# Ανοικτό Πανεπιστήμιο Κύπρου

**Σχολή Θετικών και Εφαρμοσμένων Επιστημών**

**Μεταπτυχιακό Πρόγραμμα Σπουδών**

***Ασφάλεια Υπολογιστών και Δικτύων***


## Μεταπτυχιακή Διατριβή

**Συστήματα Ηλεκτρονικής Ψηφοφορίας: Εκπόνηση Εκτίμησης Αντικτύπου ως προς τα Προσωπικά Δεδομένα σε ένα Ρεαλιστικό Σενάριο**


**Παναγιώτα Χ. Ιωάννου**

**Επιβλέπων Καθηγητής**
**Δρ. Κωνσταντίνος Λιμνιώτης**



**Μάιος 2023**

# Ανοικτό Πανεπιστήμιο Κύπρου

**Σχολή Θετικών και Εφαρμοσμένων Επιστημών**

**Μεταπτυχιακό Πρόγραμμα Σπουδών**

***Ασφάλεια Υπολογιστών και Δικτύων***


# Μεταπτυχιακή Διατριβή

## Συστήματα Ηλεκτρονικής Ψηφοφορίας: Εκπόνηση Εκτίμησης Αντικτύπου ως προς τα Προσωπικά Δεδομένα σε ένα Ρεαλιστικό Σενάριο


**Παναγιώτα Χ. Ιωάννου**

**Επιβλέπων Καθηγητής**
**Δρ. Κωνσταντίνος Λιμνιώτης**



Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών
Στην Ασφάλεια Υπολογιστών και Δικτύων
από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου.

**Μάιος 2023**

## Περίληψη

Μέσα στις νέες τάσεις της τεχνολογίας περιλαμβάνεται και η σύνδεση του ψηφιακού με τον φυσικό κόσμο. Η χρήση της ηλεκτρονικής ψηφοφορίας είναι και αυτή μέρος της τάσης αυτής, όπου η δυνατότητα του εκλέγειν και εκλέγεσθαι πραγματοποιείται πλέον ηλεκτρονικά, χωρίς της απαίτηση της φυσικής παρουσίας των ψηφοφόρων. Στην παρούσα μεταπτυχιακή διατριβή καταγράφονται οι τεχνολογίες και οι τεχνικές κρυπτογράφησης, οι οποίες χρησιμοποιούνται από τα συστήματα ηλεκτρονικής ψηφοφορίας.

Στόχος της διατριβής είναι κατ' αρχάς η μελέτη και η σύγκριση των συστημάτων ηλεκτρονικής ψηφοφορίας της αγοράς, ως προς τις τεχνικές τους δυνατότητες, αλλά και τις ιδιότητες τους σε συνάρτηση με την ασφάλεια που προσφέρουν. Περαιτέρω, το νομικό πλαίσιο και οι αρχές, οι οποίες διέπουν την επεξεργασία των προσωπικών δεδομένων, σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα αναλύονται σε συνάρτηση με την υλοποίηση της ηλεκτρονικής ψηφοφορίας, με επίκεντρο την εκτίμηση αντικτύπου στη βάση ενός ρεαλιστικού σεναρίου. Απώτατος σκοπός είναι να υλοποιηθεί μία εκτίμηση αντικτύπου ως προς τα προσωπικά δεδομένα για μία επεξεργασία που αφορά ηλεκτρονική ψηφοφορία, προκειμένου να διαφανεί η χρησιμότητα αλλά και η αναγκαιότητά της.

Η έκθεση εκτίμησης αντικτύπου αναδεικνύει τη σοβαρότητα των κινδύνων και των απειλών, τις οποίες αντιμετωπίζει το σύστημα ηλεκτρονικής ψηφοφορίας. Από την έκθεση καταδεικνύεται ότι επιβάλλεται η υλοποίηση των μέτρων που έχουν προταθεί για τη διαφύλαξη των δεδομένων προσωπικού χαρακτήρα που επεξεργάζεται ένα σύστημα ηλεκτρονικής ψηφοφορίας.

## Summary

The link between the digital and the physical world is considered to be part of the new trends in technology. Part of this trend is the usage of an electronic voting system where the possibility of being able to elect and being elected is now carried out electronically, without the voters being physically present. Thus, this thesis, deals with the technology and the encryption techniques used by electronic voting systems.

The aim of this Master Thesis is first to study and compare the electronic voting systems on the market, in terms of both technical capabilities and properties in relation to the security they offer. Furthermore, the legal framework and principles, which govern the processing of personal data according to the General Regulation for the Protection of Personal Data (GDPR), are analysed in relation to the implementation of electronic voting, focusing on the impact assessment based on a realistic scenario. The ultimate goal is to conduct a Data Protection Impact Assessment for a data process that rests with an e-voting system, in order to show its usefulness and necessity.

Furthermore, the impact assessment report highlights the severity of the risks, threats and challenges the e-voting system faces. The report illustrates that it is imperative to implement the measures that have been proposed for the safeguarding of personal data processed by an electronic voting system.

## Ευχαριστίες

Στο σημείο αυτό θα ήθελα να ευχαριστήσω τα παιδιά μου Εμμανουήλ και Χαράλαμπο για την υπομονή που επέδειξαν όσο διάστημα ετοίμαζα την παρούσα μεταπτυχιακή διατριβή. Ένα μεγάλο ευχαριστώ και στον επιβλέποντα καθηγητή μου Δρα. Κωνσταντίνο Λιμνιώτη για την πολύτιμη του στήριξη και καθοδήγηση ως προς την εκπόνηση της μεταπτυχιακής διατριβής.

Χωρίς τη στήριξη των πιο πάνω ατόμων, δεν θα ήταν δυνατή η ολοκλήρωση της παρούσας μεταπτυχιακής διατριβής.

# Περιεχόμενα

# Όροι κλειδιά - Συντομογραφίες

ΣΗΨ - Σύστημα ηλεκτρονικής ψηφοφορίας

ΓΚΠΔ - Γενικός Κανονισμός για την Προστασία Δεδομένων

ΕΑΠΔ - Εκτίμηση Αντικτύπου ως προς τα Προσωπικά Δεδομένα

C.I.A. - Confidentiality, Integrity, Availability

ΗΥ - Ηλεκτρονικός Υπολογιστής

DRE - Direct Recording Electronic Voting Machine

ΥΕ - Υπεύθυνος Επεξεργασίας Προσωπικών Δεδομένων

ΔΣ - Διοικητικό Συμβούλιο του Κλάδου των Υπαλλήλων του Οργανισμού

# Κεφάλαιο 1
# Εισαγωγή

Η τεχνολογική πρόοδος έχει επιφέρει μεγάλες αλλαγές σε ένα ευρύ φάσμα τομέων της ανθρώπινης ζωής. Ένας από τους τομείς αυτούς άπτεται των δικαιωμάτων των πολιτών, και δεν είναι άλλο από το δικαίωμα του εκλέγειν και εκλέγεσθαι. Ειδικότερα η ηλεκτρονική ψηφοφορία, δηλαδή η ψηφοφορία εξ αποστάσεως μέσω ηλεκτρονικών μέσων, αποκτά ιδιαίτερη αξία και, μάλιστα, συνθήκες όπως αυτές που η ανθρωπότητα βίωσε με την πανδημία του κορονοϊού ανέδειξαν ακόμα περισσότερο την σπουδαιότητά της. Η ηλεκτρονική ψηφοφορία έχει αναπτυχθεί σε επίπεδο όπου αριθμός κρατών, ψηφίζει πλέον μέχρι και τον Πρόεδρο τους, μέσω αυτών.

Ωστόσο, δεν είναι λίγοι εκείνοι οι οποίοι έχουν ισχυρές επιφυλάξεις ως προς το να υιοθετήσουν και να προσχωρήσουν σε ένα μοντέλο ηλεκτρονικής ψηφοφορίας: υπάρχουν έντονες ανησυχίες – και ως ένα βαθμό εύλογες – αναφορικά με την ασφάλεια και προστασία των δεδομένων, τη μυστικότητα της ψήφου, την εγκυρότητα αυτής κ.α. Οι προηγμένες κρυπτογραφικές τεχνικές που μπορούν να χρησιμοποιηθούν για την επίτευξη όλων των επιθυμητών στόχων ενός συστήματος ηλεκτρονικής ψηφοφορίας δεν είναι πάντα ευρέως διαδεδομένες ούτε πλήρως κατανοητές, ενώ επίσης υπάρχει πάντα ο φόβος για την απόκλιση μεταξύ θεωρίας και πράξης δηλαδή, ακόμα και αν θεωρητικά υπάρχουν τα εχέγγυα, εάν η υλοποίηση δεν είναι η δέουσα οι κίνδυνοι θα υπάρχουν.

## 1.1 Αναγκαιότητα και Σκοπός της Παρούσας Μεταπτυχιακής Διατριβής

Σκοπός της έρευνας είναι η μελέτη των διαφορετικών τεχνικών κρυπτογράφησης που χρησιμοποιούνται στα συστήματα ηλεκτρονικής ψηφοφορίας, συγκρίνοντας τις τεχνικές προδιαγραφές τους κυρίως ως προς την ασφάλεια και αξιοπιστία που προσφέρουν. Παράλληλα όμως, επειδή ένα σύστημα ηλεκτρονικής ψηφοφορίας

πραγματοποιεί επεξεργασία προσωπικών δεδομένων, και μάλιστα κρίσιμων, είναι ταυτόχρονα σε εφαρμογή το σχετικό νομικό πλαίσιο για την προστασία προσωπικών δεδομένων, το οποίο πρέπει να λαμβάνεται υπόψη. Αυτό συνεπάγεται ότι ένας οργανισμός που θα υιοθετήσει μία προσέγγιση ηλεκτρονικής ψηφοφορίας, θα πρέπει εξ αρχής να λάβει σημαντικές αποφάσεις ως προς το πώς θα υλοποιηθεί, οι οποίες αποφάσεις δεν άπτονται μόνο τεχνικών αλλά και νομικών ζητημάτων όπως, ποια δικαιώματα θα μπορούν οι χρήστες να ασκήσουν, αν και πώς θα ικανοποιούνται, πώς ο οργανισμός θα είναι σε θέση να αποδεικνύει ότι έπραξε σύμφωνα με τα νόμιμα, συμπεριλαμβανομένου του ότι επεξεργάστηκε τα λιγότερα δυνατά προσωπικά δεδομένα κ.α.

Στην Ευρώπη, το βασικό νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων είναι ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ). Ένα βασικό εργαλείο που παρέχει ο εν λόγω Κανονισμός, το οποίο είναι υποχρεωτικό για περιπτώσεις επεξεργασιών δεδομένων με υψηλούς κινδύνους, είναι η εκτίμηση αντικτύπου ως προς τα προσωπικά δεδομένα (ΕΑΠΔ). Η εκπόνηση μίας ΕΑΠΔ, εάν γίνει σωστά, θα εντοπίσει έγκαιρα τυχόν κινδύνους για τα δικαιώματα και τις ελευθερίες προσώπων και θα βοηθήσει στη λήψη κατάλληλων αποφάσεων για το πώς πρέπει να γίνει η επεξεργασία, πριν αυτή ξεκινήσει.

Ως εκ τούτου, η μελέτη του Γενικού Κανονισμού για την Προστασία Δεδομένων, και η εκπόνηση της εκτίμησης αντικτύπου ως προς τα προσωπικά δεδομένα στην ηλεκτρονική ψηφοφορία είναι αναγκαία αφού μπορεί να επηρεάσει τους ψηφοφόρους ώστε να μειωθούν τα ποσοστά αποχής και να ενισχυθεί η προσέλευση των ψηφοφόρων αφού θα εμπιστεύονται το σύστημα ηλεκτρονικής ψηφοφορίας, διασφαλίζοντας ταυτόχρονα τα δικαιώματά τους.

## 1.2 Βασικά Ερευνητικά Ερωτήματα

Πόσο ασφαλές και αξιόπιστο μπορεί να είναι ένα ηλεκτρονικό σύστημα ψηφοφορίας, με βάση την τεχνική κρυπτογράφησης που χρησιμοποιεί;

Οι τεχνικές κρυπτογράφησης καλύπτουν τις απαιτητικές ανάγκες ενός συστήματος ηλεκτρονικής ψηφοφορίας;

Η αυξημένη αποχή στις διαδικασίες ψηφοφορίας, η οποία καταγράφεται σε παγκόσμιο επίπεδο τα τελευταία χρόνια, αποτελεί αιτία προβληματισμού. Μπορεί η χρήση συστήματος ηλεκτρονικής ψηφοφορία να αντιστρέψει το κλίμα;

Ποιες δυσκολίες ανακύπτουν κατά την εκπόνηση μίας ΕΑΠΔ αναφορικά με σύστημα ηλεκτρονικής ψηφοφορίας; Θα μπορούσε η δημοσίευση μιας εκπόνησης εκτίμησης αντικτύπου ηλεκτρονικών συστημάτων ψηφοφορίας ως προς τα προσωπικά δεδομένα, να αυξήσει την εμπιστοσύνη άρα, τη συμμετοχή των ψηφοφόρων σε μια διαδικασία ψηφοφορίας;

## 1.3 Οργάνωση της Μεταπτυχιακής Διατριβής

Στο παρόν Κεφάλαιο αναφέρεται τόσο η αναγκαιότητα αλλά και τα βασικά ερευνητικά ερωτήματα. Στο Κεφάλαιο 2, αναλύεται το μέγεθος της χρήσης των συστημάτων ηλεκτρονικής ψηφοφορίας κατά το παρελθόν μέχρι και σήμερα. Αναφέρονται οι απαιτήσεις των συστημάτων για τη διασφάλιση της ιδιωτικότητας των προσωπικών δεδομένων στη βάση των τεχνολογιών και των τεχνικών κρυπτογραφίας, οι οποίες χρησιμοποιούνται στην ηλεκτρονική ψηφοφορία.

Στο 3ο Κεφάλαιο, καταγράφονται οι πτυχές του ΓΚΠΔ και ειδικότερα αναλύεται η εκτίμηση αντικτύπου ως προς τα προσωπικά δεδομένα. Στο επόμενο Κεφάλαιο, το 4ο, ετοιμάζεται βήμα-βήμα η εκτίμηση αντικτύπου ως προς τα προσωπικά δεδομένα στη βάση ενός ρεαλιστικού σεναρίου. Η εκπόνηση ετοιμάζεται με την βοήθεια λογισμικού, της Γαλλικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Τέλος, η μεταπτυχιακή διατριβή ολοκληρώνεται με τον επίλογο ως Κεφάλαιο υπ' αριθμό 5 όπου, συνοψίζοντας αναφέρονται τα συμπεράσματα που απορρέουν μέσα από την μελέτη και οι εισηγήσεις για μελλοντικές έρευνες.

# Κεφάλαιο 2
# Η Χρήση Της Κρυπτογραφίας Στην Ηλεκτρονική Ψηφοφορία

Πίσω από τον όρο ηλεκτρονική ψηφοφορία, βρίσκεται ένα μεγάλος όγκος από διαφορετικούς αλγόριθμους, λογισμικά και τεχνικές. Η χρήση των τεχνικών κρυπτογραφίας, εντοπίζεται σε όλα τα στάδια μιας διαδικασίας ψηφοφορίας, αφού όλα τα στάδια, έχουν αυξημένες απαιτήσεις ασφαλείας. Οι βασικές απαιτήσεις στο θέμα της ασφαλείας όπου τα συστήματα απαιτείται να διαθέτουν είναι η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας, γνωστά ως C.I.A. (Confidentiality, Integrity, Availability). Στην προκειμένη περίπτωση των συστημάτων ηλεκτρονικής ψηφοφορίας, είναι πολύ σημαντικό να διασφαλίζονται παράλληλα τόσο η ιδιωτικότητα όσο και η αυθεντικότητα. Όλα τα προαναφερθέντα χαρακτηριστικά τα προσφέρουν στα συστήματα ηλεκτρονικής ψηφοφορίας, οι διάφορες τεχνικές κρυπτογραφίας οι οποίες χρησιμοποιούνται με βάση τις ιδιότητες τους στα διάφορα στάδια της διαδικασίας της ψηφοφορίας.

## 2.1 Ηλεκτρονική Ψηφοφορία

Όπως έχει αναφερθεί και πιο πάνω, η ηλεκτρονική ψηφοφορία ενσωματώνει ένα σύνολο προηγμένων απαιτήσεων ασφαλείας και παράλληλα προστασία των συστημάτων από επιθέσεις. Η διασφάλιση της ασφάλειας σε όλα τα στάδια της διαδικασίας καθίσταται επιβεβλημένη. Τα ηλεκτρονικά συστήματα ψηφοφορίας απαιτούν ένα πολύπλοκο μοντέλο ασφάλειας λόγω του ότι απαιτείται να προσφέρουν παράλληλα μυστικότητα, ανωνυμία ψήφου, επαληθευσιμότητα και προστασία των ψηφοφόρων από τον καταναγκασμό.

Η χρήση της ηλεκτρονικής ψηφοφορίας, γίνεται όλο και πιο διαδεδομένη μέθοδος ψηφοφορίας με την πάροδο των ετών, αν και η παραδοσιακή ψηφοφορία φαίνεται πως συνεχίζει να κρατά τα ηνία. Η πανδημία του κορονοϊού επηρέασε και αυτή με την σειρά

της, στην αύξηση της χρήσης της ηλεκτρονικής ψηφοφορίας, παρόλα αυτά μελετώντας τον πιο κάτω πίνακα, παρατηρούμε πως ελάχιστα είναι τα κράτη που επιχείρησαν τη χρήση της ηλεκτρονικής ψηφοφορίας.

| **α/α** | **Υφιστάμενη χρήση ηλεκτρονικών συστημάτων ψηφοφορίας** | **Χώρες** |
|---|---|---|
| 1. | Πλήρες εφαρμογή ηλεκτρονικής ψηφοφορίας | Εσθονία, Ελβετία, Ινδία, Βραζιλία, Φιλιππίνες |
| 2. | Μερική εφαρμογή ηλεκτρονικής ψηφοφορίας | Αργεντινή, ΗΠΑ, Βέλγιο, Καναδάς, Ιαπωνία, Μεξικό, Γαλλία, Περού |
| 3. | Ακύρωση εφαρμογής | Αυστραλία, Κόστα Ρίκα, Φιλανδία, Γουατεμάλα, ΗΒ, Ιρλανδία, Ιταλία, Καζακστάν, Νορβηγία |
| 4. | Δεν συνέχισαν τη χρήση | Ολλανδία, Γερμανία, Παραγουάη |
| 5. | Βρίσκονται σε διαδικασία δοκιμής | Μπαγκλαντές,Μπουτάν, Ισημερινός, Μογγολία, Νεπάλ, Ινδονησία |

Πίνακας 1: Εφαρμογή ηλεκτρονικής ψηφοφορίας ανά κράτος *[1]*

Μελετώντας τα πιο πάνω στοιχεία καταλήγουμε στο συμπέρασμα ότι παρά την ταχεία ανάπτυξη της τεχνολογίας, λίγες είναι οι χώρες που έχουν εφαρμόσει και διατηρήσει την ηλεκτρονική ψηφοφορία, αφού οι κυβερνήσεις των χωρών, φαίνεται πως δεν είναι ακόμα έτοιμες για καθολική χρήση τέτοιου είδους συστημάτων και τερματισμό της παραδοσιακής διαδικασίας ψηφοφορίας.

