόσια, πράγμα το οποίο θεωρούν ως καταπάτηση των δημοκρατικών τους δικαιωμάτων. Μέχρις ότου το κράτος να εξασφαλίσει ένα ορισμένο επίπεδο ασφάλειας για την ψήφο, τα αποτελέσματα στη Νορβηγία είναι απίθανο να αλλάξουν - η προσέλευση των ψηφοφόρων θα είναι πιο χαμηλή ακόμη κι αν η ηλεκτρονική ψηφοφορία προσφέρει μεγαλύτερες ευκολίες[135].

7.4.1.4 Ηλεκτρονική ψηφοφορία στη Ρουμανία

Η Ρουμανία εφάρμοσε για πρώτη φορά το ηλεκτρονικό σύστημα ψηφοφορίας το 2003[136], σε περιορισμένη βάση, για να επεκτείνει τις δυνατότητες ψήφου σε στρατιώτες και άλλους που υπηρετούν στο Ιράκ και σε άλλα μέρη. Παρά τον δηλωμένο στόχο της καταπολέμησης της διαφθοράς, ο εξοπλισμός προμηθεύτηκε και εγκαταστάθηκε σε λιγότερο από 30 ημέρες από την έκδοση του κυβερνητικού διατάγματος[137] – πράγμα το οποίο δεν εμπνέει εμπιστοσύνη.

7.4.1.5 Ηλεκτρονική ψηφοφορία στην Ισπανία

Το 2014 το πολιτικό κόμμα Podimos, κατά τη διάρκεια του πρώτου συνεδρίου του, διεξήγαγε 3 εκλογές χρησιμοποιώντας το λογισμικό ανοικτού κώδικα ψηφοφορίας Agora. Με σκοπό να ψηφίσει μέσω διαδικτύου μια σειρά εγγράφων που θα καθορίζουν τις πολιτικές και οργανωτικές αρχές του κόμματος (112070 ψηφοφόροι), ψήφισμα που θα υιοθετήσει το κόμμα (38279 ψηφοφόροι) και τα άτομα που θα οριστούν από αυτή τη δομή (107488 ψηφοφόροι) [138]. Στη συνέχεια, μετά τις δημοτικές εκλογές που διεξήχθησαν τον Μάιο του 2015 αρκετοί δήμαρχοι της πόλης ανακοίνωσαν τα σχέδιά τους για διεξαγωγή δημόσιων διαβουλεύσεων χρησιμοποιώντας ηλεκτρονική ψηφοφορία[139].

7.4.1.6 Ηλεκτρονική ψηφοφορία στο Ηνωμένο Βασίλειο

Το Ηνωμένο Βασίλειο χρησιμοποίησε σύστημα ηλεκτρονικής ψηφοφορίας πιλοτικά το Μάιο του 2006[140], τον Ιούνιο του 2004[141], τον Μάιο του 2003[142], τον Μάιο του 2002 και τον Μάιο του 2000.Το 2000, τα αποτελέσματα των εκλογών του Mayoral και Assembly στο Λονδίνο υπολογίστηκαν χρησιμοποιώντας ένα σύστημα ψηφοφορίας οπτικής σάρωσης με λογισμικό που παρέχεται από την DRS plc του Milton Keynes. Το 2004, οι εκλογές του Δήμου του Λονδίνου, της Συνέλευσης και του Ευρωπαϊκού Κοινοβουλίου εξετάστηκαν και υποβλήθηκαν σε επεξεργασία χρησιμοποιώντας οπτική αναγνώριση χαρακτήρων από την ίδια εταιρεία. Και οι δύο εκλογές απαιτούσαν κάποια επεξεργασία του σχεδίου ψηφοφορίας για να διευκολυνθεί η ηλεκτρονική καταλογογράφηση, μολονότι διέφεραν ελάχιστα από το προηγούμενο.
Τον Ιανουάριο του 2016, το Κοινοβούλιο του Ηνωμένου Βασιλείου αποφάσισε να μην εισάγει με νόμο την ηλεκτρονική ψηφοφορία για εκλογές, είτε για ψηφοφορία σε εκπροσώπους εκλογικών περιφερειών είτε εξ ‘αποστάσεως μέσω διαδικτύου[143]. Παράλληλα, ένα σύστημα ψηφοφορίας με οπτική σάρωση χρησιμοποιήθηκε για την ηλεκτρονική καταμέτρηση των χάρτινων ψηφοδελτίων στις γενικές εκλογές του Σκωτικού Κοινοβουλίου και στις εκλογές του Συμβουλίου της Σκωτίας το 2007[144,145].

Σύμφωνα με τα αποτελέσματα της έρευνας της βρετανικής εκλογικής επιτροπής διαπιστώθηκαν σημαντικά λάθη στη σχεδίαση ψηφοδελτίων που παρήγαγαν περισσότερες από 150.000 ψευδείς ψήφους[146]. Το BBC ανέφερε ότι απορρίφθηκαν 86.000 εκλογικές περιφέρειες και 56.000 λίστες ψηφοφορίας, με τον ισχυρισμό ότι προκλήθηκαν από τους ψηφοφόρους που κλήθηκαν να ψηφίσουν και για τα δύο τμήματα των εκλογών, που αναφέρθηκαν παραπάνω, στο ίδιο ψηφοδέλτιο και όχι σε χωριστά ψηφοδέλτια όπως συνέβαινε στις προηγούμενες εκλογές[147]. Εκτός από αυτό, οι βουλευτικές εκλογές της Σκωτίας και οι εκλογές του Συμβουλίου της Σκωτίας χρησιμοποιούν διαφορετικά εκλογικά συστήματα. Οι εκλογές του Συμβουλίου χρησιμοποιούν ενιαία μεταβιβάσιμη ψήφο, ενώ οι εκλογές του Κοινοβουλίου χρησιμοποιούν το πρόσθετο σύστημα των μελών. Ο πρώτος απαιτεί από τον ψηφοφόρο να τοποθετήσει αριθμούς σύμφωνα με τις προτιμήσεις τους, ενώ ο τελευταίος απαιτεί ένα σταυρό για να υποδείξει την ενιαία προτίμηση τους. Στη συνέχεια, η ηλεκτρονική καταμέτρηση χρησιμοποιήθηκε στη Σκωτία και πάλι στις εκλογές του 2012 και του 2017 χωρίς να εντοπιστούν προβλήματα.

7.4.2 Προβλήματα, ανησυχίες και απομάκρυνση των Ευρωπαϊκών χωρών από την ηλεκτρονική ψηφοφορία

Ορισμένες ευρωπαϊκές χώρες, όπως η Ολλανδία, το Ηνωμένο Βασίλειο και η Γερμανία, έχουν πειραματιστεί με online ή και άλλες μορφές ηλεκτρονικής ψηφοφορίας και καταμέτρησης και έχουν αποφασίσει να διακόψουν ή να περιορίσουν τη χρήση τους στο μέλλον, καθώς τίθεται ζήτημα απώλειας της διαφάνειας και της ελεγκτικής ικανότητας στις διαδικασίες ψηφοφορίας και καταμέτρησης.
Στις Κάτω Χώρες, για παράδειγμα, σχετικά με τις μηχανές ψηφοφορίας Nedap και Groenendaal,[148] οι οποίες χρησιμοποιήθηκαν για να συγκεντρώσουν περίπου 90 τοις εκατό των ολλανδικών ψήφων, ανακοινώθηκε την 1η Οκτωβρίου 2007 σε έκθεση της συμβουλευτικής επιτροπής για τις εκλογές της Ολλανδίας το 2007 ότι οι αρχές της διαφάνειας, της επαληθευσιμότητας και της ελεύθερης και ισότιμης ψηφοφορίας δεν μπορούν να διασφαλιστούν επαρκώς στο πλαίσιο διαφόρων μορφών ηλεκτρονικής ψηφοφορίας, συμπεριλαμβανομένης της ψηφοφορίας μέσω διαδικτύου. Η

παραδοσιακή ψηφοφορία προσδιορίστηκε ως η προτιμώμενη επιλογή για λόγους διαφάνειας και επαλήθευσης.