Η παρούσα διατριβή επικεντρώνεται στη μελέτη χρήσης ηλεκτρονικών συστημάτων ασφαλείας σε μικρές ομάδες οργανωμένων συνόλων όπως τα σχολεία, τους συνδέσμους κοκ, όπου μέσα από μελέτη έχει διαπιστωθεί ότι η χρήση των συστημάτων ηλεκτρονικής ψηφοφορίας είναι ευρεία.

## 2.2 Απαιτήσεις ενός Συστήματος Ηλεκτρονικής Ψηφοφορίας

Τα συστήματα ηλεκτρονικής ψηφοφορίας εμφανίζονται σήμερα σε δύο βασικές μορφές, την ψηφοφορία με φυσική παρουσία και την εξ αποστάσεως ψηφοφορία. Η ηλεκτρονική

ψηφοφορία με φυσική παρουσία πραγματοποιείται σε εκλογικά κέντρα όπου πραγματοποιείται η διαδικασία της ψηφοφορίας, μέσω καθορισμένου εξοπλισμού ΗΥ, tablet ή μέσω μηχανών οι οποίες διαθέτουν το λογισμικό του συστήματος ψηφοφορίας (Direct Recording Electronic Voting Machine - DRE). Σε αυτή την περίπτωση οι ψήφοι αποθηκεύονται σε κεντρικό διακομιστή με τον οποίο είναι δικτυακά συνδεδεμένος ο εξοπλισμός όλων των εκλογικών κέντρων. Η εξ αποστάσεως ηλεκτρονική ψηφοφορία πραγματοποιείται χωρίς να απαιτείται η φυσική παρουσία των ψηφοφόρων σε συγκεκριμένο χώρο. Οι ψηφοφόροι, έχουν την δυνατότητα να ψηφίσουν από τον χώρο τους από όποια συσκευή διαθέτουν, όπως για παράδειγμα κινητό τηλέφωνο, φορητό υπολογιστή, tablet, ακόμη και μέσω μιας έξυπνης τηλεόρασης. Απαραίτητα και στις δύο περιπτώσεις είναι η χρήση υλισμικού, λογισμικού και σύνδεσης με το διαδίκτυο. Η παρούσα μεταπτυχιακή διατριβή επικεντρώνεται στην εξ αποστάσεως ηλεκτρονική ψηφοφορία και στις τεχνικές αλλά και τεχνολογίες που χρησιμοποιούνται στα στάδια της διαδικασίας μιας ψηφοφορίας.

Η διαδικασία ηλεκτρονικής ψηφοφορίας, αποτελείται από τα πιο κάτω βασικά στάδια:

- την εγγραφή των ψηφοφόρων με φυσική παρουσία ή ηλεκτρονικά
- την ταυτοποίηση των ψηφοφόρων,
- την υποβολή των ψήφων και
- την καταμέτρησή τους.

Στα συστήματα ηλεκτρονικής ψηφοφορίας την ασφάλεια προσφέρουν οι τεχνικές κρυπτογραφίας οι οποίες χρησιμοποιούνται, η κάθε μια με βάση τις ιδιότητες τους στο αντίστοιχο στάδιο της διαδικασίας. Επιπρόσθετα, τα συστήματα εκτός από την εμπιστευτικότητα, την ακεραιότητα, την διαθεσιμότητα, την ιδιωτικότητα και την αυθεντικότητα, χρειάζεται να πληρούν ένα κατάλογο νομικών, κοινωνικών και τεχνολογικών απαιτήσεων [2]. Όσες πιο πολλές από τις πιο κάτω απαιτήσεις καλύπτουν τόσο πιο ασφαλές και άτρωτο είναι το σύστημα:

- Μυστικότητα και ανωνυμία ψήφων, σε καμία περίπτωση δεν θα πρέπει να είναι δυνατή η σύνδεση ψηφοφόρων – ψήφων.
- Δημοκρατικότητα, ταυτοποίηση ψηφοφόρων, πρόσβαση στην διαδικασία ψηφοφορίας μόνο σε εγγεγραμμένους ψηφοφόρους, αποφυγή ψήφισης πέραν της μιας φοράς και αποφυγή συμπερίληψης μη έγκυρων ψήφων.

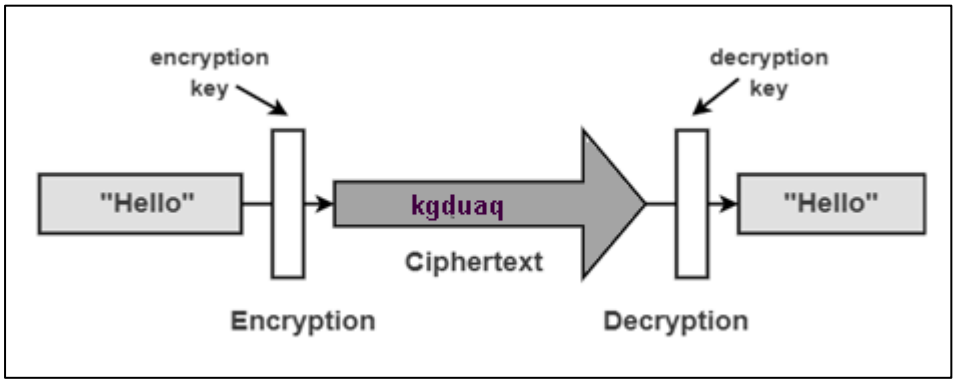
- Εγκυρότητα ψήφων, διασφάλιση δηλαδή της μη αλλοίωσης, της ακρίβειας και μοναδικότητας των ψήφων.
- Απόρρητο, διασφάλιση μυστικότητας των αποτελεσμάτων μέχρι την ολοκλήρωση της διαδικασίας ψήφισης.
- Ανθεκτικότητα, διασφάλιση της πλήρους προστασίας από κακόβουλες ενέργειες
- Επαληθευσιμότητα, να υπάρχει α) η επιλογή ελέγχου από τον ψηφοφόρο της μεταχείρισης και διαχείρισης που έτυχε η ψήφος, και β) να υπάρχει η δυνατότητα απόδειξης ότι το αποτέλεσμα των εκλογών είναι ακριβές [3].

Επιπρόσθετα ένα σύστημα ηλεκτρονικής ψηφοφορίας θα πρέπει να είναι αποδοτικό, να μπορεί δηλαδή να υποστηρίξει μεγάλο όγκο ψηφοφόρων ή/και υποψηφίων, χωρίς όμως να επηρεάζεται η απόδοση του συστήματος. Να είναι επίσης ευκολόχρηστο για να μπορεί να το χρησιμοποιήσουν όσο το δυνατόν περισσότεροι ψηφοφόροι, να προσφέρει επεκτασιμότητα αλλά και ευελιξία.

Με βάση όλα τα πιο πάνω χαρακτηριστικά τα οποία χρειάζεται να συνυπολογιστούν ως αναγκαία κατά την διαδικασία δημιουργίας ενός ηλεκτρονικού συστήματος ψηφοφορίας, καταλήγουμε στο συμπέρασμα πως μιλάμε για ένα μεγάλο και πολύπλοκο σύστημα. Ο ανθρώπινος παράγοντας όμως, είναι και αυτός απαραίτητος για την ομαλή διεξαγωγή μιας διαδικασίας ηλεκτρονικής ψηφοφορίας. Οι ρόλοι που απαιτούνται να έχουν οι υπεύθυνοι διεξαγωγής των εκλογών είναι πολλοί κατά την διάρκεια της διαδικασίας και φαίνεται να είναι σχεδόν αδύνατο να είναι αξιόπιστοι όλοι οι ρόλοι εκατό τοις εκατό [4]. Η παρουσία του ανθρώπινου παράγοντα σε διάφορους ρόλους όπου αναλαμβάνει την ετοιμασία και διεξαγωγή μιας διαδικασίας ψηφοφορίας, είναι αδύνατο να απαλειφθεί από την εξίσωση και αυτό ίσως είναι ένα τρωτό σημείο στο θέμα ασφάλειας της διαδικασίας. Όπως χαρακτηριστικά έχει αναφέρει ο Ρώσσος πολιτικός Joseph Stalin "It is enough that the people know there was an election. The people who cast the votes decide nothing. The people who count the votes decide everything" [5].

## 2.3 Κρυπτογραφία

Η κρυπτογραφία αποτελεί γνωστικό πεδίο της επιστήμης της κρυπτολογίας το οποίο μελετάει, αναπτύσσει και χρησιμοποιεί διάφορες τεχνικές κρυπτογράφησης και αποκρυπτογράφησης. Στόχος της κρυπτογράφησης είναι να κρύψει το περιεχόμενο ενός μηνύματος, ενώ στην αποκρυπτογράφηση, γίνεται η αντίστροφη διαδικασία, όπου το μήνυμα επανέρχεται στην αρχική του μορφή ως Εικόνα 1.




Εικόνα 1: Απεικόνιση κρυπτογράφησης και αποκρυπτογράφησης

Το μήνυμα Hello της Εικόνας 1, με την χρήση του κλειδιού κρυπτογραφείται. Θεωρώντας δεδομένο, ότι ο υποκλοπέας έχει πρόσβαση στο κρυπτοκείμενο kgduaq και γνωρίζει τους αλγόριθμους κρυπτογράφησης και αποκρυπτογράφησης, αυτό που χρειάζεται να διασφαλιστεί είναι η ασφάλεια του μυστικού κλειδιού. Δύο είναι τα είδη κρυπτογραφίας η συμμετρική και η ασύμμετρη, στην περίπτωση της ηλεκτρονικής ψηφοφορίας εφαρμόζονται και τα δύο αυτά είδη.

### 2.3.1 Συμμετρική Κρυπτογράφηση

Η συμμετρική κρυπτογράφηση χωρίζεται σε δύο κατηγορίες στους κρυπταλγόριθμους ροής και τμήματος. Οι κρυπταλγόριθμοι ροής (stream ciphers) είναι αρκετά απλοί και χρησιμοποιούνται σε εφαρμογές όπου απαιτείται ταχύτητα ή/και χαμηλή κατανάλωση ισχύος (όπως το Bluetooth, τα δίκτυα RFID). Η χρήση γεννήτριας ψευδοτυχαίας ακολουθίας bits, όπου η ακολουθία αυτή ενώνεται με τα bits του μηνύματος, με αποτέλεσμα να έχουμε το κρυπτοκείμενο. Η τυχαία αυτή ακολουθία χρειάζεται να ικανοποιεί ένα αριθμό κριτηρίων ούτως ώστε να μην είναι εύκολα προβλέψιμη.

Οι κρυπταλγόριθμοι τμήματος (block ciphers) λειτουργούν με διάφορους τρόπους: ένας από αυτούς είναι με την ξεχωριστή κρυπτογράφηση ανά τμήμα του κειμένου με την

εφαρμογή κλειδιού. Το συμμετρικό κλειδί είναι πολύ σημαντικό να παραμένει πάντα μυστικό και τυχαίο, αφού η ασφάλεια του αλγόριθμου έγκειται στη μυστικότητα του κλειδιού αυτού. Το πρότυπο συμμετρικής κρυπτογράφησης είναι ο αλγόριθμος AES (Advanced Encryption Standard).

### 2.3.2 Ασύμμετρη Κρυπτογράφηση

Η ασύμμετρη κρυπτογράφηση, αλλιώς γνωστή και ως κρυπτογράφηση δημοσίου κλειδιού χρησιμοποιείται σε μεγάλα δίκτυα, όπου η συμμετρική κρυπτογραφία δεν μπορεί να υλοποιηθεί με την ίδια απόδοση. Οι Diffie και Hellman το 1976 [6], είχαν προτείνει την ασύμμετρη κρυπτογράφηση η οποία προσφέρει ασφαλή ανταλλαγή του συμμετρικού κλειδιού κρυπτογράφησης. Ουσιαστικά η χρήση του Diffie-Hellman αλγόριθμου επικεντρώνεται αποκλειστικά στην ανταλλαγή του μυστικού κλειδιού, υπάρχουν αρκετοί άλλοι αλγόριθμοι δημοσίου κλειδιού οι οποίοι χρησιμοποιούνται για την πραγματοποίηση της κρυπτογράφησης.

Λόγω του ότι οι αλγόριθμοι δημοσίου κλειδιού βασίζονται πάνω σε δύσκολα μαθηματικά προβλήματα, εφαρμόζονται ευρέως στα συστήματα ηλεκτρονικής ψηφοφορίας, οι αλγόριθμοι που συναντάμε συχνά στα συστήματα ηλεκτρονικής ψηφοφορίας είναι οι αλγόριθμοι ελλειπτικών καμπυλών και ο RSA [7]. Το σχήμα ψηφιακής υπογραφής RSA, ήταν η πρώτη μέθοδος που είχε ανακαλυφθεί.

### 2.3.3 Ψηφιακή Υπογραφή και Συναρτήσεις Κατακερματισμού

Η ψηφιακή υπογραφή έχει ως σκοπό τη σύνδεση της ταυτότητας ενός ατόμου με μια πληροφορία, η σημαντικότερη ιδιότητα της είναι πως είναι υπολογιστικά απρόσιτη για οποιοδήποτε να την υπολογίσει πλην του υπογράφοντα [3]. Άλλα σχήματα ψηφιακής υπογραφής εκτός από το RSA είναι και ο αλγόριθμος El Gamal.

Οι συναρτήσεις κατακερματισμού (hash functions) έχουν και αυτές, εξίσου σημαντικό ρόλο αφού προσφέρουν ευκολία στον υπολογισμό τους και συμπίεση (ενώ μπορούν να δεχθούν είσοδο οποιουδήποτε μήκους, η έξοδος που παράγουν έχει σταθερό μήκος), γι΄ αυτό και εφαρμόζονται και στις ψηφιακές υπογραφές [3]. Ουσιαστικά χρησιμοποιούνται για επαλήθευση, μέσω των συναρτήσεων, παράγεται ένα αποτύπωμα των δεδομένων το οποίο αποστέλλεται μαζί με τα δεδομένα και μέσω αυτού ο παραλήπτης έχει την δυνατότητα -παράγοντας και εκείνος το αποτύπωμα- να

επιβεβαιώσει την ταυτότητα του αποστολέα. Οι συναρτήσεις λόγω των πιο πάνω ιδιοτήτων τους, προσφέρουν ακεραιότητα των δεδομένων και αυθεντικότητα.

## 2.4 Εφαρμογή Τεχνικών Κρυπτογραφίας στην Ηλεκτρονική Ψηφοφορία

Η επιλογή των κατάλληλων τεχνικών κρυπτογραφίας για εφαρμογή τους σε ένα σύστημα ηλεκτρονικής ψηφοφορίας δεν είναι καθόλου εύκολο επιχείρημα αφού θα πρέπει να ικανοποιεί τόσο τις αρχές του νομικού πλαισίου όσο και τους βασικούς κανόνες ασφαλείας. Πλέον όλοι οι προτεινόμενοι αλγόριθμοι, απαιτείται να αποδεικνύουν και μαθηματικά την ασφάλειά τους, ενώ οι μόνοι στόχοι δεν είναι η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικοποίηση των χρηστών.

Δεδομένου του ότι δεν υπάρχει απόλυτα ασφαλές σύστημα, δημιουργήθηκε η ανάγκη συνδυασμού διαφορετικών τεχνικών, ο συνδυασμός των οποίων παρέχει τα απαραίτητα χαρακτηριστικά για να προσφέρει ασφάλεια σε όλα τα στάδια της διαδικασίας μιας ηλεκτρονικής ψηφοφορίας. Πιο κάτω στον Πίνακα 2, παρατίθενται οι τεχνικές όπου συναντάμε πολύ συχνά στα συστήματα ηλεκτρονικής ψηφοφορίας σε συνάρτηση με τις ιδιότητες που προσφέρουν σε αυτά.

| **Ιδιότητα** | **Είδος κρυπτογραφίας** |
|---|---|
| Εμπιστευτικότητα των ψήφων | Αλγόριθμοι συμμετρικής κρυπτογραφία |
| Ασφαλής αποστολή των ψήφων | Κλειδί συμμετρικής κρυπτογραφίας, το οποίο θα κρυπτογραφηθεί με αλγόριθμο δημόσιου κλειδιού |
| Πιστοποίηση της ταυτότητας των ψηφοφόρων | Αλγόριθμοι δημόσιου κλειδιού - ψηφιακές υπογραφές, ψηφιακά πιστοποιητικά |
| Διασφάλιση της μοναδικότητας της ψήφου | Αλγόριθμοι δημόσιου κλειδιού |
| Γνησιότητα των ψήφων | Αλγόριθμοι δημόσιου κλειδιού - ψηφιακές υπογραφές, ψηφιακά πιστοποιητικά |

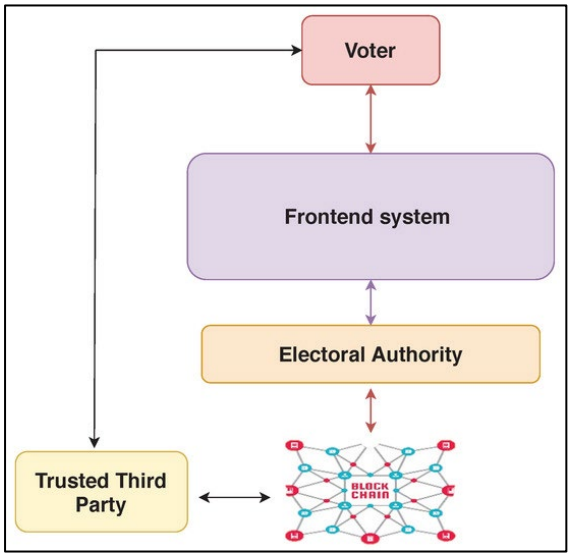
Πίνακας 2: Ιδιότητες συστημάτων ανά είδος κρυπτογραφίας

### 2.4.1 Τεχνολογίες Blockchain

Η Blockchain τεχνολογία αποτελεί μια έγκυρη δομή αποθήκευσης πληροφοριών, η οποία πρωτοεμφανίστηκε το 2008 από τον Nakamoto. Μπορεί να παρομοιαστεί με μια μεγάλη, δημόσια ψηφιακή βάση δεδομένων στην οποία καταγράφονται όλες οι συναλλαγές των χρηστών της [8].