Κατά την εξέταση της μελλοντικής εφαρμογής της τεχνολογίας στις διαδικασίες ψηφοφορίας και καταμέτρησης στις Κάτω Χώρες, η Επιτροπή υποστήριξε τη χρήση ψηφοδελτίων στην ψηφοφορία, η οποία επιτρέπει στους ψηφοφόρους να καταγράφουν ηλεκτρονικά την επιλογή τους και να επαληθεύουν την επιλογή τους σε έντυπη ψηφοφορία. Η έντυπη ψηφοφορία θα μπορούσε να αποθηκευτεί για καταμέτρηση των ψήφων από ανθρώπινο δυναμικό ή για σάρωση χρησιμοποιώντας τεχνολογία οπτικής αναγνώρισης χαρακτήρων και ηλεκτρονική καταγραφή. Η Επιτροπή υποστήριξε επίσης ότι η εφαρμογή της ψηφοφορίας μέσω του Διαδικτύου, ταχυδρομικώς ή και τηλεφώνου θα πρέπει να περιορίζεται σε δύο κατηγορίες ψηφοφόρων που υποστηρίζουν την αρχή της πρόσβασης. Πρώτον, όσοι δεν μπορούν να συμμετάσχουν στην ψηφοφορία λόγω σωματικών βλαβών, και δεύτερον εκείνων που ψηφίζουν από το εξωτερικό[149].

Στο Ηνωμένο Βασίλειο, η απόφαση να διακοπεί η χρήση της ηλεκτρονικής ψηφοφορίας ακολούθησε μια σειρά δοκιμών μερικών τεχνολογιών ηλεκτρονικής ψηφοφορίας σε επίπεδο τοπικής αυτοδιοίκησης. Η βρετανική εκλογική επιτροπή εξέφρασε ανησυχίες για τη διαφάνεια και την ασφάλεια και σημείωσε ότι η πλειοψηφία όσων ψήφισαν ηλεκτρονικά ήταν πιθανό να ψήφιζαν και με τον παραδοσιακό τρόπο ψηφοφορίας, επομένως τα έξοδα για το σύστημα ηλεκτρονικής ψηφοφορίας επιβάρυναν χωρίς λόγο τη χώρα[150].

Η Γερμανία χρησιμοποίησε μηχανές ηλεκτρονικής ψηφοφορίας στις θέσεις ψηφοφορίας από το 1999 έως το 2009, όταν το ομοσπονδιακό συνταγματικό δικαστήριο αποφάσισε πως η χρήση αυτών των μηχανών καθίσταται αντισυνταγματική. Το Συνέδριο διαπίστωσε ότι οι ηλεκτρονικές μηχανές ψηφοφορίας που χρησιμοποιούνται στις εκλογές του Bundestag το 2005 δεν ήταν σύμφωνες με τη συνταγματική απαίτηση της αρχής του δημοσίου χαρακτήρα των εκλογών, η οποία ορίζει ότι όλα τα ουσιώδη βήματα μιας εκλογής πρέπει να υπόκεινται στη δυνατότητα δημόσιας εξέτασης. Αυτό σημαίνει ότι οι ψηφοφόροι πρέπει να είναι σε θέση να επαληθεύσουν, χωρίς λεπτομερείς τεχνικές γνώσεις, ότι οι ψήφοι τους καταγράφονται και καταμετρούνται. Αυτό θεωρείται απαραίτητο για τη διασφάλιση της εμπιστοσύνης του εκλογικού σώματος στην ορθότητα του αποτελέσματος[151].

7.5 Ηλεκτρονική ψηφοφορία στις ΗΠΑ

Αρχικά, παρουσιάζεται το σύντομο ιστορικό της ηλεκτρονικής ψηφοφορίας στις ΗΠΑ διότι η πρώιμη εμφάνιση της την καθιστά ενδιαφέρουσα σε σύγκριση με τον υπόλοιπο κόσμο.

- 1964: Το σύστημα ψηφοφορίας οπτικής σάρωσης Norden - Coleman, το πρώτο τέτοιο σύστημα για πραγματική χρήση εγκρίθηκε στην Orange County, California[152].
- 1974: Ο Βίντεο Ψηφοφόρος (VideoVoter), η πρώτη μηχανή ψηφοφορίας DRE που χρησιμοποιείται σε κυβερνητικές εκλογές, που αναπτύχθηκε από την Frank Thornber Company στο Σικάγο, Ιλινόις, είδε την πρώτη δοκιμαστική χρήση της το 1974 κοντά στο Σικάγο[153].
- Μάρτιος 1975: Η κυβέρνηση των ΗΠΑ λαμβάνει έκθεση από τον Roy Saltman, σύμβουλο για την ανάπτυξη της εκλογικής τεχνολογίας και πολιτικών, στην οποία αναλύεται για πρώτη φορά η πιστοποίηση των μηχανών ψηφοφορίας.
- 28 Αυγούστου 1986: Ο Ομοιογενής και Υπερπόντιος Νόμος περί Απουσίας των Πολιτών του 1986 (UOCAVA) απαιτεί τα αμερικανικά κράτη να επιτρέπουν σε ορισμένες ομάδες πολιτών, οι οποίες είναι απών, να εγγραφούν και να ψηφίζουν στις εκλογές για ομοσπονδιακά γραφεία[154].
- 1990: Η FEC (Federal Election Commission) εξέδωσε ένα καθολικό πρότυπο για την ηλεκτρονική ψηφοφορία[155].
- 1996: Το Κόμμα Μεταρρύθμισης χρησιμοποιεί I-Voting (Internet Voting) για να επιλέξει τον προεδρικό του υποψήφιο. Αυτή η εκλογή είναι η πρώτη κυβερνητική εκλογή με τη χρήση αυτής της μεθόδου στις ΗΠΑ
- Μάιος 2002: Η FEC αναθεώρησε τα πρότυπα που θεσπίστηκαν για την ηλεκτρονική ψηφοφορία από το 1990.
- Νοέμβριος 2004: 4,438 των ψήφων στις γενικές εκλογές χάνονται από τις ηλεκτρονικές μηχανές ψηφοφορίας της Βόρειας Καρολίνας. Οι μηχανές

συνέχισαν να μετράνε ηλεκτρονικές ψήφους πέρα από τη χωρητικότητα μνήμης της συσκευής και οι ψήφοι χανόντουσαν ανεπανάληπτα.

- Δεκέμβριος 2005: Η ψηφοφορία του Black Box έδειξε πόσο εύκολο είναι να σπάσουμε ένα ηλεκτρονικό σύστημα ψηφοφορίας. Οι εμπειρογνώμονες υπολογιστών στην επαρχία Leon Fl, μιλούσαν για μια προσομοίωση, όπου άλλαξαν το αποτέλεσμα μιας ψεύτικης εκλογής, παραβιάζοντας τον πίνακα, χωρίς να αφήνουν στοιχεία για τις ενέργειές τους.
- 13 Σεπτεμβρίου 2006: Αποδείχθηκε ότι η ηλεκτρονική μηχανή ψηφοφορίας Diebold μπορεί να τεθεί σε πειρατεία σε λιγότερο από ένα λεπτό. Ο καθηγητής Πληροφορικής του Princeton, Edward Felten, ο οποίος εγκατέστησε ένα κακόβουλο λογισμικό που θα μπορούσε να κλέψει τις ψήφους και να τις αντικαταστήσει με ψευδείς αριθμούς χωρίς να έρθει σε φυσική επαφή με τη συσκευή ψηφοφορίας ή την κάρτα μνήμης. Το κακόβουλο πρόγραμμα μπορεί επίσης να προγραμματίσει έναν ιό που μπορεί να εξαπλωθεί από το μηχάνημα στη μηχανή.
- 21 Σεπτεμβρίου 2006: Ο κυβερνήτης του Μέριλαντ, Bob Ehrlich παρότρυνε τους πολίτες να χρησιμοποιήσουν μια εναλλακτική μέθοδο ψηφοφορίας (absentee ballot, DRE μηχανήματα) στις επερχόμενες εκλογές του Νοεμβρίου το 2006, και όχι τις ηλεκτρονικές μηχανές ψηφοφορίας του κράτους, καθώς έχουν παρουσιάσει προβλήματα στο παρελθόν (Το Maryland εισήγαγε την ηλεκτρονική ψηφοφορία το 2004 με τα μηχανήματαDiebold). Η ανακοίνωσή του αντιπροσωπεύει μια πλήρη αλλαγή της άποψης σχετικά με τα DRE.
- Σεπτεμβρίου 2009: Η Diebold, η οποία είναι υπεύθυνη για μεγάλο μέρος της τεχνολογίας στην επιχείρηση των συστημάτων των εκλογών, πουλάει την Election Systems & Software, Inc για $ 5 εκατομμύρια, λιγότερο από το 1/5 της τιμής της πριν από επτά χρόνια[156]
- 28 Οκτωβρίου 2009: Ο νόμος για την ενδυνάμωση των στρατιωτικών και των υπερπόντιων ψηφοφόρων (MOVE) απαιτεί από τα αμερικανικά κράτη να παρέχουν ψηφοδέλτια στους ψηφοφόρους της UOCAVA σε τουλάχιστον ένα ηλεκτρονικό μορφότυπο (ηλεκτρονικό ταχυδρομείο, φαξ ή ηλεκτρονικό σύστημα παράδοσης).