Η τεχνολογία Blockchain, βασίζεται ιδίως σε τεχνικές κρυπτογράφησης δημόσιου κλειδιού και συναρτήσεις κατακερματισμού. Στα συστήματα ηλεκτρονικής ψηφοφορίας η τεχνολογία Blockchain, προσφέρει ασφάλεια και επαληθευσιμότητα στις πληροφορίες που αποθηκεύονται και ικανοποιεί την ανάγκη για αναλλοίωτη και επαληθεύσιμη καταγραφή των ψήφων [9].

Ως διαφαίνεται και στην Εικόνα 2, το σημαντικότερο πλεονέκτημα της τεχνολογίας Blockchain συνίσταται στη μη ύπαρξη κεντρικής διαχείρισης, χαρακτηριστικό το οποίο καθιστά πιο έμπιστο και ασφαλές το σύστημα αφού αποφεύγονται με αυτό τον τρόπο εξωτερικές επιθέσεις. Επίσης η διαθεσιμότητα που προσφέρει δεν έχει τοπικούς αλλά ούτε και χρονικούς περιορισμούς. Παράλληλα προσφέρει αποκεντροποίηση και ανεξαρτητοποίηση από τους κεντρικούς παρόχους υπηρεσιών, με τη χρήση ψηφιακών υπογραφών – για ταυτοποίηση, ομομορφικής κρυπτογραφίας – για επίτευξη της μυστικότητας των ψήφων σε συνδυασμό με μη διαδραστικές αποδείξεις μηδενικής γνώσης.

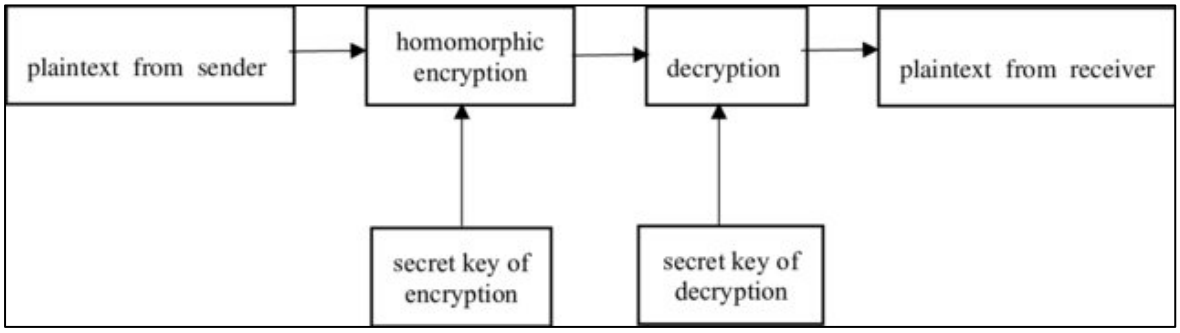



Εικόνα 2: Εφαρμογή τεχνολογίας blockchain στην ηλεκτρονική ψηφοφορία *[10]*

Επίσης, η χρήση των αλγόριθμων RSA και ελλειπτικών καμπυλών μέσω των τεχνολογιών Blockchain, επιτρέπουν στους ψηφοφόρους να συμμετέχουν και να υποβάλλουν με ασφάλεια τις ψήφους τους, όπως και να επιβεβαιώνουν τη συμμετοχή τους αλλά και να μπορούν να αλλάζουν την ψήφο τους -όπου εφαρμόζεται- εντός πάντα του προκαθορισμένου χρονικού πλαισίου. Κάποια από τα συστήματα ηλεκτρονικής ψηφοφορίας τα οποία συναντάμε στην αγορά και βασίζονται στην τεχνολογία Blockchain είναι τα Helios [11], Voatz [8], Verify-Your-Vote (VYV) [9], Follow My Vote [12] [13], Open Vote Network [14], [15], [16].

### 2.4.2 Ομομορφική Κρυπτογραφία

Η ομομορφική κρυπτογραφία αποτελεί έναν εκ των πιο γνωστών τεχνικών κρυπτογραφίας, η οποία χρησιμοποιείται στα ηλεκτρονικά συστήματα ψηφοφορίας, αφού διασφαλίζει τη μυστικότητα των ψήφων. Τα πρώτα ομομορφικά συστήματα είχαν προταθεί την δεκαετία του 1980 από τον Josh Benaloh [3]. Οι ψήφοι κρυπτογραφούνται, ενώ το κλειδί αποκρυπτογράφησης δεν το κατέχει ο καταμετρητής ψήφων οπότε, με αυτό τον τρόπο διασφαλίζεται η μυστικότητά τους. Η ιδιότητα της ομομορφικής κρυπτογραφίας η οποία την καθιστά εφαρμόσιμη στα συστήματα ηλεκτρονικής ψηφοφορίας είναι το γεγονός ότι μπορεί να αθροίζει τις κρυπτογραφημένες ψήφους και η αποκρυπτογράφηση του αθροίσματος, να αντιστοιχεί στο πραγματικό άθροισμα των ψήφων! Ουσιαστικά, εγγυάται οικουμενική επαληθευσιμότητα, χωρίς την ανάγκη παραβίασης της μυστικότητας των ψήφων.

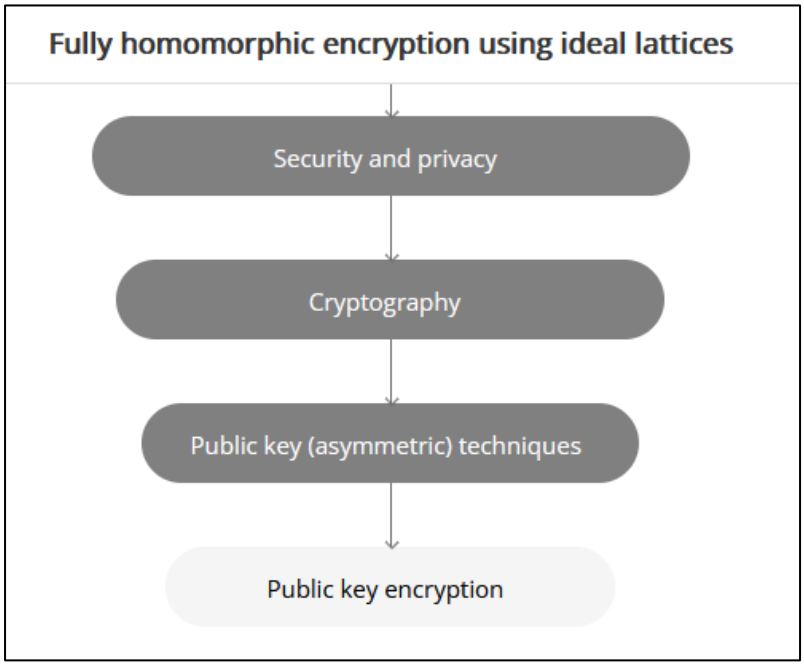


Εικόνα 3: Διαδικασίας ομομορφικής κρυπτογραφίας *[17]*

Ως Εικόνα 3 πιο πάνω, η ομομορφική κρυπτογραφία δεν απαιτεί την ύπαρξη κεντρικής διαχείρισης και σε συνδυασμό με ένα σύστημα απόδειξης μηδενικής γνώσης, το οποίο θα διασφαλίζει την εγκυρότητα της ψήφου, η ομομορφική κρυπτογραφία μπορεί να οριστεί ως απαραίτητο στοιχείο για ένα σύστημα ηλεκτρονικής ψηφοφορίας. Επίσης, οι ψηφοφόροι μπορούν να αποδείξουν την αυθεντικότητα τους στους διακομιστές, χωρίς την ανάγκη χρήσης ειδικού ασφαλούς καναλιού το οποίο θα πρέπει να επιβεβαιώνει την ιδιωτικότητα των ψηφοφόρων.

Τα συστήματα ηλεκτρονικής ψηφοφορίας τα οποία έχουν ως βάσει την ομομορφική κρυπτογραφία προσφέρουν αρκετή ασφάλεια αλλά παράλληλα έχουν υψηλότερη πολυπλοκότητα στο κομμάτι της επικοινωνίας. Στις περιπτώσεις όπου αριθμούνται αρκετοί υποψήφιοι, συνεπάγεται υψηλό υπολογιστικό κόστος για τους διακομιστές, γι΄ αυτό και θεωρούνται ιδανικά για ψηφοφορίες με δύο επιλογές - πχ Ναι και Όχι.

Πλέον όμως έχουν προταθεί συστήματα ομομορφικής κρυπτογραφίας με γραμμική ή λογαριθμική υπολογιστική πολυπλοκότητα, τα οποία και βασίζονται στο κρυπτοσύστημα Paillier [18]. Το κρυπτοσύστημα Paillier, το οποίο χρησιμοποιεί αλγόριθμο δημοσίου κλειδιού, έχει την εξής ομομορφική ιδιότητα η οποία προσφέρει εμπιστευτικότητα των δεδομένων [19], έχοντας το γινόμενο δύο κρυπτογραφημένων κειμένων, με το ιδιωτικό κλειδί μπορούμε να έχουμε το πραγματικό άθροισμα των δύο αυτών κειμένων. Αξίζει να σημειωθεί πως στην πλήρως ομομορφική κρυπτογραφία πραγματοποιούνται όλες οι μαθηματικές πράξεις και όχι μόνο μια. Η πλήρως ομομορφική κρυπτογραφία, προς το παρόν μελετάται, αλλά πρακτικά δεν έχει υλοποιηθεί, αν και έχουν περάσει ήδη δεκατέσσερα έτη από τότε όπου πρωτοπαρουσιάστηκε από τον Gentry, το πρώτο πλήρως ομομορφικό σχήμα [20] ως Εικόνα 4. Με την υλοποίηση της πλήρως ομομορφικής κρυπτογραφίας, θα μπορεί να γίνεται οποιαδήποτε μαθηματική πράξη.



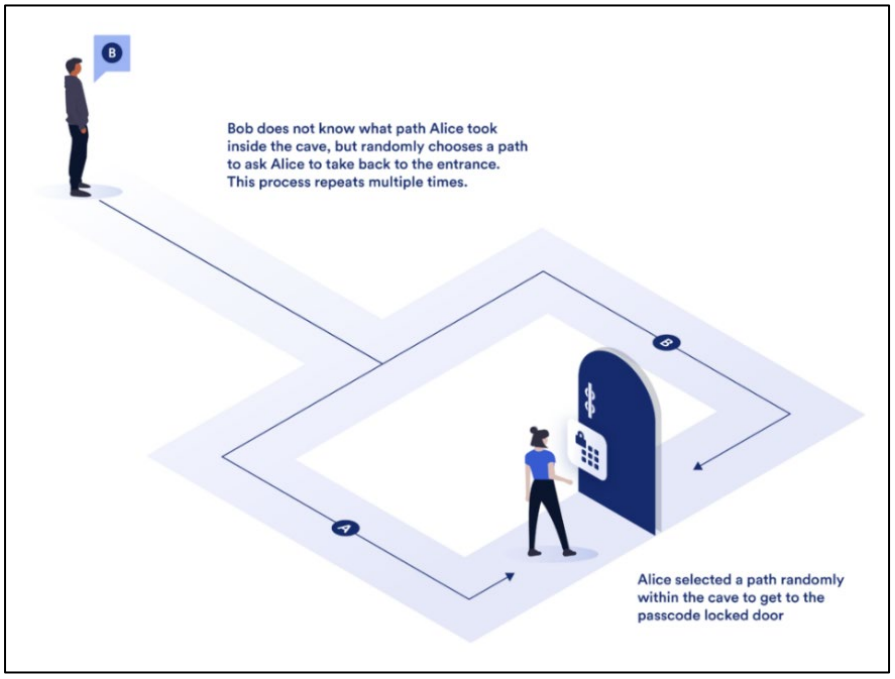
Εικόνα 4: Απεικόνιση πλήρης ομομορφικής κρυπτογραφίας *[20]*

Κάποια από τα συστήματα τα οποία χρησιμοποιούν ομομορφική κρυπτογραφία είναι τα Helios [3], VoteHere [21] και VoteBox [4].

### 2.4.3 Κρυπτογράφηση Μηδενικής Γνώσης

Περιγράφοντας την τεχνολογία Blockchain αλλά και την ομομορφική κρυπτογραφία πιο πάνω, αναφερθήκαμε, στον συνδυασμό τους με την απόδειξη μηδενικής γνώσης. Η απόδειξη μηδενικής γνώσης έχει οριστεί ως μια τεχνική κρυπτογράφησης η οποία προτάθηκε από τους ερευνητές του MIT S. Micali, S. Goldwasser και C. Rackoff γύρω στο 1980 και εξακολουθεί να είναι επίκαιρη έως και σήμερα [22].

Η απόδειξη μηδενικής γνώσης επιτρέπει σε μια οντότητα να πείσει μια δεύτερη οντότητα για την εγκυρότητα της πληροφορίας που της αποστέλλει, χωρίς όμως να απαιτείται να αποκαλύψει το περιεχόμενο της πληροφορίας, με άλλα λόγια, με μηδενική γνώση του μηνύματος. Ουσιαστικά αναζητούμε επιχειρήματα για την εγκυρότητα μιας πρότασης ή την αλήθεια ενός ισχυρισμού, τα οποία όμως δεν πρέπει να μεταφέρουν κανένα είδος γνώσης στον επαληθευτή ως Εικόνα 5.



Εικόνα 5: Απεικόνιση τρόπου λειτουργίας μιας απόδειξης μηδενικής γνώσης, χωρίς την αποκάλυψη των δεδομένων σε άλλο μέρος *[23]*

### 2.4.4 Δίκτυα Μίξης

Η ιδέα των Δικτύων Μίξης (Mix Nets) πρωτοδημοσιεύτηκε από τον David Chaum το 1981 [21]. Τα Mix Nets αποτελούνται από ένα σύνολο διακομιστών συνδεδεμένων μεταξύ τους, οι οποίοι προσφέρουν ανωνυμία, τόσο κατά την υποβολή των ψήφων όσο και κατά την διάρκεια αποκρυπτογράφησης. Ουσιαστικά αυτό επιτυγχάνεται με την επανα-κρυπτογράφηση (re-encryption) των κρυπτογραφημένων ψήφων όπου και αναμιγνύει τη σειρά τους.

Τα Mix Nets είναι φτιαγμένα με τέτοιο τρόπο ώστε μπορούν να προσφέρουν εκτός από ανωνυμία, επαληθευσιμότητα αλλά και ανθεκτικότητα σε κακόβουλες επιθέσεις που πιθανόν να επιχειρήσουν να εισβάλουν στο σύστημα. Χαρακτηρίζονται επίσης, ως αρκετά αποδοτικά. Συστήματα ηλεκτρονικής ψηφοφορίας τα οποία χρησιμοποιούν Mix Nets είναι τα Prêt a Voter και Civitas [4].

### 2.4.5 Τυφλή Υπογραφή

Στη παράγραφο 2.3.3 του παρόντος Κεφαλαίου πιο πάνω, αναφέρθηκε η χρησιμότητα των ψηφιακών υπογραφών. Η τυφλή υπογραφή συγκαταλέγεται ως μια ειδική περίπτωση ψηφιακής υπογραφής (digital signature) και στηρίζεται στην ασύμμετρη κρυπτογραφία. Σε ένα ηλεκτρονικό σύστημα ψηφοφορίας, η χρήση της τυφλής υπογραφής διασφαλίζει την ακεραιότητα των ψήφων, την ανωνυμία αλλά και την

ιδιωτικότητα. Ουσιαστικά αυτός που υπογράφει την ψήφο με το ιδιωτικό του κλειδί, δεν θα πρέπει να ξέρει τι υπογράφει, γι' αυτό και χρησιμοποιείται η «τυφλή» υπογραφή. Εφόσον ο υπογράφων είναι έμπιστη οντότητα διασφαλίζεται η εγκυρότητα της ψήφου, ότι δηλαδή δεν έχει αλλοιωθεί. Παράλληλα, με την χρήση της τυφλής υπογραφής διασφαλίζεται η αρχή της ανάγκης γνώσης. Κάποια από τα συστήματα τα οποία χρησιμοποιούν τυφλή υπογραφή είναι τα Sensus [4], REVS (Rebust electronic voting system) [4], M-SEAS [4].

Οι τεχνικές οι οποίες υπάρχουν και χρησιμοποιούνται από τα συστήματα ηλεκτρονικής ψηφοφορίας, είναι αρκετές και έχουν να προσφέρουν ποικίλα οφέλη, η κάθε μια σε διαφορετικό στάδιο της διαδικασίας. Παραθέτοντας μέρος αυτών των τεχνικών πιο πάνω, καταλήγουμε στο συμπέρασμα πως ένα σύστημα ηλεκτρονικής ψηφοφορίας είναι πολυσύνθετο, με αρκετές απαιτήσεις και πως η επιλογή ενός καλού συνδυασμού τεχνολογιών και τεχνικών, δεν είναι απλό εγχείρημα.

## 2.5 Συστήματα Ηλεκτρονικής Ψηφοφορίας Ανοιχτού Κώδικα

Μελετώντας τα ανωτέρω, όπου παρατίθενται κάποιες από τις πιο γνωστές τεχνικές κρυπτογράφησης οι οποίες χρησιμοποιούνται στα συστήματα ηλεκτρονικής ψηφοφορίας, επιβεβαιώνουμε πως, η δημιουργία ενός ασφαλούς συστήματος ηλεκτρονικής ψηφοφορίας, είναι ένα αρκετά δύσκολο εγχείρημα, αφού η επιλογή των κατάλληλων τεχνικών θα πρέπει να καλύπτει ένα μεγάλο φάσμα από ανάγκες. Θα πρέπει να διαθέτει ένα σύνολο προηγμένων απαιτήσεων ασφαλείας σε όλα τα στάδια της διαδικασίας μιας ηλεκτρονικής ψηφοφορίας και επίσης προσφέρει, προστασία από επιθέσεις αλλά να διασφαλίζει και τα δικαιώματα των ψηφοφόρων.