- Ιανουαρίου 2013: Νόμος για την Ενδυνάμωση των Εκλογών του 2013 - Αυτή η πράξη απαιτεί από κάθε αμερικανική πολιτεία να θέσει στη διάθεση του κοινού δημόσιους ιστοτόπους για την ηλεκτρονική εγγραφή ψηφοφόρων[157].
- Ιανουάριος 2019: Το DARPA χρηματοδοτεί την έρευνα και την ανάπτυξη ενός ασφαλούς συστήματος ψηφοφορίας ανοιχτού κώδικα. Η σύμβαση ύψους 10 εκατομμυρίων δολαρίων παραδόθηκε στην εταιρεία Galois με έδρα το Όρεγκον, η οποία συνεργάστηκε με άλλες κυβερνητικές υπηρεσίες όπως το Υπουργείο Εσωτερικής Ασφάλειας και η NASA. Το έργο εντάσσεται στο σύστημα SSITH (System Security Integrated Through Hardware and Firmware) της DARPA, το οποίο αναπτύσσει αρχιτεκτονικές ασφάλειας υλικού και εργαλεία που προστατεύονται καλύτερα από τις αδυναμίες υλικού που εκμεταλλεύονται το λογισμικό. Παρουσίασαν μια συσκευή με οθόνη αφής όπου οι ψηφοφόροι εισάγουν τις ψήφους τους, έναν συνδεδεμένο εκτυπωτή όπου βγαίνουν οι ψηφοφορίες και ένα μεγάλο πληκτρολόγιο ώστε να είναι εύκολη η ανάγνωση του και να μπορούν οι ψηφοφόροι να πληκτρολογήσουν με μεγαλύτερη ευκολία.

Στις ΗΠΑ παρέχεται σε όλους τους Αμερικανούς πολίτες το δικαίωμα να ψηφίζουν ελευθέρα. Ο νόμος του Τέξας έχει επιτρέψει Αμερικανούς αστροναύτες που δεν μπορούν να ψηφίσουν αυτοπροσώπως και δεν είναι σε θέση να ψηφίσουν μέσω της εκλογικής αποχής, όπως εκείνοι που βρίσκονται στο Διεθνή Διαστημικό Σταθμό και στο διαστημικό σταθμό Μιρ, να εκπέμπουν ηλεκτρονικά τις ομοσπονδιακές εκλογές από την τροχιά ήδη από το 1997. Οι ψηφοφορίες αποστέλλονται μέσω ασφαλούς ηλεκτρονικού ταχυδρομείου στο κέντρο διαστημικών πτήσεων Johnson και στη συνέχεια μεταβιβάζονται στις πατρίδες των αστροναυτών στο Τέξας[158,159].
Στα επόμενα χρόνια, τον Μάρτιο του 2000 το δημοκρατικό κόμμα της Αριζόνα στην εκλογή του προέδρου του κόμματος διοργάνωσε ψηφοφορία μέσω του διαδικτύου χρησιμοποιώντας την ιδιωτική εταιρεία votation.com[160]. Το γεγονός έλαβε σημαντική κάλυψη από τον Τύπο σε όλο τον κόσμο[161].

7.5.1 Προβλήματα και ανησυχίες σχετικά με την ηλεκτρονική ψηφοφορία στην Αμερική

Πραγματοποιήθηκαν αρκετές προσπάθειες για να σταματήσουν οι εκλογές, συμπεριλαμβανομένης και της δίκης που υποκίνησε το Σχέδιο Ακεραιότητας της Βιρτζίνια[162], το οποίο υποστήριξε ότι η ψηφοφορία μέσω του Διαδικτύου θα έπληττε τους Αφροαμερικανούς, τους Λατίνοι και τους Ιθαγενείς Αμερικανούς, όλες τις προστατευόμενες τάξεις βάσει του Νόμου περί δικαιωμάτων ψήφου. Το Σχέδιο Ακεραιότητας της Ψηφοφορίας, μαζί με δυο Αφροαμερικάνους και δύο ισπανόφωνους ενάγοντες, ισχυρίστηκε ότι, επιτρέποντας την ψηφοφορία μέσω του Διαδικτύου, οι μειονοτικές ομάδες, οι οποίες τότε είχαν λιγότερη πρόσβαση στο Διαδίκτυο, θα έχαναν το δικαίωμα ψηφοφορίας τους[163]. Ο ενάγων ζήτησε εντολή να σταματήσει η εκλογή[164]. Το δικαστήριο έπρεπε να καθορίσει εάν εφαρμόστηκε η πράξη δικαιωμάτων ψήφου και να αποφασίσει εάν οι εκλογές αδικαιολόγητα αμβλύνουν τη μειοψηφική ψήφο, δεδομένων των ισχυρισμών των εναγόντων ότι οι λευκοί ήταν πιο πιθανό να ψηφίσουν μέσω του Διαδικτύου από ό, τι οι υπόλοιποι. Στις 2 Μαρτίου 2000, ο δικαστής Paul G. Rosenblatt, του Επαρχιακού Δικαστηρίου των Ηνωμένων Πολιτειών στο Φοίνιξ, εξέδωσε την απόφασή του. Ενώ το δικαστήριο συμφώνησε με τους ενάγοντες ότι πρόκειται για δημόσια εκλογή, σημείωσε επίσης στην απόφασή του ότι υπήρχαν άλλοι τρόποι ψηφοφορίας, συμπεριλαμβανομένης της ψηφοφορίας μέσω ταχυδρομείου, και της ψηφοφορίας σε εκλογικά κέντρα, και επομένως δεν υπήρχε βάση για διακοπή των εκλογών. Το δικαστήριο αρνήθηκε το αίτημα για την αναστολή της εκλογής[165,166]. Σοβαρές ανησυχίες σχετικά με το διαδίκτυο τέθηκαν επίσης από οργανώσεις πολιτικών δικαιωμάτων στις Ηνωμένες Πολιτείες. Η υποστήριξη των Ιθαγενών Αμερικανών είναι ιδιαίτερα σημαντική στην Αριζόνα, όπου αριθμούν περισσότερους από 250.000[167]. Εκτός από αυτά τα προβλήματα, δεν έχουν λείψει και οι επιθέσεις από χάκερς στις διαδικασίες της ηλεκτρονικής ψηφοφορίας. Ισχυρές ανησυχίες έχουν προκύψει από εμπειρογνώμονες για την ασφάλεια των υπολογιστών στις Ηνωμένες Πολιτείες σχετικά με τη δυνατότητα ενός συστήματος ψηφοφορίας μέσω διαδικτύου και των επιθέσεων στον κυβερνοχώρο. Το Ινστιτούτο Πολιτικής Ίντερνετ διεξήγαγε μια μελέτη σχετικά με την ψηφοφορία στο Internet το 2001 και κατέληξε στο συμπέρασμα ότι τα συστήματα απομακρυσμένης ψηφοφορίας μέσω του Διαδικτύου ενέχουν σημαντικό κίνδυνο για την ακεραιότητα της διαδικασίας ψηφοφορίας και δεν πρέπει να χρησιμοποιούνται σε δημόσιες εκλογές μέχρις ότου αντιμετωπιστούν σημαντικά τεχνικά και κοινωνικά ζητήματα[168].

7.6 Ηλεκτρονική ψηφοφορία στην Ινδία

Η ηλεκτρονική ψηφοφορία εισήχθη για πρώτη φορά στην Ινδία το 1982 και χρησιμοποιήθηκε σε πειραματική βάση στην εκλογική περιφέρεια της Βόρειας Παραβούρ στο κρατίδιο της Κεράλα. Ο νόμος για την ηλεκτρονική ψηφοφορία στην Ινδία ήρθε ως συνέχεια του νόμου περί αντιπροσώπευσης του λαού του 1951. Το 2003, πραγματοποιήθηκαν όλες οι εθνικές και οι τοπικές εκλογές με χρήση EVM(μηχάνημα ηλεκτρονικής ψηφοφορίας). Τα μηχανήματα ηλεκτρονικής ψηφοφορίας χρησιμοποιήθηκαν επίσης κατά τις εθνικές εκλογές που διεξήχθησαν για το Κοινοβούλιο της Ινδίας το 2004 και το 2009. Σύμφωνα με τις διαθέσιμες αναφορές, περισσότερα από 400 εκατομμύρια ψηφοφόροι (περίπου το 60% των ψηφοφόρων της Ινδίας) ψήφισαν και η καταμέτρηση των ψήφων διήρκησε μόνο λίγες ώρες. Τον Απρίλιο του 2011, το Γκουτζαράτ έγινε το πρώτο ινδικό κρατίδιο που εφάρμοσε με την ψηφοφορία μέσω διαδικτύου.

Συμπεράσματα

Μετά τη διεξοδική μελέτη που διεξάχθηκε για τις ανάγκες συγγραφής της παρούσας εργασίας, προέκυψαν ορισμένα συμπεράσματα σχετικά με την ηλεκτρονική ψηφοφορία.

Πρώτα απ' όλα πρέπει να επισημανθεί πως όσα πλεονεκτήματα αναφέρονται από την εφαρμογή της ηλεκτρονικής ψηφοφορίας, επαληθεύονται από την βιβλιογραφική ανασκόπηση. Η ηλεκτρονική ψηφοφορία είναι μια αποτελεσματική λύση για γρήγορη και αποτελεσματική καταμέτρηση των ψήφων σε χώρες με μεγάλο πληθυσμό όπως η Ινδία ή οι ΗΠΑ. Ακόμη, η γραφειοκρατία αποδεδειγμένα μειώνεται, ενώ μειώνονται και τα κόστη της εκλογικής διαδικασίας.

Ταυτόχρονα, ορισμένες χώρες όπως το Ηνωμένο Βασίλειο τονίζουν ότι το κόστος εγκαθίδρυσης του συστήματος ηλεκτρονικής ψηφοφορίας είναι από μόνο του πολυδάπανο. Επίσης, δεν είναι λίγες οι περιπτώσεις όπου αναφέρθηκαν ανησυχίες των πολιτών και έλλειψη εμπιστοσύνης στα συστήματα ηλεκτρονικής ψηφοφορίας εκ μέρους των ψηφοφόρων. Ακόμη, σε περιοχές όπου επικρατεί ο πληροφορικός αναλφαβητισμός, παρατηρήθηκε πως δημιουργούνται προβλήματα καθώς οι ψηφοφόροι αδυνατούν να συμμετάσχουν.

Καθώς δεν έχει εδραιωθεί ένα απόλυτα ασφαλές σύστημα ηλεκτρονικής ψηφοφορίας οι αναπτυγμένες χώρες της Ευρώπης έχουν απομακρυνθεί από την εφαρμογή της ηλεκτρονικής ψηφοφορίας.

Στην παραδοσιακή ψηφοφορία όλοι γνωρίζουν και κατανοούν πως λειτουργεί το σύστημα και μπορούν, ακόμη αν το επιθυμούν να παρακολουθήσουν την καταμέτρηση των ψηφοδελτίων. Εν αντιθέσει με την ηλεκτρονική ψηφοφορία όπου καμία εμπορική ηλεκτρονική πλατφόρμα ψηφοφορίας δεν καθιστά τον πηγαίο κώδικα διαθέσιμο για δημόσιο έλεγχο.

Ωστόσο, λανθάνει η πιθανότητα τα ψηφιακά συστήματα ηλεκτρονικής ψηφοφορίας να μην παρουσιάσουν αδυναμίες, τις οποίες ενδέχεται να εκμεταλλεύονται τα κράτη για να καλλιεργήσουν τη δημόσια δυσπιστία σχετικά με τη διαδικασία και τα αποτελέσματα των εκλογών ούτως ώστε να επαναληφθούν οι εκλογές. Επίσης, ενώ οι μη ασφαλείς μηχανές ψηφοφορίας τράβηξαν την μεγαλύτερη προσοχή από τις προεδρικές εκλογές των ΗΠΑ το 2016, τα κράτη και οι δήμοι εξακολουθούν να

χρησιμοποιούν την ηλεκτρονική ψηφοφορία, συμπεριλαμβανομένων 31 κρατών στις ΗΠΑ, δύο επαρχίες στον Καναδά και δύο κράτη στην Αυστραλία. Ακόμη, η Εσθονία συγκαταλέγεται στις χώρες που χρησιμοποιούν την ηλεκτρονική ψηφοφορία. Η Ουαλία στο Ηνωμένο Βασίλειο είναι μια περίπτωση από τις χώρες που ασκούν μεγάλη πίεση για την ηλεκτρονική ψηφοφορία.
Οι ερευνητές της ασφάλειας επισημαίνουν τα ελαττώματα στην ηλεκτρονική ψηφοφορία, παρόλα αυτά οι εκλογικοί αξιωματούχοι τείνον να αγνοούν τα ζητήματα ασφαλείας που απειλούν την ακεραιότητα των αποτελεσμάτων της ψηφοφορίας. Με αποτέλεσμα να τίθεται το ερώτημα για το αν το κλειστό λογισμικό ηλεκτρονικής ψηφοφορίας αποτελεί απειλή για την δημοκρατία.

Τα τελευταία χρόνια παρατηρήθηκε σταθερή αύξηση της δημοτικότητας της ηλεκτρονικής ψηφοφορίας σε πολλές χώρες της Ευρώπης και στον υπόλοιπο κόσμο, συμπεριλαμβανομένης της Εσθονίας, της Ελβετίας, των Ηνωμένων Πολιτειών και της Αυστραλίας. Η υιοθέτηση μοντέλων ηλεκτρονικής ψηφοφορίας στις εγχώριες εκλογές και τα δημοψηφίσματα συζητούνται ευρέως όχι μόνο μεταξύ των μελών των κοινοβουλίων και των υπουργών εθνικής κυβέρνησης, αλλά και του πληθυσμού που ψηφίζει γενικά. Συγκεκριμένα, οι νέες τεχνολογίες ψηφοφορίας παρέχουν ένα όφελος με το οποίο οι ψηφοφόροι, εξαλείφουν το εμπόδιο της απόστασης μεταξύ αυτών και των εκλογικών κέντρων.

Άλλα πλεονεκτήματα της ηλεκτρονικής ψηφοφορίας, τα οποία είναι οργανωτικής και διαδικαστικής φύσης (π.χ. ψηφοφορία ψηφοφορίας), λειτουργούν προς όφελος τόσο των διαχειριστών όσο και των πολιτικών.

Ωστόσο, πρέπει να έχουμε κατά νου τα μειονεκτήματα της ηλεκτρονικής ψηφοφορίας που σχετίζονται ιδίως με την ασφάλεια της ψηφοφορίας και της καταμέτρησης των ψήφων στις εκλογές και τα δημοψηφίσματα. Παρά τα επίμονα τεχνικά ζητήματα που σχετίζονται με την ασφάλεια των εκλογών κ.λπ., το ευρύ φάσμα των οφελών που μπορούν να απολαμβάνουν διάφορα τμήματα της κοινωνίας, όπως ψηφοφόροι, πολιτικοί και διοικητικοί υπάλληλοι, καθώς και η θετική εμπειρία πολλών χωρών, μπορεί να προσφέρουν ένα ισχυρό κίνητρο για την υιοθέτηση της ηλεκτρονικής ψηφοφορίας.

Αν και σίγουρα θα χρειαστεί πολύς χρόνος προτού τεθεί σε εφαρμογή ένα μοντέλο ηλεκτρονικής ψηφοφορίας, δεν πρέπει να παραβλέψουμε τη δημοφιλή έγκριση για ηλεκτρονική ψηφοφορία που αποδεικνύεται από την έρευνα που πραγματοποιήθηκε σε αυτήν την εργασία.

Όμως δεν μπορούμε να παραλείψουμε το γεγονός πως, μετά από έρευνα και χρόνια προσπάθειας ύψους $ 100 εκατομμυρίων δολαρίων, το NIST (το αμερικανικό ινστιτούτο για τα πρότυπα ασφάλειας στον κυβερνοχώρο) το οποίο έχει επιφορτιστεί με την εξέταση του θέματος, κατέληξε στο συμπέρασμα ότι η ηλεκτρονική ψηφοφορία είναι αδύνατη. Αναφέροντας συγκεκριμένα πως «Δεν είναι ξεκάθαρο ότι τα ηλεκτρονικά απομακρυσμένα συστήματα μπορούν να προσφέρουν υψηλό επίπεδο ελεγκτικής συμπεριφοράς στα συστήματα ψηφοφορίας. Καθίσταται εξαιρετικά δύσκολο η επικύρωση και η επαλήθευση του λογισμικού στους απομακρυσμένους servers του ηλεκτρονικού συστήματος ψηφοφορίας και στους προσωπικούς υπολογιστές των χρηστών. Επομένως, η διασφάλιση της δυνατότητας ελέγχου των απομακρυσμένων ηλεκτρονικών συστημάτων ψηφοφορίας παραμένει σε μεγάλο βαθμό ένα δύσκολο πρόβλημα ».