Εν έτη 2023 πλέον στην αγορά κυκλοφορούν αρκετά συστήματα ηλεκτρονικής ψηφοφορίας. Τα συστήματα ηλεκτρονικής ψηφοφορίας συνήθως είναι μέρος μιας σουίτας υπηρεσιών που προσφέρουν οι εταιρείες, όπου τα περισσότερα είτε προσφέρουν δωρεάν δοκιμαστική έκδοση, είτε δωρεάν χρήση για μικρό αριθμό ψηφοφόρων. Στον Πίνακα 3 παρουσιάζονται ενδεικτικά κάποια από αυτά τα συστήματα, που έχουν εντοπιστεί στο διαδίκτυο.

| **ΕΜΠΟΡΙΚΗ ΕΠΩΝΥΜΙΑ ΣΥΣΤΗΜΑΤΟΣ** | **ΔΩΡΕΑΝ ΥΠΗΡΕΣΙΕΣ** |
|---|---|
| **Eligo (www.eligo.social/en)** | Trial για 14 μέρες |
| **AssociationVoting (www.associationvoting.com)** | Trial για 2 βδομάδες για 15 ψηφοφόρους |
| **ElectionBuddy (https://electionbuddy.com)** | Trial & Δωρεάν μέχρι 20 ψηφοφόρους |
| **OpaVote (www.opavote.com)** | Δωρεάν μέχρι 25 ψηφοφόρους |
| **NemoVote (https://nemovote.com)** | Trial |
| **Rankedvote (www.rankedvote.co)** | Δωρεάν μέχρι 100 ψηφοφόρους |

Πίνακας 3: Δωρεάν υπηρεσίες συστημάτων ηλεκτρονικής ψηφοφορίας ανοιχτού κώδικα

Μέσα από την πιο πάνω έρευνα στο διαδίκτυο καταλήγουμε στο συμπέρασμα πως τα πλείστα συστήματα της αγοράς έχουν το αντίτιμό τους. Θα μπορούσε να γίνει μια έρευνα ως προς το αν τα οργανωμένα σύνολα τα οποία χρησιμοποιούν συστήματα ηλεκτρονικής ψηφοφορίας, εμπιστεύονται περισσότερο αυτές τις εταιρείες, ενώ έχουν τη δυνατότητα χρήσης άλλων συστημάτων ηλεκτρονικής ψηφοφορίας, τα οποία προσφέρουν την ίδια ασφάλεια και είναι και δωρεάν.

Στο διαδίκτυο προσφέρονται αρκετά ασφαλή συστήματα ηλεκτρονικής ψηφοφορίας ανοιχτού κώδικα, συστήματα τα οποία προσφέρουν διαφάνεια ως προς τον τρόπο λειτουργίας τους. Τα συστήματα αυτά έχουν διαθέσιμο για έλεγχο τον πηγαίο κώδικά. Στον Πίνακα 4 διαφαίνονται οι ιδιότητες ασφαλείας οι οποίες καλύπτουν σύστημα ηλεκτρονικής ψηφοφορίας της αγοράς, ανοιχτού κώδικα τα οποία χρησιμοποιούν τεχνολογίες Blockchain.

| **Ιδιότητες** [3] | **Helios** | **Verify-Your-Vote (VYV)** | **TIVI** | **FollowMy Vote** | **OpenVoteNetwork (OV-net)** | **Agora** |
|---|---|---|---|---|---|---|
| Εγκυρότητα | ✓<br>Εξαρτάται όμως από τον εκλογικό διαχειριστή | ✓ | ✓ | ✓ | ✓<br>Εξαρτάται όμως από τον εκλογικό διαχειριστή | ✓ |

| **Ιδιότητες** [3] | **Helios** | **Verify-Your-Vote (VYV)** | **TIVI** | **FollowMy Vote** | **OpenVoteNetwork (OV-net)** | **Agora** |
|---|---|---|---|---|---|---|
| Δικαιοσύνη | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ |
| Ακεραιότητα | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ |
| Ατομική επαληθευσιμότητα | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Καθολική επαληθευσιμότητα | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ |
| Ιδιωτικότητα της ψήφου | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ |
| Αποφυγή εκτύπωσης της ψήφου σε χαρτί | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ |
| Αντίσταση στον καταναγκασμό | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Πολιτική ψηφοφορίας | Δυνατότητα αλλαγής τη ψήφου | Δυνατότητα αλλαγής τη ψήφου | Δεν υπάρχει δυνατότητα αλλαγής της αρχικής ψήφου | Δυνατότητα αλλαγής τη ψήφου | Δεν υπάρχει δυνατότητα αλλαγής της αρχικής ψήφου | N/A |

Πίνακας 4: Χαρακτηριστικά συστημάτων ηλεκτρονικής ψηφοφορίας ανοιχτού κώδικα *[11, 14, 9, 12]*

Μελετώντας τον Πίνακα 4, διαφαίνεται ότι υπάρχουν διαθέσιμα αρκετά συστήματα ανοιχτού κώδικα, τα οποία καλύπτουν ένα μεγάλο εύρος των απαραίτητων ιδιοτήτων ενός συστήματος. Τα συστήματα αυτά φαίνεται να χρησιμοποιούνται κυρίως από οργανωμένα σύνολα όπως σχολεία και συνδέσμους.

Το στοιχείο το οποίο δεν έχει εντοπιστεί, είναι το ποσοστό των ψηφοφόρων οι οποίοι συμμετάσχουν στις διαδικασίες ηλεκτρονικής ψηφοφορίας μέσω αυτών των συστημάτων και άρα ο βαθμός διείσδυσής τους στους πολίτες. Είναι κατανοητός ο λόγος για τον οποίο οι εμπορικές εταιρείες δεν δημοσιεύουν τέτοιου είδους πληροφορίες, για την παρούσα όμως μεταπτυχιακή διατριβή θα ήταν πολύ χρήσιμες για περαιτέρω μελέτη και σύγκριση επί των στοιχείων ανά σύστημα.

# Κεφάλαιο 3
# Νομικό Πλαίσιο

Με την ψηφιακή εξέλιξη, η οποία έχει επιφέρει ευρεία χρήση λογισμικών συστημάτων στην πλειοψηφία των οργανισμών ανά την υφήλιο, διαφάνηκε πως η ανάγκη για προστασία των φυσικών προσώπων ως προς την επεξεργασία των προσωπικών τους δεδομένων και της ιδιωτικότητας τους σε συνδυασμό με την ελεύθερη κυκλοφορία αυτών, ήταν οι βασικοί λόγοι όπου το Ευρωπαϊκό Κοινοβούλιο προχώρησε στην ετοιμασία και εφαρμογή του Γενικού Κανονισμού για την Προστασία Δεδομένων (Genera Data Protection Regulation) - ΓΚΠΔ. Ο Κανονισμός αυτός, που είναι ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου ημερομηνίας 27 Απριλίου 2016, τέθηκε σε εφαρμογή στις 25 Μαΐου 2018 σε αντικατάσταση της Οδηγίας 95/46/ΕΚ [24].

## 3.1 Γενικός Κανονισμός για την Προστασία Δεδομένων

Με την εφαρμογή του ΓΚΠΔ, ουσιαστικά καθορίζονται οι προϋποθέσεις νομιμότητας της επεξεργασίας των προσωπικών δεδομένων, τα δικαιώματα αλλά και οι υποχρεώσεις στη βάση της ιδιωτικότητας. Ο Κανονισμός αυτός ενισχύει την προστασία των προσωπικών δεδομένων και παράλληλα ενισχύει τα δικαιώματα των πολιτών.

Ο ΓΚΠΔ αποτελείται από 99 Άρθρα τα οποία κατανέμονται σε 11 Κεφάλαια και σε όλο το κείμενο χρησιμοποιούνται συγκεκριμένοι ορισμοί οι οποίοι και αναλύονται στο Άρθρο 4 του Κανονισμού. Οι βασικοί ορισμοί οι οποίοι θα χρησιμοποιηθούν και στην παρούσα διατριβή, είναι οι ακόλουθοι:

- **Δεδομένα προσωπικού χαρακτήρα** – κάθε πληροφορία που αφορά φυσικό πρόσωπο

- **Επεξεργασία δεδομένων** – κάθε πράξη ή σειρά πράξεων όπως η συλλογή, καταχώριση, οργάνωση, αποθήκευση, τροποποίηση, ανάκτηση, αναζήτηση, χρήση, διαβίβαση, διάδοση, διαγραφή των προσωπικών δεδομένων
- **Υποκείμενο δεδομένων** – φυσικό πρόσωπο το οποίο αφορούν τα δεδομένα
- **Υπεύθυνος επεξεργασίας** – φυσικό ή νομικό πρόσωπο ή δημόσια αρχή που καθορίζει το σκοπό και τον τρόπο επεξεργασίας των δεδομένων
- **Εκτελών την επεξεργασία** - φυσικό ή νομικό πρόσωπο ή δημόσια αρχή που επεξεργάζεται τα προσωπικά δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας.

Οι αρχές που διέπουν κάθε επεξεργασία προσωπικών δεδομένων καταγράφονται στο Άρθρο 5 του ΓΚΠΔ:

α. Αρχή της νομιμότητας, της αντικειμενικότητας και της διαφάνειας
β. Αρχή του περιορισμού του σκοπού
γ. Αρχή της ελαχιστοποίησης
δ. Αρχή της ακρίβειας - επικαιροποίηση
ε. Αρχή του περιορισμού της περιόδου αποθήκευσης
στ. Αρχή της ακεραιότητας και της εμπιστευτικότητας
ζ. Αρχή της λογοδοσίας [24].

Μελετώντας τις αρχές που διέπουν την επεξεργασία των προσωπικών δεδομένων, διακρίνουμε ότι υπάρχει μία κατά κάποιο τρόπο αντιστοίχιση με τις προδιαγραφές που έχουν ήδη αναφερθεί στο Κεφάλαιο 2 της παρούσας μεταπτυχιακής διατριβής, ως απαιτούμενες ιδιότητες των συστημάτων ηλεκτρονικής ψηφοφορίας. Παρατίθεται πιο κάτω στον Πίνακα 5, η εφαρμογή των αρχών που διέπουν την επεξεργασία προσωπικών δεδομένων σε ένα σύστημα ηλεκτρονικής ψηφοφορίας.

| **α/α** | **Βασικές Αρχές** [24] | **Υλοποίηση στην ηλεκτρονική ψηφοφορία** |
|---|---|---|
| Α | Αρχή νομιμότητας, Αντικειμενικότητας και Διαφάνειας | Η επεξεργασία δεδομένων προσωπικού χαρακτήρα των ψηφοφόρων, θα πρέπει να είναι θεμιτή και να πραγματοποιείται με διαφάνεια. |
| Β | Αρχή περιορισμού του σκοπού | Τα στοιχεία των ψηφοφόρων συμπεριλαμβανομένων των ψήφων αυτών, συλλέγονται και επεξεργάζονται αποκλειστικά |

| α/α | **Βασικές Αρχές** [24] | **Υλοποίηση στην ηλεκτρονική ψηφοφορία** |
|---|---|---|
| | | και μόνο για τον σκοπό πραγματοποίησης της ψηφοφορίας |
| Γ | Αρχή ελαχιστοποίησης | Η συλλογή και επεξεργασία των προσωπικών δεδομένων των ψηφοφόρων, θα πρέπει να περιορίζεται μόνο στα απαραίτητα στοιχεία που χρειάζονται για την εκπλήρωση του σκοπού της ηλεκτρονικής ψηφοφορίας. |
| Δ | Αρχή ακρίβειας – επικαιροποίηση | Ο κατάλογος με τα στοιχεία των ψηφοφόρων, θα πρέπει να είναι ακριβής και να επικαιροποιείται συχνά. Επίσης τα δεδομένα της ηλεκτρονικής ψηφοφορίας θα πρέπει να είναι ακριβή. |
| Ε | Αρχή περιορισμού της περιόδου αποθήκευσης | Τα δεδομένα των ηλεκτρονικών ψηφοφοριών τα οποία συλλέγονται για τους σκοπούς της εν λόγω επεξεργασίας, θα πρέπει να αποθηκεύονται μόνο για το χρονικό διάστημα που απαιτείται. |
| Στ | Αρχή ακεραιότητας και εμπιστευτικότητας | Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα των ψηφοφόρων, θα πρέπει να εγγυάται την ασφάλεια και προστασία τους από μη εξουσιοδοτημένα άτομα. |
| Ζ | Αρχή λογοδοσίας | Ο υπεύθυνος επεξεργασίας θα πρέπει να έχει τα μέσα να αποδείξει την εφαρμογή όλων των πιο πάνω βασικών αρχών. |

Πίνακας 5: Βασικές Αρχές ΓΚΠΔ & ηλεκτρονική ψηφοφορία

Περαιτέρω, κάθε επεξεργασία προσωπικών δεδομένων πρέπει να έχει μία «νομική βάση» για να είναι επιτρεπτή, όπως αυτές παρατίθενται στο άρθρο 6 του ΓΚΠΔ. Μία συνηθισμένη νομική βάση είναι η συγκατάθεση του χρήστη, η οποία μπορεί να είναι η σωστή όταν οι χρήστες έχουν όντως ελευθερία στο να συναινέσουν για την επεξεργασία των δεδομένων τους, και δηλώνουν τη συγκατάθεση τους με σαφήνεια και με ειδική προς τούτο ενέργεια, έχοντας πλήρως ενημερωθεί για το τι συνεπάγεται πρακτικά η συγκατάθεση που δίνουν.

## 3.2 Εκτίμηση Αντικτύπου ως προς τα Προσωπικά Δεδομένα

Πιο πάνω αναφέρθηκαν οι επτά αρχές του ΓΚΠΔ, οι οποίες διέπουν την επεξεργασία προσωπικών δεδομένων. Η εκτίμηση αντικτύπου ως προς τα προσωπικά δεδομένα, σύμφωνα με τον Άρθρο 35 του ΓΚΠΔ, είναι ένα από τα βασικά εργαλεία που μπορεί να χρησιμοποιήσει ο υπεύθυνος επεξεργασίας ή/και οι εκτελούντες για να στηρίξουν την αρχή της λογοδοσίας.

Η εκτίμηση αντικτύπου ουσιαστικά:

- περιγράφει τη φύση, το πεδίο εφαρμογής και τον σκοπό της επεξεργασίας,
- αξιολογεί την αναγκαιότητα, αναλογικότητα και τα μέτρα συμμόρφωσης,
- εντοπίζει και αξιολογεί τους κινδύνους για τα εμπλεκόμενα πρόσωπα και
- προσδιορίζει τυχόν πρόσθετα μέτρα με σκοπό τον μετριασμό των κινδύνων που θα εντοπίσει.

Με άλλα λόγια, στόχος της εκπόνησης της εκτίμησης αντικτύπου ως προς τα Προσωπικά Δεδομένα (ΕΑΠΔ) ενός συστήματος, είναι η εξεύρεση των κινδύνων της επεξεργασίας των προσωπικών δεδομένων, με σκοπό την καταγραφή των κενών ασφαλείας και προστασίας δεδομένων του συστήματος και την καταγραφή προτεινόμενων μέτρων.

Η κλίμακα η οποία συνήθως χρησιμοποιείται για την εκτίμηση της σοβαρότητας του κινδύνου είναι τα επίπεδα αμελητέος, περιορισμένος, σημαντικός, μέγιστος [25]. Η εκπόνηση ΕΑΠΔ, σύμφωνα με το άρθρο 35 του Κανονισμού, είναι υποχρεωτική για το υπεύθυνο επεξεργασίας όταν το επίπεδο του κινδύνου είναι υψηλό. Στην προκειμένη στην ηλεκτρονική ψηφοφορία, η εκπόνηση ΕΑΠΔ κρίνουμε ότι είναι απαραίτητη αφού η επεξεργασία προσωπικών δεδομένων των ψηφοφόρων είναι αναπόφευκτη (υπό την έννοια ότι δεν υπάρχει τρόπος να συμμετέχει κάποιος στις εκλογές χωρίς να ψηφίσει) και σαφώς ενδέχεται να έχει υψηλό κίνδυνο. Η ΕΑΠΔ ιδανικά θα πρέπει να χρησιμοποιείται ως εργαλείο που βοηθά στη λήψη αποφάσεων σε σχέση με την επεξεργασία, γι΄ αυτό το λόγο θα πρέπει να ετοιμάζεται πριν από την επεξεργασία των δεδομένων, ούτως ώστε να συνάδει με τις αρχές προστασίας τους.

# Κεφάλαιο 4
# Εκπόνηση Εκτίμησης Αντικτύπου Ως Προς Τα Προσωπικά Δεδομένα: Μελέτη Περίπτωσης

Ένα ηλεκτρονικό σύστημα ψηφοφορίας, σε σύγκριση με την παραδοσιακή ψηφοφορία, επιτρέπει τη βελτίωση της δημοκρατικής διαδικασίας και τη μείωση του κόστους υλοποίησης της διαδικασίας εκλογών, αυξάνοντας την συμμετοχή των ψηφοφόρων και οδηγώντας σε πιο άμεσο αποτέλεσμα. Επίσης, προσφέρει την δυνατότητα στους ψηφοφόρους να επιβεβαιώσουν ότι η ψήφος τους έχει καταχωρηθεί και καταμετρηθεί.

Τα συστήματα ηλεκτρονικής ψηφοφορίας, είναι αρκετά πολύπλοκα συστήματα αφού θα πρέπει παράλληλα να πληρούν έναν μεγάλο κατάλογο νομικών, κοινωνικών και τεχνολογικών απαιτήσεων [2].

Στο Κεφάλαιο αυτό αναπτύσσεται, ως μελέτη περίπτωσης, μία εκτίμηση αντικτύπου ως προς τα προσωπικά δεδομένα ενός πραγματικού σεναρίου που αφορά ένα Κλάδο Υπαλλήλων ενός οργανισμού ο οποίος δραστηριοποιείται πανευρωπαϊκά. Απώτερος σκοπός είναι να διερευνηθεί ο βαθμός στον οποίο μία εκτίμηση αντικτύπου μπορεί να οδηγήσει/κατευθύνει, έναν υπεύθυνο επεξεργασίας, στη σωστή λήψη αποφάσεων ως προς τις διάφορες παραμέτρους ενός συστήματος ηλεκτρονικής ψηφοφορίας – ενώ το ρεαλιστικό σενάριο το οποίο παρουσιάζεται ως μελέτη περίπτωσης θα μπορούσε, ως προς τη μεθοδολογική σκοπιά, να αποτελεί βάση αναφοράς για κάθε αντίστοιχη επεξεργασία.

## 4.1 Στοιχεία Σεναρίου Χρήσης Ηλεκτρονικού Συστήματος Ψηφοφορίας

Η παρούσα ΕΑΠΔ βασίζεται σε ρεαλιστικό σενάριο χρήσης του ηλεκτρονικού συστήματος ψηφοφορίας ανοιχτού κώδικα Helios. Η ανάλυση των τεχνικών χαρακτηριστικών του εν λόγω συστήματος στα θέματα που αφορούν την επεξεργασία προσωπικών δεδομένων των ψηφοφόρων, βοηθάει στην εκπόνηση μιας ολοκληρωμένης έκθεσης αντικτύπου ως προς τα προσωπικά δεδομένα.