Ελπιδοφόρες μπορούν να χαρακτηριστούν κάποιες έρευνες και μετατροπές που πραγματοποιούνται όπως αυτή των Thomas Haines και Xavier Boyen η οποία αποτελεί μια βελτιωμένη έκδοση του συστήματος ψηφοφορίας Prˆet-`a-Voter του Ryan, το οποίο παρέχει προστασία της ιδιωτικότητας σε ad hoc συσκευές για ψηφοφορία η οποίες δεν έχουν κάποια εξάρτηση από άλλους ή προηγούμενους κωδικούς ασφαλείας ή από κάποια ατομική έμπιστη συσκευή. Επιπλέον, η βελτίωση τους προστατεύει το απόρρητο της δημιουργίας και αποθήκευσης της ψηφοφορίας καθώς δεν απαιτείται το περιεχόμενο να είναι πλέον μυστικό, ενώ ταυτόχρονα επιλύει το πρόβλημα της προώθησης του απορρήτου και της δυνατότητας ελέγχου των εκτυπωτών. Η λύση τους βασίζεται στην χρήση αυτόματης και αυτόνομης ανάμιξης των ψήφων αλλά και την επιπλέον κρυπτογράφηση τους εντός του εκλογικού θαλάμου.

Ενώ η ανάγκη για πρόσθετο υλικό εντός θαλάμου μπορεί να το καταστήσει ακατάλληλο για ορισμένα σενάρια ψηφοφορίας, υποστηρίζουν ότι τα οφέλη υπερτερούν του κόστους, ιδίως σε περιπτώσεις όπου οι ψηφοφόροι δεν επιθυμούν να εμπιστευτούν την εκλογική αρχή. Η μέθοδος τους φαίνεται ανεφάρμοστη στο STAR-Vote ή σε οποιοδήποτε σχήμα που χρησιμοποιεί άμεση κρυπτογράφηση.

Κλείνοντας, χωρίς τη δυνατότητα ελέγχου των εκλογών για παρατυπίες, η ηλεκτρονική ψηφοφορία καθιστά αδύνατη την εμπιστοσύνη στα αποτελέσματα οποιασδήποτε εκλογής που χρησιμοποιεί αυτή την τεχνολογία και αμφισβητεί τα αποτελέσματα των παλαιότερων εκλογών οι οποίες πραγματοποιήθηκαν με τέτοια μέσα. Επομένως, στην εποχή της ηλεκτρονικής ψηφοφορίας, δεν αρκεί να παράγουμε ένα αποτέλεσμα αλλά πρέπει να υπάρχει εμπιστοσύνη στο αποτέλεσμα, πρέπει το κοινό να έχει εμπιστοσύνη στο αποτέλεσμα και πρέπει να δοθεί ένας λόγο στους ανθρώπους να έχουν αυτή την εμπιστοσύνη.

Παράρτημα Α

Ορισμοί

Voting Booth: Μια φυσική συσκευή με την οποία ένας ψηφοφόρος μπορεί να επικοινωνεί διαδραστικά με ένα κόμμα, διατηρώντας την επικοινωνία απόλυτα μυστική σε όλα τα άλλα κόμματα.

Zero-Knowledge Proofs: Πιθανές αποδείξεις που καταδεικνύουν, έως το επιθυμητό επίπεδο βεβαιότητας, μέλος της φυσικής γλώσσας χωρίς να μεταφέρουν επιπλέον γνώσεις. Με άλλα λόγια, zero-knowledge proofs χρησιμοποιούνται για να αποδείξουν τη γνώση των πληροφοριών χωρίς να αποκαλύψουν τίποτα γι 'αυτήν.

Blind Signatures: Μια ειδική κατηγορία ψηφιακών υπογραφών. Ο στόχος των τυφλών υπογραφών είναι να επιτρέψει σε μια οντότητα Α να αποκτήσει υπογραφή άλλης οντότητας Β σε ένα μήνυμα m χωρίς να αποκαλύψει το m στο Β. Οι τυφλές υπογραφές χρησιμοποιούνται στην ηλεκτρονική ψηφοφορία ως μέθοδος επικύρωσης ψήφων.

Anonymous channels.: Αυτά διασφαλίζουν την ανωνυμία των ψηφοφόρων. Έχουν προταθεί συστήματα που βασίζονται σε διακομιστές μεσολάβησης όπως το Anonymizer και το σύστημα LPWA. Μια διαφορετική προσέγγιση, η οποία συνδυάζει αρκετά χαρακτηριστικά τόσο των συνδυασμένων διχτυών όσο και των συστημάτων μεσολάβησης είναι το σύστημα CROWDS

Βιβλιογραφία

1. Lance J. Hoffman. "Internet voting: will it spur or corrupt democracy?" Proceedings of the tenth conference on Computers, freedom privacy: challenging the assumptions, 2000, Pages 219 - 223.

2. R. G. Saltman, Accuracy, Integrity, and Security in Computerised Vote-Tallying (Washington: U.S. Department of Commerce, 1998).
3. David Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, 1979
4. Benaloh, J.C. & Yung, M. Distributing the Power of a Government to Enhance the Privacy of Voters. Proc. of 5th Annual ACM Symposium on Principles of Distributed Computing, pp. 52-62, 1986.
5. Sako, K. & Kilian, J. Secure Voting Using Partially Compatible Homomorphisms. Proc. of Crypto '94, LNCS 839, pp. 411-424, 1994.
6. Cramer, R., Franklin, M., Schoenmakers, B. & Yung, M. Multi-Authority Secret-Ballot Elections with Linear Work. Proc. of Eurocrypt '96, LNCS 1070, pp. 72- 83, 1996.
7. Cramer, R., Gennaro, R. & Schoenmakers, B. A Secure and Optimally Efficient Multi-Authority Election Scheme. Proc. of Eurocrypt '97, LNCS 1233, pp. 103-118, 1997.
8. Cranor, L.F. Electronic Voting: Computerized Polls May Save Money, Protect Privacy. ACM Crossroads, April 1996.
9. Rivest, R. "Electronic Voting". In Financial Cryptography '01, http://theory.lcs.mit.edul-rivestlRivest-Electronic Voting-ppt.pdf
10. Rubin, A. "Security Considerations for Remote E-Voting over the Internet", AT&T Labs Research, June 2001. http://avirubin.comle-voting.security.html
11. California Internet Voting Task Force. A Report on the Feasibility of Internet Voting, Jan 2000. http://www.ss.ca.gov/executive/ivotel
12. Coleman, S. "Elections in the 21st Century: From Paper Ballot to E-Voting". Report by the Independent Commission on Alternative Voting Methods, London, Electoral Reform Society, February 2002.
13. Internet Policy Institute. Report of the National Workshop on Internet Voting, March 2001, www.internetpolicy.org.
14. Schneier, B., Applied Cryptography - Protocols, Algorithms and Source Code in C. 2nd Edition, 1996.
15. Kersting, N., Baldersheim, H.: Electronic voting and democratic issues an introduction. In: Kersting, N., Baldersheim, H. (eds.) Electronic Voting and Democracy A comparative Analysis, p. 11. Palgrave Macmillan, New York (2004)
16. Maurer, A.D.: Legality, separation of powers, stability of electoral law, the impact of new voting technologies. In: 1st Scientific Electoral Expert Debate, Bucharest (2016)
17. Caarls, S.: E-Voting Handbook: Key Steps in the Implementation of E-Enabled Elections. Council of Europe, Strasbourg (2010)
18. Hall, T.E., Wang, T.A.: International principles for election integrity. In: Alvarez, R.M., Hall, T.E., Hyde, S.D. (eds.) Election Fraud: Detecting and Deterring Electoral Manipulation, p. 49. Brookings Institution Press, Washington, D.C. (2008)
19. Alvarez, M.R., Hall, T.E.: Electronic Elections: The Perils and Promises of Digital Democracy, p. 184. Princeton University Press, Princeton (2008)