Με βάση το σενάριό μας, οι πλείστοι λειτουργοί του οργανισμού, οι οποίοι είναι μέλη του Κλάδου και κατά συνέπεια και ψηφοφόροι, ζουν και εργάζονται στο εξωτερικό, έτσι η χρήση του συστήματος ηλεκτρονικής ψηφοφορίας διαφαίνεται να είναι η ιδανική λύση σε σύγκριση με την παραδοσιακή ψηφοφορία. Στο παρελθόν, πριν την χρήση του συστήματος Helios, οι εκλογές γίνονταν με τον παραδοσιακό τρόπο, συγκεκριμένα αποστέλλονταν τα ψηφοδέλτια στο εξωτερικό, μέσω ιδιωτικής ταχυδρομικής εταιρείας ταχείας μεταφοράς και με τον ίδιο τρόπο παραλάμβανε η Επιτροπή Εκλογών τα ψηφοδέλτια για καταμέτρηση και προσθήκη τους στον εκλογικό αποτέλεσμα. Ο τρόπος αυτός εκτός από δαπανηρός, δεν διασφάλιζε σχεδόν καμία από τις αρχές του ΓΚΠΔ.

Το Νοέμβριο του 2021, ο οργανισμός επιχείρησε για πρώτη φορά, την αντικατάσταση της παραδοσιακής διαδικασίας με την χρήση του ηλεκτρονικού συστήματος Helios. Οι ψηφοφόροι εμπιστεύτηκαν με ευκολία το εν λόγω σύστημα και η συμμετοχή στην ψηφοφορία ξεπέρασε το 70%. Στη συνέχεια το σύστημα Helios, χρησιμοποιήθηκε άλλες δύο φορές εντός ενός τετραμήνου, με αρκετά μεγάλη συμμετοχή. Στον Πίνακα 6 παρατίθενται τα ποσοστά συμμετοχής, όπου ο μέσος όρος δείγματος συμμετοχής ήταν οι 166 ψηφοφόροι.

| **α/α** | **Ποσοστό συμμετοχής ανά ψηφοφορία** |
|---|---|
| 1 | 74,0% |
| 2 | 80,8% |
| 3 | 67,6% |

Πίνακας 6: Ποσοστά συμμετοχής ανά ψηφοφορία

Η πρώτη ηλεκτρονική ψηφοφορία διεξήχθη τον Νοέμβριο του 2021, όπου είχαν τεθεί προς τους ψηφοφόρους πέντε επιλογές και συμμετείχαν 122 ψηφοφόροι από τους 165 που ήταν το σύνολο. Το ποσοστό του 74%, μπορεί να θεωρηθεί ένα πολύ ενθαρρυντικό, αν λάβουμε υπόψη ότι το σύνολο των ψηφοφόρων, πρώτη φορά ερχόταν σε επαφή με τέτοιου είδους σύστημα. Το λάθος της Επιτροπής εκλογών ήταν ο μεγάλος αριθμός επιλογών (πέντε), που είχε δοθεί στους ψηφοφόρους, το οποίο είχε ως αποτέλεσμα οι ψήφοι να διαμοιραστούν και έτσι καμία επιλογή δεν είχε ξεπεράσει το 50%. Με βάση το καταστατικό του Κλάδου, στις περιπτώσεις όπως η απεργία, για να μπορεί να γίνει δεχθεί η απόφαση απαιτείται να ψηφίσει θετικά τουλάχιστον το 50% του συνόλου.

Ένα μήνα μετά, πραγματοποιήθηκε μια άλλη διαδικασία ηλεκτρονικής ψηφοφορίας, όπου η συμμετοχή είχε φτάσει τους 135 ψηφοφόρους εκ των 167. Η αύξηση αυτή οφείλεται τόσο στην ευκολία της διαδικασίας ψήφισης, η οποία ήταν πλέον γνώριμη στους πλείστους ψηφοφόρους, όσο και στο γεγονός ότι το αποτέλεσμα της ψηφοφορίας ήταν καίριο. Σε αυτή την διαδικασία είχαν δοθεί τρείς επιλογές προς ψήφιση, όπου μια εξ αυτών έλαβε πέραν του 50% (83 ψήφους). Να σημειωθεί ότι, η αύξηση των ψηφοφόρων από 165 σε 167, οφείλεται στο γεγονός ότι οι εν λόγω υπάλληλοι ενεγράφησαν στο Κλάδο γιατί επιθυμούσαν να συμμετέχουν στις διαδικασίες ψηφοφορίας.

Στην συνέχεια ακολούθησε μια τρίτη διαδικασία σε πολύ μικρό χρονικό διάστημα, όπου η συμμετοχή ανήλθε στους 113 εκ των 167. Οι παράγοντες που συνέτειναν στην μείωση αυτή, διαφαίνεται πως δεν είχαν να κάνουν με την λειτουργία ή αξιοπιστία του συστήματος ηλεκτρονικής ψηφοφορίας που χρησιμοποιήθηκε. Την ετοιμασία της διαδικασίας, τον ορισμό των επιλογών, καθώς και την καταχώρηση των στοιχείων των ψηφοφόρων (ονοματεπώνυμο, ηλεκτρονική διεύθυνση και ένα username) και την αποστολή ηλεκτρονικών μηνυμάτων και την κυκλοφορία των αποτελεσμάτων των ψηφοφοριών είχε αναλάβει η Επιτροπή Εκλογών, η οποία αποτελείτο από εκλεγμένα μέλη του συνόλου των ψηφοφόρων, μέσω του συστήματος Helios. Στο σύστημα καταχωρήθηκαν οι εταιρικές ηλεκτρονικές διευθύνσεις των ψηφοφόρων, στις οποίες στάλθηκε ο σύνδεσμος της ψηφοφορίας, το επιβεβαιωτικό μήνυμα καταχώρησης της ψήφου, αλλά και το αποτελέσματα της ψηφοφορίας. Η μελέτη του ρεαλιστικού αυτού σεναρίου και η περιγραφή των διαδικασιών είναι σημαντικά στοιχεία ούτως ώστε να μελετήσουμε τόσο την εφαρμογή του συστήματος Helios, όσο και τις αντιδράσεις των

ψηφοφόρων. Επιτρέπει παράλληλα την ανάλυση των θετικών και αρνητικών σημείων, ως προς την επεξεργασία προσωπικών δεδομένων των ψηφοφόρων.

## 4.2 Εκπόνηση Έκθεσης Αντικτύπου ως προς τα Προσωπικά Δεδομένα

Τα λογισμικά τα οποία έχουν αναπτυχθεί για την υποβοήθηση την εκπόνηση μίας ΕΑΠΔ είναι χρήσιμα εργαλεία στη διενέργεια εκτίμησης αντικτύπου, αφού «κατευθύνουν» κατάλληλα τους υπεύθυνους επεξεργασίας ενώ παράλληλα παρέχουν την απαραίτητη νομική και γνωστική βάση για τη δημιουργία μιας ολοκληρωμένης έκθεσης εκτίμησης αντικτύπου. Στην παρούσα μεταπτυχιακή διατριβή έγινε χρήση του λογισμικού Privacy Impact Assessment, [26] PIA έκδοση 3.0.3, της Γαλλικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Το λογισμικό αυτό έχει βοηθήσει στην ορθή εκτέλεση της εκτίμησης αντικτύπου και επελέγη γιατί πέραν του ότι είναι ελεύθερα διαθέσιμο και ανοιχτού κώδικα εργαλείο, έχει αναπτυχθεί από μια αρμόδια εποπτική Αρχή Προστασίας Δεδομένων, το οποίο αποτελεί εχέγγυο για το ότι έχει λάβει υπόψη όλες τις παραμέτρους αναφορικά με τους κινδύνους για τα προσωπικά δεδομένα. Στο Παράρτημα Α έχουν περιληφθεί φωτογραφίες ενοτήτων της έκθεσης.

Η διαδικασία εκπόνησης της έκθεσης αντικτύπου περιλαμβάνει:

1. Τον καθορισμό και την ανάλυση του βαθμού επεξεργασίας ανά προσωπικό δεδομένο, των στοιχείων των ψηφοφόρων και των ψήφων αφού είναι απαραίτητη η επεξεργασία τους σε ένα σύστημα ηλεκτρονικής ψηφοφορίας.
2. Την αξιολόγηση των πιθανών κινδύνων και της επαρκούς ή μη αντιμετώπισής τους.
3. Τον καθορισμό των μέτρων που θα ληφθούν προκειμένου να διασφαλιστεί η συμμόρφωση με τις απαιτήσεις του σχετικού Κανονισμού.
4. Τέλος, τον έλεγχο και την λήψη αποφάσεων για την εφαρμογή ή όχι της διαδικασίας ψηφοφορίας - και, σε καταφατική περίπτωση, με τι χαρακτηριστικά. Συγκεκριμένα η έκθεση χωρίζεται στις πιο κάτω ενότητες:

1. Γενικό Πλαίσιο
2. Θεμελιώδεις Αρχές
3. Κίνδυνοι
4. Επικύρωση [26].

Παραθέτονται ανα ενότητα οι ερωτοαπαντήσεις της ΕΑΠΔ.

### 4.2.1 Γενικό Πλαίσιο

Η ενότητα Γενικό Πλαίσιο περιγράφει τη φύση, το πεδίο εφαρμογής και τον σκοπό της επεξεργασίας. Πιο κάτω παρουσιάζεται το αντικείμενο της μελέτης, η υπό εξέταση επεξεργασία, οι ευθύνες που συνδέονται με αυτήν και η λεπτομερής παρουσίαση του αντικειμένου επεξεργασίας.

- Ποια είναι η υπό εξέταση επεξεργασία;

Το Διοικητικό Συμβούλιο του Κλάδου Υπαλλήλων του Οργανισμού Χ, αποφάσισε να αντικαταστήσει τον παραδοσιακό τρόπο ψήφισης. Τα μέλη του Κλάδου εργάζονται τόσο στην Κύπρο όσο και σε χώρες του εξωτερικού, έτσι η χρήση ενός συστήματος ηλεκτρονικής ψηφοφορίας είναι το ιδανικό εργαλείο, στην περίπτωση αυτή. Με αυτό τον τρόπο μπορούν να ασκήσουν το εκλογικό τους δικαίωμα όλα τα μέλη χωρίς μεγάλη απώλεια χρόνου, χωρίς κόστος και κυρίως με μυστικότητα.

Πλέον οι ψηφοφορίες μεταξύ των μελών του Κλάδου πραγματοποιούνται με τη χρήση του συστήματος ηλεκτρονικής ψηφοφορίας Helios. Η επεξεργασία προσωπικών δεδομένων εκτελείται από το επταμελές ΔΣ το οποίο έχει αναλάβει την εκτέλεση της διεξαγωγής της ψηφοφορίας μέσω του συστήματος. Ο Υπεύθυνος επεξεργασίας (ΥΕ) είναι το επταμελές ΔΣ του Κλάδου των Υπαλλήλων του Οργανισμού Χ.

- Ποιες είναι οι ευθύνες που συνδέονται με την επεξεργασία;

Μέσα στις ευθύνες του ΥΕ (ΔΣ Κλάδου), περιλαμβάνονται, η εξασφάλιση ανανεωμένου καταλόγου με τα ονοματεπώνυμα των μελών του Κλάδου μαζί με τις εταιρικές τους ηλεκτρονικές διευθύνσεις. Παράλληλα ετοιμάζει τα ερωτήματα της ψηφοφορίας, τις απαντήσεις/επιλογές οι οποίες θα έχουν οι ψηφοφόροι καθώς και την ημερομηνία και ώρα έναρξης και λήξης της διαδικασίας της ψηφοφορίας.

- Ποια προσωπικά δεδομένα υφίστανται επεξεργασία;

Τα προσωπικά δεδομένα τα οποία υφίστανται επεξεργασία είναι τα στοιχεία των μελών του Κλάδου του Οργανισμού τα οποία θα καταχωρηθούν στο ηλεκτρονικό σύστημα ψηφοφορίας δηλαδή το ονοματεπώνυμό τους, ένα username και η εταιρική τους ηλεκτρονική διεύθυνση. Επίσης, το σύστημα επεξεργάζεται τις ψήφους, με την διαδικασία συλλογής των ψήφων, ανάμειξή τους και ετοιμασία αποτελέσματος. Κατά τη

διαδικασία της ψηφοφορίας, κάνοντας log in στο σύστημα, όλοι όσοι έλαβαν κωδικούς πρόσβασης, μπορούν να δουν ποιοι ψήφισαν και ποιοι όχι.

- Πώς λειτουργεί ο κύκλος ζωής των δεδομένων και των διαδικασιών;

Το ΔΣ ζητά επικαιροποιημένο κατάλογο των μελών του Κλάδου του, από τα κεντρικά γραφεία της Συντεχνίας όπου ανήκει. (Τα μέλη πληρώνουν μηνιαία συνδρομή στην Συντεχνία γι' αυτό και η τελευταία διατηρεί επικαιροποιημένο κατάλογο των μελών). Ο κατάλογος των μελών, περιλαμβάνει ονοματεπώνυμα, αριθμό δελτίου ταυτότητας και αριθμό κοινωνικών ασφαλίσεων (ΑΚΑ) των μελών. Ο ΥΕ ετοιμάζει σε ένα csv file, τα ονοματεπώνυμα των μελών, ένα username και την ηλεκτρονική τους διεύθυνση. Τα προσωπικά δεδομένα όπως αριθμός ταυτότητας και ΑΚΑ, δεν απαιτούνται, έτσι δεν θα πρέπει να γίνεται χρήση τους. Ιδανικά ούτε το ΔΣ θα έπρεπε να έχει αυτά τα ευαίσθητα προσωπικά στοιχεία.

Ο ΥΕ καταχωρεί όλα τα απαραίτητα στοιχεία στο σύστημα, όπως τις ερωτήσεις, τις επιλογές που έχουν οι ψηφοφόροι προς ψήφιση, καθώς και τα χρονικά πλαίσια της διαδικασίας και ανεβάζει το csv file στο σύστημα.

Με την ολοκλήρωση της καταχώρησης των απαραίτητων στοιχείων και αφού φτάσει η ώρα έναρξης της ψηφοφορίας, ο ΥΕ δίνει την εντολή στο σύστημα να αποστείλει ηλεκτρονικά μηνύματα στους ψηφοφόρους, προσκαλώντας τους να ψηφίσουν. Στο μήνυμα αυτό περιλαμβάνεται κείμενο στο οποίο αναφέρεται, η ημερομηνία και ώρα λήξης της ψηφοφορίας, το ονοματεπώνυμο, το username, το password του ψηφοφόρου (γίνεται αυτόματα generated από το σύστημα) και ο σύνδεσμος μέσω του οποίου μπορεί να ψηφίσει. Είναι επίσης εφικτό κατά τη διάρκεια της ψηφοφορίας -μέσω του συστήματος- να σταλεί υπενθύμιση στους ψηφοφόρους, είτε σε όλους είτε μόνο σε αυτούς που δεν έχουν ψηφίσει μέχρι εκείνη τη στιγμή. Με τη λήξη της ψηφοφορίας ο ΥΕ ενεργοποιεί το ανακάτεμα των ψήφων και λαμβάνει τα αποτέλεσμα της ψηφοφορίας. Τα αποτελέσματα είναι διαθέσιμα σε όλους εφόσον ο ΥΕ ενεργοποιήσει μέσω του συστήματος, την αποστολή των αποτελεσμάτων στους ψηφοφόρους. Σημειώνεται ότι, τα αποτελέσματα καθώς και τα ονόματα των ψηφοφόρων που έχουν ψηφίσει είναι προσβάσιμα από όλα τα μέλη, χωρίς χρονικό περιορισμό.

- Ποια είναι τα στοιχεία που υποστηρίζουν τα δεδομένα;

Το σύστημα ηλεκτρονικής ψηφοφορίας είναι το Helios, ένα web based, δωρεάν σύστημα ανοικτού κώδικα. Ο ΥΕ, έχει την δυνατότητα να κάνει log in μέσω gmail ή github, χωρίς την ανάγκη εγκατάστασης οποιουδήποτε εξειδικευμένου λογισμικού ή υλικού. Το σύστημα Helios προσφέρει ως αναφέρονται και στον Πίνακα 4, εγκυρότητα, ακεραιότητα, επαληθευσιμότητα αλλά και ιδιωτικότητα. Όλα αυτά τα χαρακτηριστικά τα προσφέρουν οι τεχνικές κρυπτογράφησης οι οποίες χρησιμοποιούνται στον εν λόγω σύστημα. Η αρχιτεκτονική του είναι βασισμένη στο κλασσικό σύστημα ψηφοφορίας το οποίο είχε προταθεί από τον Cramer et al με κάποιες τροποποιήσεις του Josh Benaloh, ενός από τους τρείς δημιουργούς του κώδικα του συστήματος [27]. Το σύστημα χρησιμοποιεί ομομορφική κρυπτογραφία η οποία προσφέρει μυστικότητα στις ψήφους. Με τη χρήση του αλγόριθμου κρυπτογράφησης El Gamal [28] ασύμμετρης κρυπτογραφίας η οποία βασίζεται στην απόφαση του Diffie-Hellman [19], διασφαλίζεται η ακεραιότητα της κάθε ψήφου. Επιπρόσθετα το Helios όταν γίνεται η αποκρυπτογράφηση του αποτελέσματος, χρησιμοποιεί κρυπτογράφηση μηδενικής γνώσης, για να μπορέσει να αποδείξει ο ΥΕ πως το αποτέλεσμα είναι ορθό, χωρίς να χρειαστεί να αποκαλύψει το δικό του μυστικό [29].

### 4.2.2 Θεμελιώδεις Αρχές

Ακολουθεί η ενότητα Θεμελιώδεις Αρχές στην οποία διαμορφώνεται το πλαίσιο συμμόρφωσης για τις αρχές του απορρήτου και αποτελείται από δύο υπο-ενότητες ως πιο κάτω:

#### 4.2.2.1 Αξιολόγηση Αναγκαιότητας και Αναλογικότητα

- Είναι σαφείς, ρητοί και νόμιμοι οι σκοποί επεξεργασίας;

Ο σκοπός της επεξεργασίας είναι σαφώς προσδιορισμένος και γνωστός σε όλους τους συμμετέχοντες. Το ΔΣ αποστέλλει σε όλα τα μέλη του το ενημερωτικό ηλεκτρονικό μήνυμα με οδηγίες χρήσης του συστήματος και ενημέρωση για την επεξεργασία των στοιχείων τους (ονοματεπώνυμο, ηλεκτρονική διεύθυνση, αποτελέσματα ψηφοφορίας).

- Ποια είναι η νομική βάση που καθιστά την επεξεργασία νόμιμη;

Η επεξεργασία των δεδομένων καθίσταται νόμιμη εφόσον οι ψηφοφόροι ενημερώνονται εκ των προτέρων για την πραγματοποίηση της διαδικασίας και ουσιαστικά δεν υπάρχει ανάγκη να τους ζητηθεί συγκατάθεση σύμφωνα με το άρθρο 6(1)(α) του ΓΚΠΔ, αφού η διαδικασία γίνεται σε εθελοντική βάση (και, άρα, η συμμετοχή από μόνη της στην

ψηφοφορία συνιστά δήλωση συγκατάθεσης). Παράλληλα αφού η άσκηση του εκλογικού τους δικαιώματος δεν είναι υποχρεωτική, θα πρέπει να αποφεύγεται οποιοδήποτε είδος εξαναγκασμού της συμμετοχής των ψηφοφόρων.

- Τα προσωπικά δεδομένα που συλλέγονται είναι επαρκή, συναφή και περιορίζονται σε όσα είναι απαραίτητα σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»);

Τα προσωπικά δεδομένα τα οποία συλλέγονται είναι επαρκή, συναφή και περιορίζονται σε όσα είναι απαραίτητα σε σχέση πάντα με το σκοπό για τον οποίο υποβάλλονται σε επεξεργασία. Για την αποστολή του συνδέσμου ψηφοφορίας, απαιτείται η εξεύρεση των ηλεκτρονικών διευθύνσεων των μελών του Κλάδου, όπου την λίστα αυτή την εξασφαλίζει από τη Συντεχνία του ο ΥΕ. Η λίστα περιλαμβάνει επιπλέον προσωπικά δεδομένα των μελών όπως Αριθμό Δελτίου Ταυτότητας και Αριθμό Κοινωνικών Ασφαλίσεων, όπου θα πρέπει να διασφαλίζεται η μη επεξεργασία αυτών των στοιχείων ή οποιωνδήποτε άλλων στοιχείων των ψηφοφόρων, αλλιώς υπάρχει σοβαρός κίνδυνος ο οποίος θα πρέπει να αντιμετωπιστεί αναλόγως. Η εν λόγω λίστα δεν κοινοποιείται στα μέλη.

Η επεξεργασία των αποτελεσμάτων γίνεται αποκλειστικά προς ενημέρωση των ψηφοφόρων, επομένως η χρήση του καταλόγου των ψηφοφόρων που δεν έχουν ψηφίσει θα πρέπει να αποφεύγεται. Όπως έχει αναφερθεί και πιο πάνω, σε χώρες όπως πχ στη Γαλλία η πληροφορία αυτή δεν πρέπει να κοινοποιείται στους λοιπούς ψηφοφόρους. Σε καμία περίπτωση δεν συλλέγονται περισσότερα δεδομένα από όσα πρέπει και αν γίνεται αυτό, είναι ένας σοβαρός κίνδυνος που πρέπει να αντιμετωπιστεί.

- Τα δεδομένα είναι ακριβή και ενημερωμένα;

Το ΔΣ έχει την ευθύνη να εξασφαλίσει την ενημερωμένη λίστα των μελών του Κλάδου, μέσω της Συντεχνίας του. Επιπρόσθετα είναι αρμόδιο να εξασφαλίσει και να καταχωρίσει στο σύστημα τις ακριβείς ηλεκτρονικές διευθύνσεις των μελών, αφού σε αντίθετη περίπτωση τα μέλη δεν θα έχουν την δυνατότητα συμμετοχής στην διαδικασία της ψηφοφορίας.

- Ποια είναι η διάρκεια αποθήκευσης των δεδομένων;

Το σύστημα διατηρεί αποθηκευμένα τα δεδομένα στο διακομιστή του συστήματος τόσο τις ηλεκτρονικές διευθύνσεις όλων των ψηφοφόρων, όσο και τις ψήφους τους, τα οποία παραμένουν αναλλοίωτοι. Όσον αφορά τη διάρκεια αποθήκευσης των δεδομένων στο σύστημα, επαφίεται στις πρόνοιες της σχετικής νομοθεσίας της κάθε χώρας.

#### 4.2.2.2 Μέτρα για την προστασία των προσωπικών δικαιωμάτων των ψηφοφόρων

- Πώς ενημερώνονται οι ψηφοφόροι σχετικά με την επεξεργασία;

Οι ψηφοφόροι ενημερώνονται από το ΔΣ για την λήψη μηνύματος από το σύστημα Helios, στο οποίο περιλαμβάνεται ο σχετικός σύνδεσμος μέσω του οποίου μπορούν να ασκήσουν το δικαίωμα του εκλέγειν.

- Εάν ισχύει, πώς επιτυγχάνεται η συγκατάθεση των υποκειμένων των δεδομένων;

Δεν απαιτείται η συγκατάθεση τους, από την στιγμή που η συμμετοχή τους δεν είναι υποχρεωτική, με την ψήφο του ο κάθε υποψήφιος, εφόσον έχει προηγουμένως ενημερωθεί για τον εθελοντικό χαρακτήρα της διαδικασίας, υποδηλώνει τη συγκατάθεσή του.

Να σημειωθεί ότι οι ψηφοφόροι έχουν την δυνατότητα να αλλάξουν τη ψήφο τους όσες φορές επιθυμούν, όπου μόνο η τελευταία ψήφος θα προστεθεί στο αποτέλεσμα, για αυτή την δυνατότητα τα μέλη ενημερώνονται, πριν την έναρξη της διαδικασίας, με αναφορά στο γεγονός ότι θα μετρήσει μόνο η τελευταία ψήφος τους, αφού κάθε νέα ψήφος σβήνει την προηγούμενη – δικαίωμα διόρθωσης. Την δυνατότητα αυτή την έχουν τα μέλη μέχρι την λήξη της διαδικασίας της ψηφοφορίας. Με την ολοκλήρωση της διαδικασίας είναι αδύνατη οποιαδήποτε τροποποίηση στις ψήφους.

- Πώς μπορούν τα μέλη να ασκήσουν το δικαίωμα πρόσβασης και φορητότητας των προσωπικών τους δεδομένων;

Το σύστημα αποστέλλει στους ψηφοφόρους ηλεκτρονικό μήνυμα στο οποίο περιέχονται οι κωδικοί πρόσβασης, με τους οποίους μπορούν ανά πάσα στιγμή να συνδεθούν στο σύστημα. Κάθε μέλος το οποίο ψηφίζει, αυτόματα λαμβάνει επιβεβαιωτικό μήνυμα, στο οποίο αναφέρεται ότι η ψήφος του έχει υπολογιστεί και μαζί του αποστέλλεται και το αποτύπωμα. Σε περίπτωση που εκ παραδρομής ψηφοφόρος διαγράψει το ηλεκτρονικό μήνυμα με τους κωδικούς τους, ο ΥΕ, έχει την δυνατότητα μέσω του συστήματος να του

σταλούν ξανά, έτσι θα μπορεί να συνδεθεί στο σύστημα. Όπως έχει αναφερθεί, υπάρχει η επιλογή αλλαγής της ψήφου. Σε αυτό εξυπακούεται το σβήσιμο της προηγούμενης ψήφου και το σύστημα θα καταμετρήσει μόνο την τελευταία ψήφο του κάθε ψηφοφόρου.

- Πώς μπορούν τα μέλη να ασκήσουν τα δικαιώματα διόρθωσης και διαγραφής;

Τα μέλη έχουν την δυνατότητα να αλλάξουν τη ψήφο τους όσες φορές επιθυμούν, έτσι ώστε μόνο η τελευταία ψήφος θα μετρηθεί στο αποτέλεσμα, για αυτή την δυνατότητα τα μέλη ενημερώνονται, πριν την έναρξη της διαδικασίας, με αναφορά στο γεγονός ότι θα μετρήσει μόνο η τελευταία ψήφος τους, αφού κάθε νέα ψήφος σβήνει την προηγούμενη – δικαίωμα διόρθωσης. Την δυνατότητα αυτή την έχουν τα μέλη μέχρι τη λήξη της διαδικασίας της ψηφοφορίας, με την ολοκλήρωση της διαδικασίας είναι αδύνατη οποιαδήποτε τροποποίηση στις ψήφους. Δεν εφαρμόζεται το δικαίωμα διαγραφής.

Στην περίπτωση κατά την οποία εντοπιστεί κάποια λανθασμένη καταχώρηση στοιχείων, όπως για παράδειγμα οι ηλεκτρονικές διευθύνσεις, οι ψηφοφόροι θα χρειαστεί να ενημερώσουν άμεσα τον ΥΕ για να προβεί στις δέουσες τροποποιήσεις.

Με την ολοκλήρωση της διαδικασίας αν το αποφασίσει ο Υπεύθυνος Επεξεργασίας, ενημερώνονται οι ψηφοφόροι μέσω του συστήματος για το αποτέλεσμα της ψηφοφορίας (απαιτείται να κάνουν Login για να δουν τα αποτελέσματα), διαφορετικά το ΔΣ ετοιμάζει ανακοίνωση με τα αποτελέσματα και τους την κοινοποιεί. Σε κάθε περίπτωση οι ψηφοφόροι έχουν την δυνατότητα να συνδεθούν στο σύστημα και να επιβεβαιώσουν ότι η ψήφος τους έχει καταχωρηθεί και καταμετρηθεί -δικαίωμα πρόσβασης-, χωρίς όμως να μπορούν να δουν τι έχουν ψηφίσει.

### 4.2.3 Κίνδυνοι

Η παρούσα ενότητα αποτελείται από πέντε υπο-ενότητες στις οποίες αξιολογείται ο κίνδυνος όσον αφορά την ιδιωτική ζωή των ψηφοφόρων σε συνάρτηση με τα μέτρα στη βάση του C.I.A..

#### 4.2.3.1 Υπάρχοντα Μέτρα

- Κρυπτογράφηση: Τεχνικές κρυπτογράφησης χρησιμοποιούνται ευρέως στα συστήματα ηλεκτρονικής ψηφοφορίας. Οι τεχνικές αυτές λειτουργούν ως προληπτικό μέτρο, για την διατήρηση της μυστικότητας των δεδομένων των ψηφοφόρων και των ψήφων τους. Στο σύστημα Helios η κρυπτογράφηση χρησιμοποιείται σε όλα τα στάδια της ψηφοφορίας, συγκεκριμένα γίνεται χρήση της El Gamal ασύμμετρης κρυπτογραφίας, ομομορφικής κρυπτογραφίας καθώς και η πρόκληση Benaloh.
- Μέτρο της λογικής πρόσβασης: Δεν εφαρμόζεται οποιοδήποτε μέτρο επαλήθευσης της ταυτότητας των ψηφοφόρων. Ο ΥΕ καταχωρεί στο σύστημα τις ηλεκτρονικές διευθύνσεις και έπειτα το σύστημα αποστέλλει τα μηνύματα στις διευθύνσεις αυτές. Αν καταχωρήθηκε λανθασμένη ηλεκτρονική διεύθυνση δεν μπορεί να γίνει αντιληπτό από το σύστημα, ούτε λαμβάνει ο ΥΕ κάποια ενημέρωση λόγου χάρη "undeliverable message". Πολύ σημαντικό να γίνει ορθή καταχώρηση των ηλεκτρ. διευθύνσεων για να αποφευχθεί συμπερίληψη διευθύνσεων μη εξουσιοδοτημένων προσώπων. Η επαλήθευση της ταυτότητας δεν μπορεί να γίνει σε μεταγενέστερο στάδιο, γι' αυτό και είναι σημαντικό να καταχωρηθούν εξ αρχής σωστά τα στοιχεία των ψηφοφόρων στο σύστημα. Οι κωδικοί πρόσβασης που λαμβάνουν οι χρήστες δίνονται αυτόματα μέσω του συστήματος. Οι κωδικοί πρόσβασης αποτελούνται από 10 χαρακτήρες, γράμματα (πεζά και κεφαλαία) και αριθμούς. Η χρήση των κωδικών δεν έχει χρονικούς περιορισμούς, οποιαδήποτε στιγμή μπορούν τα μέλη να συνδεθούν και να δουν την πορεία των εκλογών ή τα αποτελέσματα.
- Ασφάλεια και Παρακολούθηση της δραστηριότητας του δικτύου: Το δίκτυο του Οργανισμού προσφέρει δικλείδες ασφαλείας για τον εξοπλισμό του οργανισμού. Υπάρχει ομάδα λειτουργών η οποία είναι υπεύθυνη για την αναβάθμιση, ανανέωση και έλεγχο του υλισμικού και των λογισμικών. Διαθέτουν πλατφόρμες όπως ελέγχουν την κίνηση του δικτύου και αποτρέπουν τυχόν ύποπτες κινήσεις. Μέσω αυτού του δικτύου έχουν την δυνατότητα τα μέλη να ψηφίσουν, αλλά τίποτα δεν τους απαγορεύει να ψηφίσουν από οποιοδήποτε άλλο δίκτυο.
- Διαχείριση του προσωπικού: Ο ανθρώπινος παράγοντας είναι μια από τις μεγαλύτερες απειλές για τα δεδομένα ενός οργανισμού. Η επιλογή του/των ατόμου/ατόμων που θα υποστηρίξουν τεχνικά και οργανωτικά την ηλεκτρονική ψηφοφορία επιβάλλεται να γίνεται με μεγάλη προσοχή. Οι αρμοδιότητες και τα προσωπικά δεδομένα που έχει στην διάθεση του να επεξεργαστεί, απαιτούν υπευθυνότητα και εχεμύθεια. Θα πρέπει να έχουν υπογράψει εξουσιοδότηση εμπιστευτικότητας. Ο ΥΕ θα χρειαστεί να εκτελέσει όλα τα στάδια της διαδικασίας της

ψηφοφορίας, εντός του δικτύου της εταιρείας από ΗΥ του οργανισμού, ο οποίος θα έχει ανανεωμένο λειτουργικό και antivirus. Όπως αναφέρθηκε και στην κρυπτογραφία, το σύστημα προσφέρει δικαιοσύνη και εγκυρότητα εφόσον όμως ο ΥΕ εργάζεται αδιάλειπτα και δίκαια.

- Ελαχιστοποίηση του αριθμού των δεδομένων προσωπικού χαρακτήρα: Η διάρκεια αποθήκευσης των δεδομένων στο σύστημα, παίζει μεγάλο ρόλο, στο παρόν στάδιο η περίοδος επαφίεται στις πρόνοιες της σχετικής νομοθεσίας της κάθε χώρας.

#### 4.2.3.2 Απώλεια Εμπιστευτικότητας (Confidentiality)

Η υπο-ενότητα αυτή περιλαμβάνει τις κύριες επιπτώσεις που έχουν οι ψηφοφόροι αν επερχόταν κίνδυνος, τις κύριες απειλές, τις πηγές κινδύνου, και τα μέτρα όσον αφορά την απώλεια της εμπιστευτικότητας.

Οι πιθανές επιπτώσεις είναι η ψήφιση από μη εξουσιοδοτημένα άτομα, η διαρροή προσωπικών δεδομένων ή/και η ακύρωση της όλης διαδικασίας. Οι κύριες απειλές ο ανθρώπινος παράγοντας και η πιθανή παράνομη πρόσβαση στα δεδομένα, σφάλμα λογισμικού ακόμη και η παραβίαση του συστήματος. Πιθανή πηγή κινδύνου είναι το ανθρώπινο λάθος, λόγου χάρη η σύνδεση μέλους του Κλάδου στο σύστημα μέσω «μολυσμένου» εξοπλισμού.

Τα μέτρα που συμβάλλουν στην αντιμετώπιση των προαναφερθέντων κινδύνων είναι η ορθή διαχείριση του προσωπικού, η ενημέρωση των ψηφοφόρων, η παρακολούθηση της δραστηριότητας του δικτύου από αρμόδια άτομα, και η χρήση απαραίτητων τεχνικών κρυπτογραφίας.

Η σοβαρότητα του κινδύνου, είναι σημαντική αφού τυχόν απώλεια της εμπιστευτικότητας, ίσως επιφέρει μέχρι και ακύρωση της όλης διαδικασίας της ψηφοφορίας. Αντίστοιχα και η πιθανότητα υπολογίζεται ως σημαντική, με βάση τα πιο πάνω.

#### 4.2.3.3 Απώλεια Ακεραιότητας (Integrity)

Αντίστοιχα στην υπο-ενότητα αυτή αναλύονται τόσο τα αίτια και οι συνέπειες μιας ανεπιθύμητης αλλαγής των δεδομένων όσο και η εκτίμηση της σοβαρότητας και της πιθανότητας, στη βάση της απώλειας της ακεραιότητας.

Σε αυτή την περίπτωση οι κύριες επιπτώσεις είναι η μη συμπερίληψη ψηφοφόρων στην διαδικασία της ψηφοφορίας, η συμμετοχή στην διαδικασία μη εξουσιοδοτημένων προσώπων και το μη έγκυρο αποτέλεσμα της ψηφοφορίας. Η κύρια απειλή η οποία θα μπορούσε να οδηγήσει στην επέλευση του κινδύνου, είναι η καταχώρηση λανθασμένης ηλεκτρονικής διεύθυνσης ενός ή περισσότερων ψηφοφόρων λόγω ανθρώπινου λάθους, με αποτέλεσμα ο ανθρώπινος παράγοντας να αποτελεί την κύρια πηγή κινδύνου.

Τα μέτρα που μπορούν να συμβάλουν στην αντιμετώπιση του προαναφερόμενου κινδύνου είναι η ορθή διαχείριση του προσωπικού, η χρήση τεχνικών κρυπτογράφησης αλλά και η προστασία του δικτύου του οργανισμού.

Η σοβαρότητα του κινδύνου αυτού μπορεί να χαρακτηριστεί ως σημαντική με βάση τις πιθανές επιπτώσεις τις οποίες είναι δυνατόν να επιφέρει και η πιθανότητα εξίσου σημαντική.

#### 4.2.3.4 Μη Διαθεσιμότητα Δεδομένων (Availability)

Με τον ίδιο τρόπο διαμορφώνονται και σε αυτό το σημείο όλα τα προαναφερθέντα με βάση την απώλεια της διαθεσιμότητας των δεδομένων.