20. Schwartz, D., Grice, D.: Establishing a legal framework for e-voting in Canada. Elections Canada (2013)
21. Hall, T.E., Wang, T.A.: International principles for election integrity. In: Alvarez, R.M., Hall, T.E., Hyde, S.D. (eds.) Election Fraud: Detecting and Deterring Electoral Manipulation, p. 40. Brookings Institution Press, Washington, D.C. (2008)
22. International IDEA: Introducing Electronic Voting: Essential Considerations, Policy Paper, December 2011
23. Goldsmith, B., Ruthrauff, H.: Implementing and Overseeing Electronic Voting and Counting Technologies. International Foundation for Electoral Systems and National Democratic Institute, Washington, D.C. (2013)
24. Electronic Voting: Challenges and Opportunities. Ministry of Local Government and Regional Development (2006)
25. Lauer, T.W.: The risk of e-voting. Electron. J. E-gov. 2(3), 177–186 (2004)
26. Gross, O.: Constitutions and emergency regimes. In: Ginsburg, T., Dixon, R. (eds.) Comparative Constitutional Law, p. 348. Edward Elgar Publishing Limited, Cheltenham (2011)
27. Alvarez, R.M., et al.: Machines versus humans: the counting and recounting of prescored punchcard ballots. In: Alvarez, R.M., Atkeson, L.R., Hall, T.E. (eds.) Confirming Elections, Creating Confidence and Integrity through Election Auditing, p. 83. Palgrave MacMillan, New York (2012)
28. Ryan, P.: A variant of the Chaum voter-verifiable scheme. In: Proceedings of the 2005 Workshop on Issues in the Theory of Security, pp. 81–88. ACM (2005)
29. Chaum, D.: Secret-ballot receipts: true voter-verifiable elections. IEEE Secur. Priv. 2(1), 38–47 (2004)
30. . Ryan, P.Y.A., Teague, V.: Ballot permutations in pret a voter. In: Proceedings of Electronic Voting Technology/Workshop on Trustworthy Elections (2009)
31. Abe, M.: Mix-networks on permutation networks. In: Lam, K.-Y., Okamoto, E.,Xing, C. (eds.) ASIACRYPT 1999. LNCS, vol. 1716, pp. 258–273. Springer,
32. Chaum, D.: Untraceable mail, return addresses and digital pseudonyms. Commun. ACM 24(2), 84–88 (1981)
33. Chaum, D., Ryan, P.Y.A., Schneider, S.: A practical voter-verifiable election scheme. In: Vimercati, S.C., Syverson, P., Gollmann, D. (eds.) ESORICS 2005.
34. Park, C., Itoh, K., Kurosawa, K.: Efficient anonymous channel and all/nothing election scheme. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 248–259. Springer, Heidelberg (1994). doi:10.1007/3-540-48285-7 21
35. Sako, K., Kilian, J.: Receipt-free mix-type voting scheme. In: Guillou, L.C., Quisquater, J.-J. (eds.) EUROCRYPT 1995. LNCS, vol. 921, pp. 393–403. Springer, Heidelberg (1995). doi:10.1007/3-540-49264-X 32
36. Wikstr¨om, D.: A universally composable mix-net. In: TCC, pp. 317–335 (2004)
37. Benaloh, J.: Verifiable secret-ballot elections. Ph.D. thesis, Yale University (1987)
38. Cohen, J.D., Fischer, M.J.: A robust and verifiable cryptographically secure election scheme. In: FOCS, pp. 372–382 (1985)
39. Cramer, R., Franklin, M., Schoenmakers, B., Yung, M.: Multi-authority secretballot elections with linear work. In: Maurer, U. (ed.) EUROCRYPT 1996.

LNCS, vol. 1070, pp. 72–83. Springer, Heidelberg (1996). doi:10.1007/3-540-68339-9 7
40. Hirt, M., Sako, K.: Efficient receipt-free voting based on homomorphic encryption. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 539–556. Springer, Heidelberg (2000). doi:10.1007/3-540-45539-6 38
41. Chaum, D.: Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA. In: Barstow, D., et al. (eds.) EUROCRYPT 1988. LNCS, vol. 330, pp. 177–182. Springer, Heidelberg (1988). doi:10.1007/3-540-45961-8 15
42. Fujioka, A., Okamoto, T., Ohta, K.: A practical secret voting scheme for large scale elections. In: Seberry, J., Zheng, Y. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 244–251. Springer, Heidelberg (1993). doi:10.1007/3-540-57220-1 66
43. Okamoto, T.: An electronic voting scheme. In: Terashima, N., Altman, E. (eds.) Advanced IT Tools, pp. 21–30. Springer, New York (1996)
44. Okamoto, T.: Receipt-free electronic voting schemes for large scale elections. In: Christianson, B., Crispo, B., Lomas, M., Roe, M. (eds.) Security Protocols 1997. LNCS, vol. 1361, pp. 25–35. Springer, Heidelberg (1998). doi:10.1007/BFb0028157
45. Carback, R., Chaum, D., abd John Conwaym, J.C., Essex, A., Hernson, P.S., Mayberry, T., Popoveniuc, S., Rivest, R.L., Shen, E., Sherman, A.T., Vora, P.L.: Scantegrity II municipal election at Takoma Park: the first E2E binding governmental election with ballot privacy. In: Proceedings of USENIX Accurate Electronic Voting Technology Workshop (2010)
46. Essex, A., Clark, J., Hengartner, U., Adams, C.: How to print a secret. In: Proceedings of USENIX Hot Topics in Security (2009)
47. Grundland, E.: An analysis of the wombat voting system model (2012)
48. Benaloh, J., Byrne, M., Kortum, P.T., McBurnett, N., Pereira, O., Stark, P.B., Wallach, D.S.: Star-vote: a secure, transparent, auditable, and reliable voting system. CoRR abs/1211.1904 (2012)
49. Moran, T., Naor, M.: Split-ballot voting: everlasting privacy with distributed trust. ACM Trans. Inf. Syst. Secur. 13(2), 16 (2010)
50. Chaum, D., Carback, R., Clark, J., Essex, A., Popoveniuc, S., Rivest, R.L., Ryan, P.Y.A., Shen, E., Sherman, A.T.: Scantegrity ii: end-to-end verifiability for optical scan election systems using invisible ink confirmation codes. In: EVT. USENIX Association (2008)
51. Gogolewski, M., Klonowski, M., Kubiak, P., Kutylowski, M., Lauks, A., Zag´orski, F.: Kleptographic attacks on e-voting schemes. In: M¨uller, G. (ed.) ETRICS 2006. LNCS, vol. 3995, pp. 494–508. Springer, Heidelberg (2006). doi:10.1007/ 11766155 35
52. Culnane, C., Heather, J., Joaquim, R., Ryan, P.Y.A., Schneider, S., Teague, V.: Faster print on demand for prˆet `a voter. J. Election Technol. Sys. 2(1), 1–14 (2013)
53. Ryan, P.: The computer ate my vote. In: Boca, P., Bowen, J.P., Siddiqi, J. (eds.) Formal Methods: State of the Art and New Directions, pp. 147–184. Springer, London (2010)
54. Lee, B., Boyd, C., Dawson, E., Kim, K., Yang, J., Yoo, S.: Providing receipt freeness in mixnet-based voting protocols. In: Lim, J.-I., Lee, D.-H. (eds.) ICISC 2003. LNCS,

vol. 971, pp. 245–258. Springer, Heidelberg (2004). doi:10.1007/978-3-540-24691-6 19
55. Ryan, P.Y.A., Teague, V.: Ballot permutations in pret a voter. In: Proceedings of Electronic Voting Technology/Workshop on Trustworthy Elections (2009)
56. Aditya, R., Lee, B., Boyd, C., Dawson, E.: An efficient mixnet-based voting scheme providing receipt-freeness. In: Katsikas, S., Lopez, J., Pernul, G. (eds.) TrustBus 2004. LNCS, vol. 3184, pp. 152–161. Springer, Heidelberg (2004). doi:10.1007/978-3-540-30079-3 16
57. Adeshina, S.A.: Towards improved adoption of e-voting - analysis of the case of Nigeria. In: 8th ACM International Conference on Theory and Practice of Electronic Governance, Portugal (2014)
58. Pomares, J., et al.: From piloting to roll-out: voting experience and trust in the first full e-election in Argentina. In: IEEE 6th International Conference on Electronic Voting.Lochau/Bregenz, Austria (2014)
59. Kuye, C.O., et al.: Design and analysis of electronic voting system in Nigeria. Int. Arch.Appl. Sci. Technol. 4(2), 15–20 (2013)
60. Ishaq, S.R., et al.: Adoption of e-voting system in Nigeria: a conceptual framework. Int. J. Appl. Inf. Syst. 5(5), 8–14 (2013)
61. Ayo, C., Adebiyi, A., Sofoluwe, A.B.: E-voting implementation in Nigeria: the successfactors, In: Salawu, R.I. (ed.) Curbing Political Violence in Nigeria: The Role of Security Profession, Institute of Security, pp. 50–60. Mukagamu and Brothers Ent., Nigeria (2009)
62. . Musa, M., Aliyu, F.: Design of electronic voting systems for reducing election process. Int. J. Recent Technol. Eng. 2(1), 183–186 (2013)
63. Olaniyi, O.M., et al.: Framework for multilingual mobile e-voting service infrastructure fordemocratic governance. Afr. J.Comput. ICT 4(3), 23–32 (2011)
64. Yadav, S., Singh, A.: A biometric traits-based authentication system for Indian voting system. Int. J. Comput. Appl. 65(15), 28–32 (2013)
65. Filho, J.R.: E-Voting in Brazil - Reinforcing institutions while diminishing citizenship. In:Electronic Voting 2008, Caste Hofen, Bregenz, Austria (2008)
66. . Avgerou, C., et al.: ICT and Citizens' trust in government: lessons from electronic voting in Brazil. In: 9th International Conference on Social Implications of Computers in Developing Countries, Sao Paulo, Brazil (2007)
67. Filho, J.R.: E-Voting and the creation of trust for socially marginalized citizens in Brazil.eJ. eDemocr. Open Govern. 2(2), 184–193 (2016)
68. Khan, G.F., et al.: A Socio-technical perspective on e-government issues in developing countries: a scientometrics approach. Scientometrics 87, 267–286 (2011)
69. Bostrom, R.P., Heinen, J.S.: MIS problems and failures: a socio-technical perspective part I: the causes. MIS Q. 1(3), 17–32 (1977)
70. Bostrom, R.P., Heinen, J.S.: MIS problems and failures: a socio-technical perspective part I: the causes. MIS Q. 1(3), 17–32 (1977)
71. Heeks, R., Bailur, S.: Analyzing E-government research: perspectives, philosophies, theories, methods, and practice. Gov. Inf. Q. 24, 243–265 (2007)
72. Oostveen, A.-M.: Users' experiences with e-voting: a comparative case study. Int.J. Electron. Gov. 2(4), 357–377 (2009)

73. Al-Shammari, A., Villafiorita, A., Weldemariam, K.: Understanding the development trends of electronic voting systems. In: Seventh International Conference on Availability, Reliability and Security (2012)
74. Prandini, M., Sartori, L., Oostveen, A.-M.: Why electronic voting? In: Conference foreDemocracy and open Government (2014)
75. Kling, R.: Learning about information technologies and social change: the contribution of social informatics. Inf. Soc. Int. J. 16(3), 217–232 (2000)
76. Oostveen, A.-M.: Users' experiences with e-voting: a comparative case study. Int.J. Electron. Gov. 2(4), 357–377 (2009)
77. Gauld, R., Goldfinch, S.: Dangerous Enthusiasms: E-government, computer failure and information systems development. Otago University Press, Dunedin (2006)
78. Benoist, E., Anrig, B., Jaquet-Chiffelle, D.-O.: Internet-voting: opportunity or threat for democracy? In: Alkassar, A., Volkamer, M. (eds.) Vote-ID 2007. LNCS, vol. 4896, pp. 29–37.Springer, Heidelberg (2007). doi:10.1007/978-3-540-77493-8_3
79. Oostveen, A.-M.: Outsourcing democracy: losing control of e-voting in the Netherlands. Policy Internet 2(4), 201–220 (2010)
80. Liptrott, M.: e-Voting: Same pilots, same problems, different agendas. Electron. J. E-Gov.5(2), 205–212 (2007)
81. Moynihan, D.P.: Building secure elections: e-voting, security, and systems theory. Pub.Adm. Rev. 64(5), 515–528 (2004)
82. Oostveen, A.-M.: Outsourcing democracy: losing control of e-voting in the Netherlands.Policy Internet 2(4), 201–220 (2010)
83. Moynihan, D.P.: Building secure elections: e-voting, security, and systems theory. Pub.Adm. Rev. 64(5), 515–528 (2004)
84. Robert Krimmer · Melanie Volkamer, Jordi Barrat · Josh Benaloh, Nicole Goodman · Peter Y.A. Ryan, Vanessa Teague (Eds.), Lecture Notes in Computer Science, Electronic Voting, First International Joint Conference, E-Vote-ID 2016, Bregenz, Austria, October 18–21, 2016, Proceedings
85. Robert Krimmer · Melanie Volkamer, Jordi Barrat · Josh Benaloh, Nicole Goodman · Peter Y.A. Ryan, Vanessa Teague (Eds.), Lecture Notes in Computer Science, Electronic Voting, First International Joint Conference, E-Vote-ID 2016, Bregenz, Austria, October 18–21, 2016, Proceedings
86. Alvarez, R. M., Hall, T. E., &Trechsel, A. H. (2009). Internet Voting in Comparative Perspective: The Case of Estonia. PS: Political Science and Politics (42), 497-505
87. Elections BC, Discussion Paper: Internet Voting, August 2011
88. https://www.elections.nsw.gov.au/Postal-voting-and-iVote-applications
89. Chowdhury, M. J. (2010, September 6). Comparison of e-voting schemes: Estonian and Norwegian solutions.
90. Serdult, Uwe (2015). "Fifteen years of internet voting in Switzerland [History, Governance and Use]". 2015 Second International Conference on e Democracy & e Government (ICEDEG). IEEE. pp. 126–132. doi:10.1109/ICEDEG.2015.7114482. ISBN 978-3-9075-8910-6.
91. Fenazzi, Urs Geiser, swissinfo ch/urs with additional input Sonia. "E-voting to be introduced permanently". SWI swissinfo.ch. Retrieved 2019-02-08.
92. https://www.bfs.admin.ch/bfs/portal/de/index/themen/17/02/blank/key/national_rat/wahlbeteiligung.html

93. Milic, Thomas. "Attitudes Of Swiss Citizens Toward The Generalisation Of E-Voting" https://www.zdaarau.ch/dokumente/SB-10-Evoting-ZDA.pdf. Zentrum für Demokratie Aarau. Zentrum für Demokratie Aarau. Retrieved 9 May 2019.
94. swissinfo.ch, S. W. I.; Corporation, a branch of the Swiss Broadcasting. https://www.swissinfo.ch/eng/politics/online-democracy_opposition-against-e-voting-project-gathers-pace/44708930. SWI swissinfo.ch. Retrieved 2019-02-10
95. Goodman, N., Pammett, J. H., &DeBardeleben, J. (2010). A Comparative Assessment of Electronic Voting. Ottawa: Elections Canada.
96. Alvarez, R. M., Hall, T. E., &Trechsel, A. H. (2009). Internet Voting in ComparativePerspective: The Case of Estonia. PS: Political Science and Politics (42), 497-505
97. Serdult, Uwe (2015). "Fifteen years of internet voting in Switzerland [History, Governance and Use]". 2015 Second International Conference on e Democracy & e Government (ICEDEG). IEEE. pp. 126–132. doi:10.1109/ICEDEG.2015.7114482. ISBN 978-3-9075-8910-6.
98. Krimmer, Robert; Volkamer, Melanie; Cortier, Véronique; Duenas-Cid, David; Goré, Rajeev; Hapsara, Manik; Koenig, Reto; Martin, Steven; McDermott, Ronan; Roenne, Peter; Serdült, Uwe; Truderung, Tomasz. "Third Joint International Conference on Electronic Voting E-Vote-ID 2018". https://www.researchgate.net/publication/327980266_Third_International_Joint_Conference_on_Electronic_Voting_E-Vote-ID_2018_TUT_Press_Proceedings
99. (Wikipedia, 2020), https://en.wikipedia.org/wiki/Electronic_voting_in_Switzerland
100. Gasser, Urs; Gerlach, Jan. "hree Case Studies from Switzerland: E-Voting. Berkman Center, Mar. 2009" https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/Gerlach-Gasser_SwissCases_Evoting.pdf.
101. Krimmer, Robert; Volkamer, Melanie; Cortier, Véronique; Duenas-Cid, David; Goré, Rajeev; Hapsara, Manik; Koenig, Reto; Martin, Steven; McDermott, Ronan; Roenne, Peter; Serdült, Uwe; Truderung, Tomasz. "Third Joint International Conference on Electronic Voting E-Vote-ID 2018". https://www.researchgate.net/publication/327980266_Third_International_Joint_Conference_on_Electronic_Voting_E-Vote-ID_2018_TUT_Press_Proceedings
102. Buchsbaum, Thomas M. ""E-Voting: International Developments and Lessons Learnt ." Security Assets in E-Voting, Research Gate, Jan. 2004" https://www.researchgate.net/publication/220789172_Security_Assets_in_E-Voting
103. Franke, Daniel. "Security Analysis of the Geneva e-Voting System. TU Darmstadt" https://subs.emis.de/LNI/Proceedings/Proceedings220/789.pdf
104. Zetter, Kim. "Researchers Find Critical Backdoor in Swiss Online Voting System" https://www.vice.com/en_us/article/zmakk3/researchers-find-critical-backdoor-in-swiss-online-voting-system
105. Zetter, Kim "Experts Find Serious Problems With Switzerland's Online Voting System" https://www.vice.com/en_us/article/vbwz94/experts-find-serious-problems-with-switzerlands-online-voting-system-before-public-penetration-test-even-begins