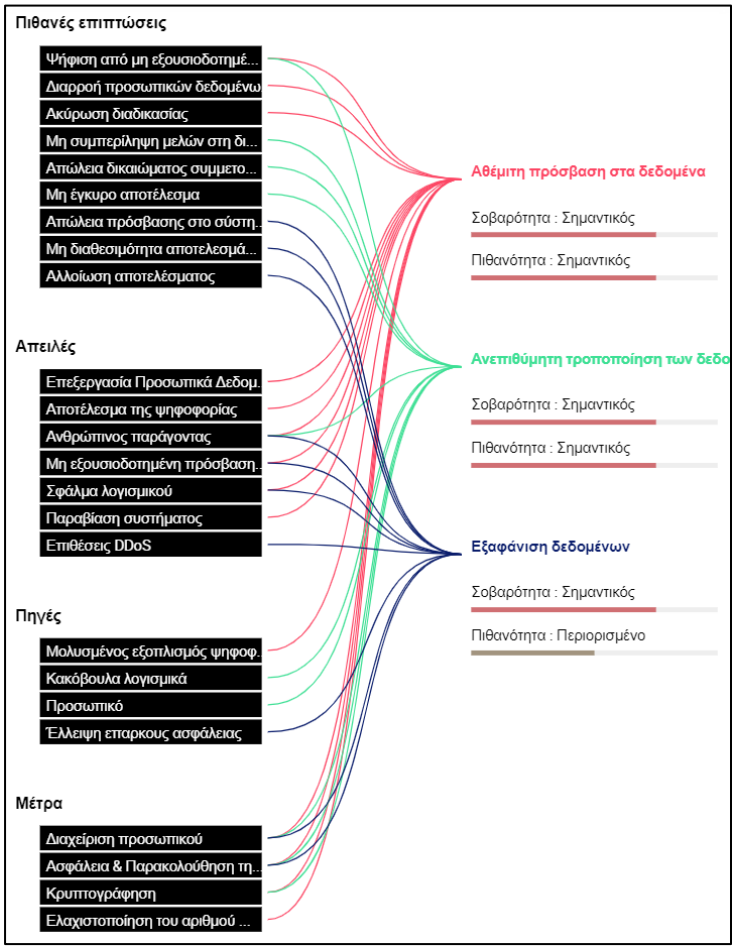
Ως κύριες επιπτώσεις σε περίπτωση επέλευσης του κινδύνου μπορούν να χαρακτηριστούν η αλλοίωση του αποτελέσματος της ψηφοφορίας, η μη διαθεσιμότητα των αποτελεσμάτων της ψηφοφορίας και η απώλεια πρόσβασης με αποτέλεσμα τη μη επαληθευσιμότητα των ψήφων. Οι κύριες απειλές οι οποίες θα μπορούσαν να οδηγήσουν στην επέλευση του κινδύνου είναι ο ανθρώπινος παράγοντας, η μη εξουσιοδοτημένη πρόσβαση στο δίκτυο του οργανισμού λόγω μη ανανεωμένου λειτουργικού ή/και antivirus. Μια άλλη απειλή είναι και η παράνομη πρόσβαση με απώτερο σκοπό τη διαγραφή του αποτελέσματος της ψηφοφορίας ή την «πτώση» του συστήματος πχ μέσω επίθεσης DDoS. Οι πηγές κινδύνου σε αυτή την περίπτωση είναι η χρήση μη κατάλληλου λογισμικού ή/και εξοπλισμού ο οποίος να μην διαθέτει την απαραίτητη ασφάλεια όπως για παράδειγμα ενημερωμένο antivirus.

Τα μέτρα τα οποία συμβάλλουν στην αντιμετώπιση του κινδύνου είναι η παρακολούθηση της δραστηριότητας του δικτύου του οργανισμού, και η συμμόρφωση των ψηφοφόρων στους κανόνες της διαδικασίας.

Η σοβαρότητα του κινδύνου χαρακτηρίζεται ως σημαντική, ενώ η πιθανότητα ως περιορισμένη.

#### 4.2.3.5 Επισκόπηση Κινδύνων

Σε αυτή την υπο-ενότητα έχουμε την δυνατότητα να δούμε σε απεικόνιση (Εικόνα 6), την αποτίμηση της σπουδαιότητας των απειλών, την αξιολόγηση των κινδύνων επεξεργασίας προσωπικών δεδομένων και τις επιπτώσεις στα δεδομένα, σε συνάρτηση με τα υφιστάμενα μέτρα στη βάση του C.I.A..



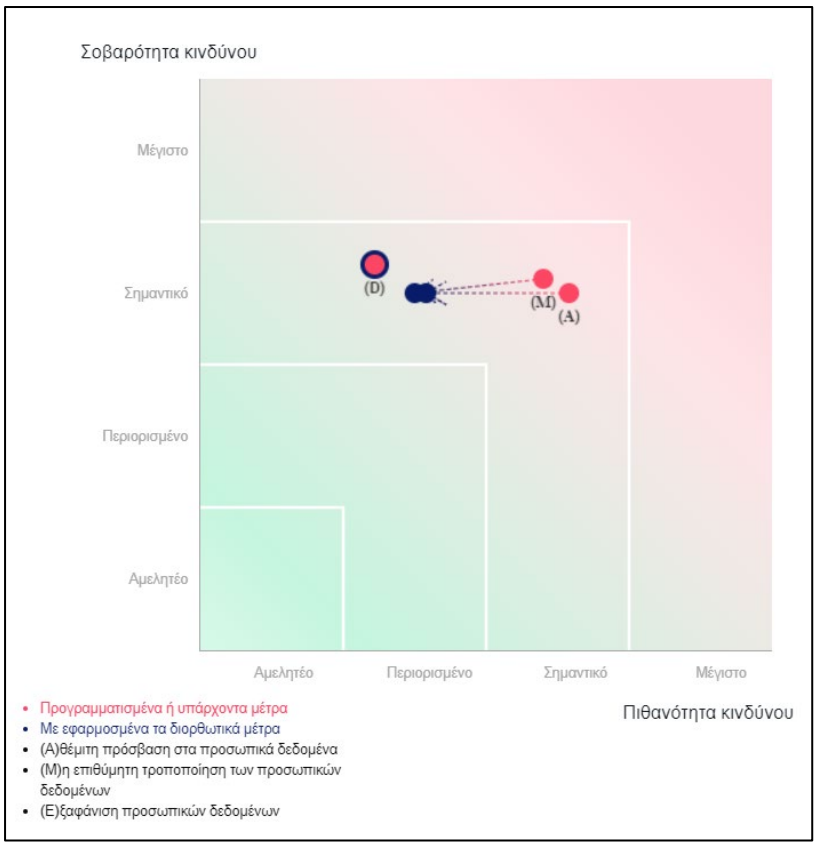
Εικόνα 6: Επισκόπηση κινδύνου

Αφού ολοκληρωθεί η καταχώρηση των στοιχείων στο λογισμικό PIA, επόμενο βήμα είναι η αξιολόγηση των μέτρων όπου εδώ καταλήγουμε στο γεγονός ότι, τα μέτρα είναι εν

μέρει επαρκή και πως υπάρχει δυνατότητα βελτίωσης της ασφάλειας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας, των προσωπικών δεδομένων.

### 4.2.4 Επικύρωση

Η επικύρωση της έκθεσης, περιλαμβάνει τη χαρτογράφηση των κινδύνων (Εικόνα 7), πριν και μετά την εφαρμογή των συμπληρωματικών μέτρων.



Εικόνα 7: Χαρτογράφηση κινδύνων

#### 4.2.4.1 Σχέδιο Δράσης

Στο Σχέδιο Δράσης αναγράφονται αναλυτικά όλα τα πρόσθετα μέτρα τα οποία έχουν εντοπιστεί στην ΕΑΠΔ. Τα μέτρα δεν περιορίζονται μόνο στη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των προσωπικών δεδομένων των μελών αλλά και της μυστικότητας, ιδιωτικότητας και εγκυρότητας των δεδομένων. Ακολουθούν αναλυτικά όλα τα συμπληρωματικά μέτρα της ΕΑΠΔ.

##### 4.2.4.1.1 Θεμελιώδεις Αρχές

- **Διάρκεια αποθήκευσης**

**Σχέδιο δράσης / διορθωτικές ενέργειες:** Αλλαγή πλαισίου, να καθοριστεί εύλογος χρόνος διατήρησης των αποτελεσμάτων και των λοιπών στοιχείων των ψηφοφόρων, στις βάσεις δεδομένων του συστήματος ψηφοφορίας.

**Σχόλιο αξιολόγησης:** Να γίνει άμεσα καθορισμός εύλογου χρόνου διατήρησης των αποτελεσμάτων και των λοιπών στοιχείων των ψηφοφόρων στις βάσεις δεδομένων του συστήματος ψηφοφορίας.

- **Δικαίωμα διόρθωσης και διαγραφής**

**Σχέδιο δράσης / διορθωτικές ενέργειες:** Η διαγραφή της ψήφου δεν επιτρέπεται αλλά η προσθήκη της επιλογής του ΛΕΥΚΟΥ, προσφέρει τη δυνατότητα στους ψηφοφόρους της τροποποίησης της ψήφου τους.

**Σχόλιο αξιολόγησης:** Ένα επιπλέον μέτρο το οποίο θα μπορούσε να φανεί χρήσιμο είναι στις επιλογές που δίνονται στους ψηφοφόρους, να υπάρχει και η επιλογή ΛΕΥΚΟ, και οι ψηφοφόροι να είναι ενήμεροι από πριν για αυτό. Με την προσθήκη της επιλογής ΛΕΥΚΟ, όλοι βλέπουν πως οι εν λόγω ψηφοφόροι έχουν μεν ψηφίσει, χωρίς να γνωρίζουν ότι έχουν δε ρίξει ΛΕΥΚΟ, έτσι αποφεύγεται τόσο ο καταναγκασμός ψήφισής όσο και η συμπερίληψη του ψηφοφόρου στην λίστα αυτών που δεν έχουν συμμετάσχει στην ψηφοφορία.

#### 4.2.4.1.2 Υφιστάμενα Μέτρα

- **Κρυπτογράφηση**

**Σχέδιο δράσης / διορθωτικές ενέργειες:** Καλό σημείο θα ήταν η έναρξη διερεύνησης της δημιουργίας συστημάτων που να είναι μετα-κβαντικά ασφαλή.

**Σχόλιο αξιολόγησης:** Οι τεχνικές κρυπτογράφησης που χρησιμοποιεί το σύστημα HELIOS είναι ικανοποιητικές για εκλογές μεταξύ φοιτητών, οργανώσεων, συνδέσμων κτλ.

- **Μέτρο λογικής πρόσβασης**

**Σχέδιο δράσης / διορθωτικές ενέργειες:** Θα μπορούσε η χρήση Authentication application, κάτι το οποίο ήδη έχουν τα μέλη στα κινητά τους -για τις ηλεκτρονικές τους διευθύνσεις- να προσφέρει περισσότερη ασφάλεια των προσωπικών δεδομένων.

- **Ασφάλεια & Παρακολούθηση της δραστηριότητας του Δικτύου**

**Σχέδιο δράσης / διορθωτικές ενέργειες:** Η συνεχής παρακολούθηση του δικτύου του οργανισμού είναι επιβεβλημένη. Θα μπορούσε να περιοριστεί η πρόσβαση στο σύστημα. Να υπάρχει δυνατότητα να ψηφίσουν μόνο μέσω του δικτύου του οργανισμού για να ελαχιστοποιηθεί ο κίνδυνος κακόβουλης πρόσβασης στο σύστημα. Το δίκτυο του οργανισμού θεωρείται ότι διαθέτει όλες τις απαραίτητες δικλείδες ασφαλείας, για τους ΗΥ και τους χρήστες του.

- **Διαχείριση προσωπικού**

**Σχέδιο δράσης / διορθωτικές ενέργειες:** Το προσωπικό οφείλει να ενημερώσει όλα τα μέλη του Κλάδου -πριν την έναρξη της διαδικασίας ηλεκτρονικής ψηφοφορίας- για μια σειρά από πληροφορίες. Διαπιστώθηκε ότι η ενημέρωση δεν είναι πλήρης (π.χ. δεν γνώριζαν εξ αρχής οι ψηφοφόροι ότι μπορούν να μάθουν οι υπόλοιποι αν ψήφισαν ή όχι) οπότε το προσωπικό θα πρέπει να ετοιμάζει ένα εμπεριστατωμένο μήνυμα προς όλα τα μέλη, στο οποίο θα περιλαμβάνονται όλες οι απαραίτητες πληροφορίες για να υπάρχει αναλυτικότερη και πληρέστερη ενημέρωση.

**Σχόλιο αξιολόγησης:** Συνεχής εκπαίδευση, ενημέρωση για τους σχετικούς κανονισμούς και εποπτεία του προσωπικού. Επιλογή κατάλληλου προσωπικού με βάση τα καθήκοντα που έχουν να εκτελέσουν.

- **Ελαχιστοποίηση του αριθμού των δεδομένων προσωπικού χαρακτήρα**

**Σχέδιο δράσης / διορθωτικές ενέργειες :** Ο χρόνος αποθήκευσης των δεδομένων θα πρέπει να είναι περιορισμένος και να μην επαφίεται στις πρόνοιες της εκαστοτε χώρας.

#### 4.2.4.1.3 Κίνδυνοι – Απώλεια Εμπιστευτικότητας - Confidentiality

**Σχέδιο δράσης / διορθωτικές ενέργειες:** Η εκτέλεση επιπρόσθετων μέτρων μπορεί να επιφέρει μείωση της απώλειας της εμπιστευτικότητας των δεδομένων. Τα μέτρα αυτά είναι η καλύτερη διαχείριση του προσωπικού με εκπαιδεύσεις, η ετοιμασία οδηγού προς τους ψηφοφόρους ο οποίος θα περιλαμβάνει όλες τις απαραίτητες πληροφορίες και τα αποτελέσματα της ΕΑ, η λήψη περαιτέρω μέτρων προστασίας του δικτύου του Οργανισμού, η δυνατότητα ψήφισης μόνο μέσω του δικτύου του Οργανισμού, διαγραφή των αποθηκευμένων στοιχείων από το σύστημα σε εύλογο χρονικό πλαίσιο.

**Σχόλιο αξιολόγησης:** Η απώλεια της εμπιστευτικότητας των δεδομένων είναι ένα πολύ σοβαρό ζήτημα, γι΄ αυτό και θα πρέπει να εξασφαλιστεί η μέγιστη διασφάλιση της.

Λαμβάνοντας υπόψη το σχέδιο δράσης, πώς επαναξιολογείτε τη σοβαρότητα αυτού του κινδύνου (Αθέμιτη πρόσβαση στα προσωπικά δεδομένα); **Σημαντική**
Λαμβάνοντας υπόψη το σχέδιο δράσης, πώς επαναξιολογείτε την πιθανότητα αυτού του κινδύνου (Αθέμιτη πρόσβαση στα προσωπικά δεδομένα); **Περιορισμένη**

#### 4.2.4.1.4 Κίνδυνοι – Απώλεια Ακεραιότητας - Integrity

**Σχέδιο δράσης / διορθωτικές ενέργειες:** Η εκτέλεση συμπληρωματικών μέτρων μπορούν θα επιφέρουν μείωση της απώλειας της ακεραιότητας των δεδομένων. Τα μέτρα αυτά είναι η καλύτερη διαχείριση του προσωπικού με εκπαιδεύσεις, η λήψη περαιτέρω μέτρων προστασίας του δικτύου του Οργανισμού και των ΗΥ, η δυνατότητα ψήφισης μόνο μέσω του δικτύου του Οργανισμού, η χρήση two factor authentication μέσω πχ Authentication app, η λήψη εφεδρικών αντιγράφων ασφαλείας.

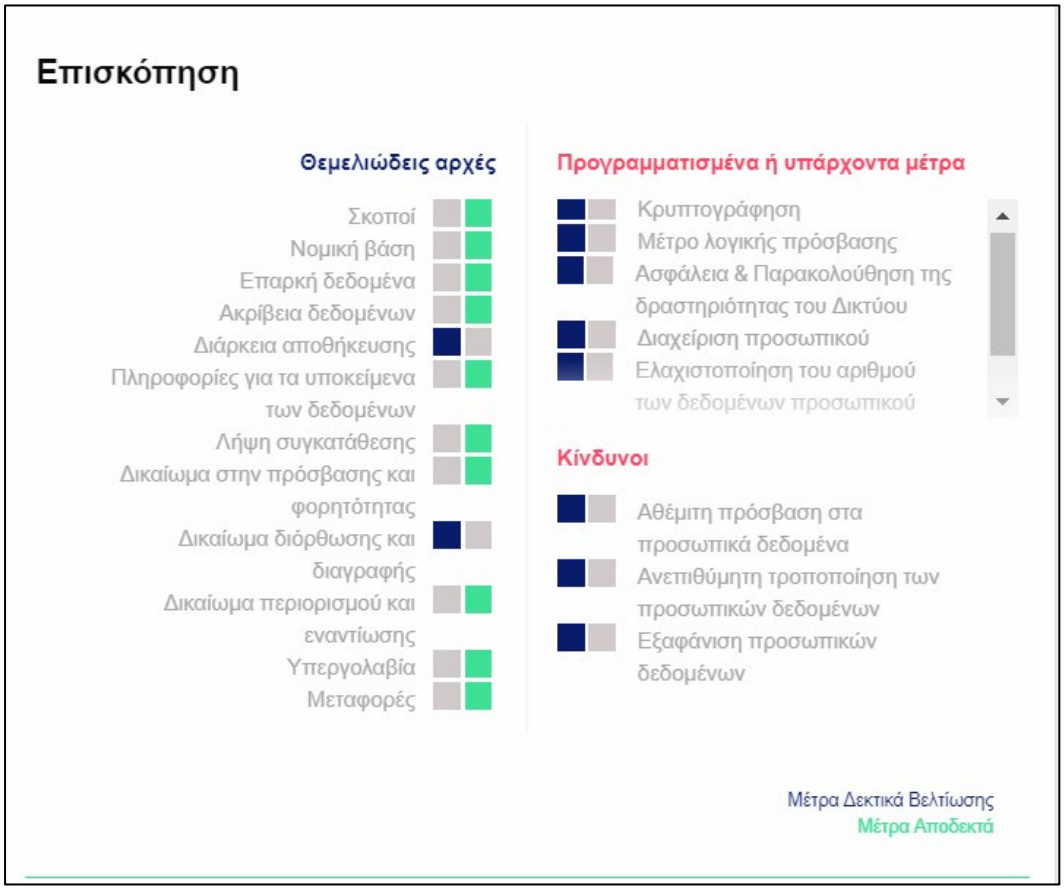
Λαμβάνοντας υπόψη το σχέδιο δράσης, πώς επαναξιολογείτε τη σοβαρότητα αυτού του κινδύνου (Ανεπιθύμητη τροποποίηση των προσωπικών δεδομένων); **Σημαντική**
Λαμβάνοντας υπόψη το σχέδιο δράσης, πώς επαναξιολογείτε την πιθανότητα αυτού του κινδύνου (Ανεπιθύμητη τροποποίηση των προσωπικών δεδομένων); **Περιορισμένη**

#### 4.2.4.1.5 Κίνδυνοι – Μη Διαθεσιμότητα - Availability

**Σχέδιο δράσης / διορθωτικές ενέργειες:** Το Σχέδιο Δράσης να περιλαμβάνει, καλύτερη διαχείριση του προσωπικού με εκπαιδεύσεις, η λήψη περαιτέρω μέτρων προστασίας του δικτύου του Οργανισμού και των ΗΥ, η δυνατότητα ψήφισης μόνο μέσω του δικτύου του Οργανισμού, η χρήση two factor authentication μέσω πχ Authentication app, η δημιουργία εφεδρικών αντιγράφων ασφαλείας.