106. Franke, Daniel "Security Analysis of the Geneva e-Voting System. TU Darmstadt" https://subs.emis.de/LNI/Proceedings/Proceedings220/789.pdf
107. Buchsbaum, Thomas M. ""E-Voting: International Developments and Lessons Learnt ." Security Assets in E-Voting, Research Gate, Jan. 2004" https://www.researchgate.net/publication/220789172_Security_Assets_in_E-Voting
108. Krimmer, Robert; Volkamer, Melanie; Cortier, Véronique; Duenas-Cid, David; Goré, Rajeev; Hapsara, Manik; Koenig, Reto; Martin, Steven; McDermott, Ronan; Roenne, Peter; Serdült, Uwe; Truderung, Tomasz. "Third Joint International Conference on Electronic Voting E-Vote-ID 2018". https://www.researchgate.net/publication/327980266_Third_International_Joint_Conference_on_Electronic_Voting_E-Vote-ID_2018_TUT_Press_Proceedings
109. http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics
110. "Verifiable Internet Voting in Estonia" http://research.cyber.ee/~jan/publ/mobileverification-ieee.pdf
111. https://kov2017.valimised.ee/valimistulemus-vald.html
112. https://rk2019.valimised.ee/en/voting-result/voting-result-main.html
113. Madise, Ü., Martens, T.: E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. In: Krimmer, R. (ed.) Electronic Voting 2006, vol. P-87, pp. 27–35. Gesellschaft für Informatik, Bonn (2006)
114. Maaten, E.: Towards remote E-voting: Estonian case. In: Prosser, A.,Krimmer, R. (eds.) Electronic Voting in Europe Technology, Law, Politics and Society, vol. P-47, pp. 83–90. GI,Bregenz (2004)
115. Vassil, K., Solvak, M., Vinkel, P.: E-valimiste levik Eesti valijate hulgas. Riigikogu Toimetised (Parliamentary Journal) 30(2), 116–128 (2014)
116. Ehin, P., Madise, Ü., Solvak, M., Taagepera, R., Vassil, K., Vinkel, P.: Independent candidates in National and European elections: study, Brussels (2013)
117. Heinsalu, A., Koitmäe, A., Pilving, M., Vinkel, P.: Elections in Estonia 1992–2015. National Electoral Committee, Tallinn (2016)
118. Vassil, K., Solvak, M.: Ten years of internet voting in Estonia: overview of research on internet voting in 2005–2014. Seminar on 22 January 2015 (2015)
119. Vassil, K., Solvak, M.: E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005–2015) (2016)
120. Madise, Ü., Vinkel, P.: Internet voting in Estonia: from constitutional debate to evaluation of experience over six elections. In: Kerikmäe, T. (ed.) Regulating eTechnologies in the European Union, pp. 1–19. Springer, Berlin (2014)
121. Trechsel, A.: Internet voting in the March 2007 parliamentary elections in Estonia. Report for the council of Europe (2007)
122. Trechsel, A., Vassil, K.: Internet voting in Estonia: a comparative analysis of five elections since 2005 (2011)
123. Spycher, O., Volkamer, M., Koenig, R.: Transparency and technical measures to establish trust in Norwegian internet voting. In: Kiayias, A., Lipmaa, H. (eds.) Vote-ID 2011. LNCS, vol. 7187, pp. 19–35. Springer, Heidelberg (2012). doi:10.1007/978-3-642-32747-6_2

124. Volkamer, M., Spycher, O., Dubuis, E.: Measures to establish trust in internet voting. In: Estevez, E., Janssen, M. (eds.) Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance (ICEGOV 2011). ACM (2011)
125. Vassil, K., Solvak, M., Vinkel, P.: E-valimiste levik Eesti valijate hulgas. Riigikogu Toimetised (Parliamentary Journal) 30(2), 116–128 (2014)
126. Webmedia, R. T. (2007, December 20). Isikut tõendavate dokumentide seadus (lühend - ITDS). Retrieved May 19, 2020, from https://www.riigiteataja.ee/akt/1042877
127. “What Is It? - Applying for an ID Card for an Adult.” Police and Border Guard Board, www.politsei.ee/en/instructions/applying-for-an-id-card-for-an-adult.
128. Interactive, E-turundusagentuur ADM. Home > ID.ee, www.id.ee/?lang=en.
129. Elections and E-Voting". https://web.archive.org/web/20150407234848/https:/www.valimised.ee/teema_eng.html Archived from the original on 2015-04-07. Retrieved 2020-05-25.
130. Krimmer, Robert; Duenas-Cid, David; Krivonosova, Iuliia; Vinkel, Priit; Koitmae, Arne (2018), Krimmer, Robert; Volkamer, Melanie; Cortier, Véronique; Goré, Rajeev (eds.), "How Much Does an e-Vote Cost? Cost Comparison per Vote in Multichannel Elections in Estonia", Electronic Voting, Springer International Publishing, 11143, pp. 117–131, doi:10.1007/978-3-030-00419-4_8, ISBN 9783030004187
131. Nore, H. (2010). Open Source Remote Electronic Voting in Norway. Vienna: The Ministry of Local and Regional Development.
132. ACE Electoral Knowledge Network
133. http://www.fastcompany.com/3032497/fast-feed/norway-ends-online-voting-for-local-and-national-elections
134. Nestas, L. H. (2010). Building Trust in Remote Internet Voting. Bergen: University ofBergen, Department of Informatics.
135. Ansper, A., Heiberg, S., Lipmaa, H., Overland, T. A., & van Laenen, F. (2011). Security and Trust for the Norwegian E-voting Pilot Project. Oslo: Ministry of LocalGovernment and Regional Development.
136. https://www.bbc.com/news/technology-28055678
137. Romanian General Inspectorate for Communications and Information Technology
138. European Commission finding on Romania 2003
139. https://web.archive.org/web/20140918040948/http://asambleaciudadana.podemos.info/
140. Provincial deputation elections since 1979, http://www.historiaelectoral.com/diputacions83.html
141. May 2006 pilot schemes from the UK Electoral Commission,
142. European Parliamentary and Local Elections (all-postal) Pilot Order 2004 από the UK Electoral Commission
143. 2003 election reports archive από the UK Electoral Commission
144. Penrose, John (2016). "UK Government response". webrootsdemocracy.org.

145. Electronic counting to take over from tellers at elections, The Scotsman, 19 April 2006
146. Green light for DRS & ERS to deliver e-Count for 2007 Scottish Elections, DRS Data Services Limited
147. Scottish Elections Review". UK Electoral Commission. October 23, 2017.
148. Rejected votes more than thought". BBC News. 9 May 2007.
149. Πρόκειται για μια μορφή ηλεκτρονικής ψηφοφορίας (DRE), η οποία καταγράφει, αποθηκεύει και συγκεντρώνει τις ψηφοφορίες ηλεκτρονικά χωρίς να παράγει χαρτί για την επαλήθευση των ψηφοφόρων.
150. Election Process Advisory Commission. (2007). Voting with Confidence. The Hague: Ministry of Interior and Kingdom Relations.
151. The Electoral Commission, 2007
152. Federal Constitutional Court. (2009, March 3). Use of voting computers in 2005 Bundestag election unconstitutional. http://www.bundesverfassungsgericht.de/en/press/bvg09-019en.html
153. E. G. Arnold, History of Voting Systems in California, Wayback Machine, California Secretary of State Bill Jones, June 1999.
154. Douglas W. Jones and Barbara Simons, Broken Ballots, CSLI Publications, 2012; see Section 5.2, page 96.
155. How E-voting Works, https://people.howstuffworks.com/e-voting.htm
156. Electronic Voting, http://lorrie.cranor.org/pubs/evoting-encyclopedia.html
157. Historical Timeline, https://votingmachines.procon.org/historical-timeline/
158. Voter Empowerment Act of 2013 (2013; 113th Congress H.R. 12) - GovTrack.us.
159. "Astronauts beam votes home". CNN. 2 November 2010, https://www.govinfo.gov/content/pkg/PLAW-111publ84/html/PLAW-111publ84.htm
160. James, Kate (2 November 2010). "Astronauts Cast Vote From Space Thanks to 1997 Texas Law". Gather.com.
161. Arizona Democratic Party Selects Votation.com to Hold World's First Legally-Binding Public Election Over the Internet". Business Wire. December 16, 1999.
162. Berman, Dennis (February 28, 2000). "We the E-People". BusinessWeek. Archived from the original on October 11, 2008.
163. Fairley Raney, Rebecca (January 22, 2000). "Suit Seeks to Block Net Vote in Arizona". The New York Times.
164. "Online voting debate rages in run-up to election". Reuters. CNN. November 1, 2000.
165. https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/bureau-of-global-public-affairs/foreign-press-centers/
166. Memorandum and Order by Judge Paul Rosenblatt, March 2, 2000, Voting Integrity Project, LuciousBain, et al, vs. Mark Fleisher and the Arizona Democratic Party, US District Court, District of Arizona, Page 17

167. Fairley Raney, Rebecca (March 1, 2000). "Judge Lets Internet Primary in Arizona Proceed". The New York Times
168. References 2000 Census, 2009, http://edrp.arid.arizona.edu/tribes.html
169. Internet Policy Institute. (2001). Report of the National Workshop on Internet Voting: Issues and Research Agenda. Internet Policy Institute.