Λαμβάνοντας υπόψη το σχέδιο δράσης, πώς επαναξιολογείτε τη σοβαρότητα αυτού του κινδύνου (Εξαφάνιση προσωπικών δεδομένων); **Σημαντική**
Λαμβάνοντας υπόψη το σχέδιο δράσης, πώς επαναξιολογείτε την πιθανότητα αυτού του κινδύνου (Εξαφάνιση προσωπικών δεδομένων); **Περιορισμένη**

Το σχέδιο δράσης (Εικόνα 8) περιλαμβάνει την εφαρμογή των πιο πάνω πρόσθετων μέτρων που εντοπίστηκαν κατά τη διάρκεια της εκτίμησης του αντικτύπου.



Εικόνα 8: Επισκόπηση εκτίμησης αντικτύπου – Σχέδιο Δράσης

# Κεφάλαιο 5
# Επίλογος

Η ραγδαία ανάπτυξη της τεχνολογίας επιβάλλει τη συνεχή αναβάθμιση των συστημάτων ηλεκτρονικής ψηφοφορίας σε συνάρτηση πάντα με τη συμμόρφωσή τους με τα μέτρα του ΓΚΠΔ. Μέχρι σήμερα, σε ερευνητικό τουλάχιστον επίπεδο, δεν φαίνεται να είχε επιχειρηθεί μία τέτοια εκτίμηση αντικτύπου στον τομέα αυτό, ο οποίος παρουσιάζει ιδιαίτερες προκλήσεις λόγω του ότι πέρα από την προστασία των προσωπικών δεδομένων, πρέπει και οι ψηφοφόροι να πειστούν και να εμπιστευτούν το σύστημα προκειμένου να υπάρξει ελεύθερη συμμετοχή.

## 5.1 Συμπεράσματα

Με την ολοκλήρωση της παρούσας μεταπτυχιακής διατριβής, συμπεραίνουμε ότι, οι απαιτήσεις των συστημάτων ηλεκτρονικής ψηφοφορίας είναι ποικίλες κυρίως ως προς την ασφάλεια των προσωπικών δεδομένων των ψηφοφόρων. Τα πλεονεκτήματα χρήσης των συστημάτων ηλεκτρονικής ψηφοφορίας είναι πολλά, έτσι ώστε ο κίνδυνος να καθίσταται δυσανάλογος σε σχέση με τα αναμενόμενα οφέλη.

Η μελέτη ανέδειξε ότι υπάρχουν αρκετές μέθοδοι κρυπτογράφησης οι οποίες καλύπτουν τις απαιτήσεις των συστημάτων ηλεκτρονικής ψηφοφορίας. Η αλλαγή κουλτούρας των ψηφοφόρων, το να πειστούν όσο πιο πολλοί ψηφοφόροι στο να μπουν στην διαδικασία να ψηφίσουν, είναι ίσως ένα από τα μεγαλύτερα εμπόδια. Για να πετύχουμε τη βελτίωση της συμμετοχής στις διαδικασίες ηλεκτρονικής ψηφοφορίας χρειάζεται:

- αλλαγή της κουλτούρας των ψηφοφόρων πείθοντας όσους πιο πολλούς ψηφοφόρους γίνεται ότι η διαδικασία ψήφισης μέσω ενός συστήματος ηλεκτρονικής ψηφοφορίας, είναι ασφαλής και αξιόπιστη και ότι κανένας παράγοντας ή αρχή δεν μπορεί να παρέμβει στο σύστημα [2].
- ενδιαφέρον για το αποτέλεσμα της διαδικασίας αλλιώς, η δυνατότητα ψήφισης μέσω ενός συστήματος ηλεκτρονικής ψηφοφορίας, προφανώς δεν θα βελτιώσει την συμμετοχή.

- η χρήση συστημάτων με ανοιχτό κώδικα, βοηθάει τόσο στο να καθοριστούν τα κενά ασφαλείας όσο και να εδραιωθεί στο μυαλό των ψηφοφόρων πως η ευκολία δεν είναι πανάκεια.

Μέσα από το ρεαλιστικό σενάριο που χρησιμοποιήθηκε στην παρούσα μεταπτυχιακή διατριβή, η χρήση ενός συστήματος ηλεκτρονικής ψηφοφορίας μπορεί να χαρακτηριστεί ως η μόνη επιλογή, αφού ένας μεγάλος αριθμός των ψηφοφόρων βρίσκεται διασκορπισμένος σε χώρες του εξωτερικού. Παράλληλα η χρήση ηλεκτρονικής ψηφοφορίας είναι ο πιο άμεσος, ταχύς, ασφαλής και οικονομικός τρόπος ψήφισης σε σύγκριση με την παραδοσιακή διαδικασία ψηφοφορίας.

Η απόλυτη διαφάνεια στην επεξεργασία των δεδομένων, υπό την έννοια ότι όλοι οι χρήστες γνωρίζουν επακριβώς πώς προστατεύονται τα δεδομένα τους χωρίς να διακινδυνεύεται η εκλογική διαδικασία, καθώς και μία επίσημη εκπόνηση εκτίμηση αντικτύπου - στην οποία μάλιστα θα πρέπει να συμβάλλει και ο Υπεύθυνος Προστασίας Δεδομένων (Data Protection Officer – DPO) του οργανισμού - μπορούν να αυξήσουν την εμπιστοσύνη των χρηστών στα συστήματα αυτά, και άρα την αποτελεσματικότητα της ηλεκτρονικής ψηφοφορίας. Σε περίπτωση μάλιστα που ο αρμόδιος φορέας κρίνει ότι παραμένουν υψηλοί κίνδυνοι, μπορεί σε κάθε περίπτωση να διαβουλευτεί με την αρμόδια Αρχή Προστασίας Δεδομένων.

Εν κατακλείδι, η πλήρης αντικατάσταση της παραδοσιακής διαδικασίας ψηφοφορίας με ένα σύστημα ηλεκτρονικής ψηφοφορίας δεν φαίνεται να είναι ακόμη εφικτή.

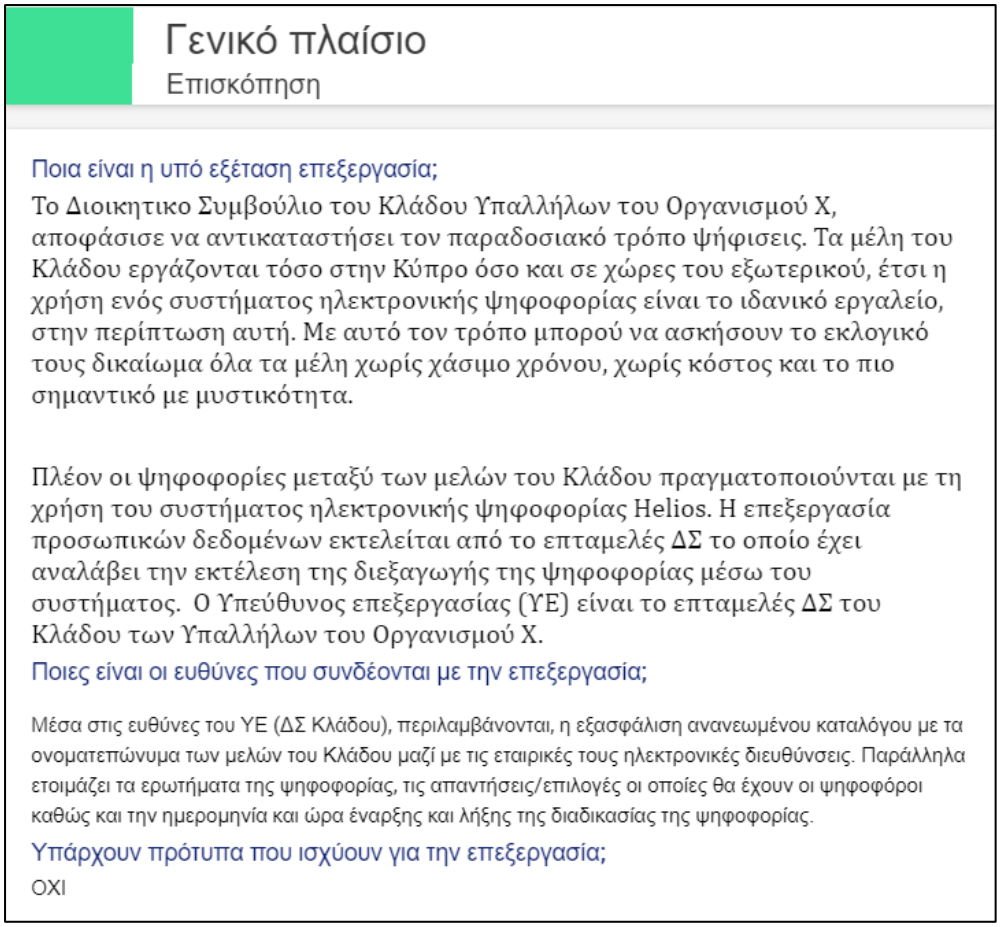
## 5.2 Θέματα για μελλοντική έρευνα

Η ηλεκτρονική ψηφοφορία είναι ένας πολύπλοκος αλλά και πολύ ενδιαφέρων τομέας, του οποίου το μέλλον προμηνύεται λαμπρό. Με βάση τους κινδύνους που έχουν εντοπιστεί στην εκτίμηση αντικτύπου στο 4ο Κεφάλαιο της παρούσας μεταπτυχιακής διατριβής, αναδεικνύεται ότι θα πρέπει να αρχίσουν να διερευνώνται συστήματα ηλεκτρονικής ψηφοφορίας τα οποία να είναι μετα-κβαντικά ασφαλή. Με αυτό το μέτρο επιτυγχάνεται η μείωση της εξάπλωσης των προσωπικών δεδομένων και διασφαλίζεται η αιώνια ιδιωτικότητα των ψήφων.

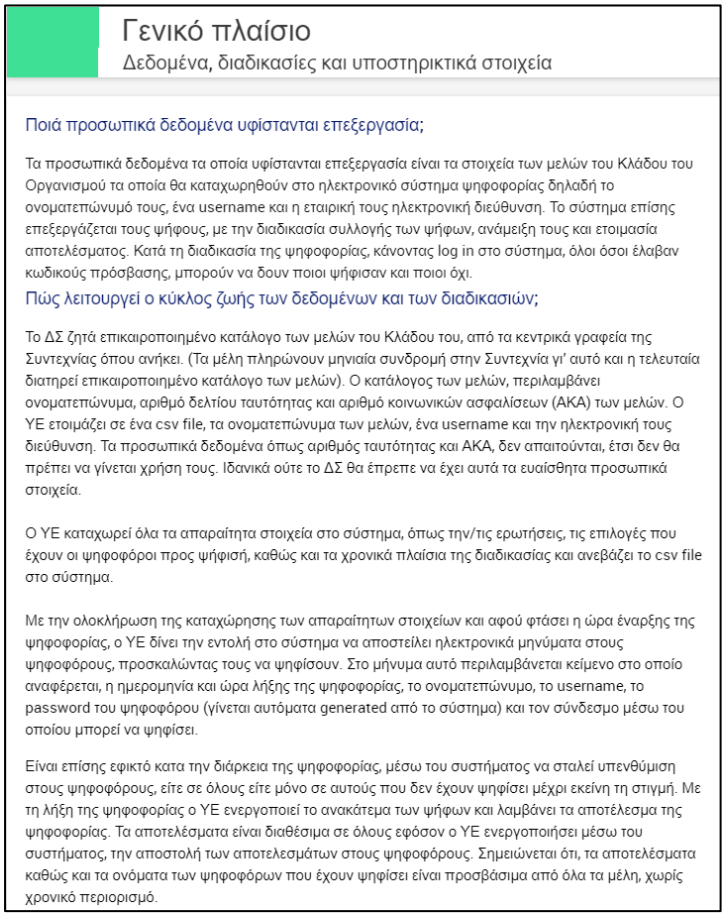
Θα μπορούσε επίσης η ετοιμασία της εκτίμησης αντικτύπου ως προς τα προσωπικά δεδομένα να γίνει υποχρεωτική και να ολοκληρώνεται πριν από την έναρξη χρήσης των συστημάτων ηλεκτρονικής ψηφοφορίας. Παράλληλα τα αποτελέσματα της έκθεσης αντικτύπου να κοινοποιούνται στους ψηφοφόρους, έτσι θα πείθονται όλο και περισσότεροι ότι το σύστημα είναι αξιόπιστο και προσφέρει δικλείδες ασφαλείας, με αποτέλεσμα την αύξηση της συμμετοχής.

# Παράρτημα Α

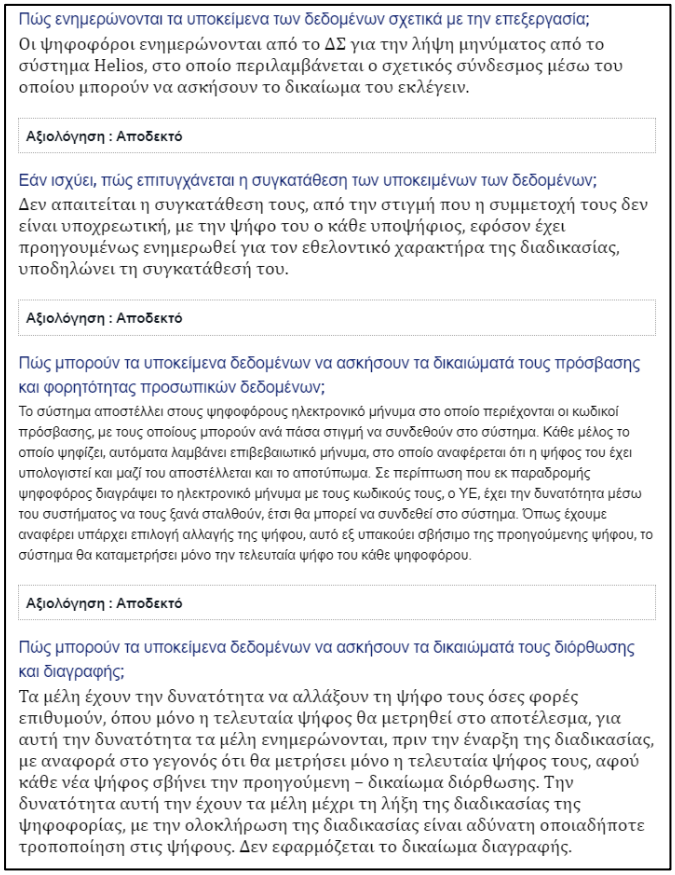
Στο Παράρτημα παρουσιάζεται αναλυτικά μέρος του υλικού, το οποίο έχει καταχωρηθεί ανά ενότητα στο λογισμικό PIA.



Εικόνα 9: Γενικό Πλαίσιο



Εικόνα 10: Θεμελιώδεις Αρχές - Αναλογικότητα και αναγκαιότητα



Εικόνα 11: Θεμελιώδεις Αρχές - Μέτρα για την προστασία των προσωπικών δεδομένων των ψηφοφόρων

# Βιβλιογραφία


[1] S. Risnanto, Y. Abd Rahim, O. Mohd, A. Abdurrohman, «E-Voting: Technology Requirements Mapping,» *TEM Journal,* τόμ. 11, αρ. 3, pp. 1282-1290, 2022.

[2] S. K. M. K. V. T. D. S. K. C. LAMBRINOUDAKIS, «Electronic Voting Systems: Security Implications of the Administrative Workflow».

[3] Ε. Ζάχος, Α. Παγουρτζής, Π. Γρόντας, Υπολογιστική Κρυπτογραφία, Αθήνα: Καλλιπος, 2015.

[4] K. H. Wang, S. K. Mondal, K. Chan, X. Xie, «A Review of Contemporary E-voting: Requirements, Technology, Systems and Usability,» *Data Science and Pattern Recognition, Ubiquitous International,* τόμ. 1, αρ. 1, pp. 31-47, 2017.

[5] «It is enough that the people know there was an election. The people who cast the votes decide nothing. The people who count the votes decide everything.,» 1 12 2017. [Ηλεκτρονικό]. Available: https://observerid.com/it-is-enough-that-the-people-know-there-was-an-election-the-people-who-cast-the-votes-decide-nothing-the-people-who-count-the-votes-decide-everything-joseph-stalin/.

[6] W. Diffie, M. E. Hellman, «New Directions in Cryptography,» *IEEE Transactions on Information Theory,* τόμ. 22, αρ. 6, pp. 644-654, 1976.

[7] Σ. Γ. Σ. Κ. Β. Χ. Μ. Burmester, Σύγχρονη Κρυπτογραφία - Θεωρία και Εφαρμογές, Παπασωτηρίου, 2011.

[8] M. S. N. N. R. R. S. PARK, «Going from bad to worse: from Internet voting to blockchain voting,» *Journal of Cybersecurity,* 2021.

[9] Chaieb M., Yousfi S., Lafourcade P., Robbana R., «Verify-Your-Vote: A Verifiable Blockchain-Based Online Voting Protocol,» σε *Themistocleous M., Rupino da Cunha P. (eds) Information Systems. EMCIS 2018*, Limassol, Cyprus, 2019.

[10] M. Sallal, R. de Frein, A.Malik, «PVPBC: Privacy and Verifiability Preserving E-Voting Based on Permissioned Blockchain,» *Future Internet,* τόμ. 4, αρ. 121, p. 15, 2023.

[11] M. Meyer, B. Smyth, «Exploiting re-voting in the Helios election system,» *Information Processing Letters,* τόμ. 143, pp. 4-19, 2019.

[12] A. Ernest, «The State of Follow My Vote,» 2022. [Ηλεκτρονικό]. Available: https://followmyvote.com/the-state-of-follow-my-vote-2022-report/.

[13] Casaleggio D., Di Nicola V., Marchesi M., Missineo S., Tonelli R., «A Digital Voting System for the 21st Century,» σε *Balis B. et al. (eds) Euro-Par 2020: Parallel Processing Workshops. Euro-Par 2020*, 2021.

[14] U. Jafar, M. Juzaiddin Ab Aziz, Z. Shukur, «Blockchain for Electronic Voting System - Review and Open Research Challenges,» *Sensors (Basel),* Τόμ. %1 από %221,17 5874, 2021.

[15] A. Filipiak, «Design and formal analysis of security protocols, an application to electronic voting and mobile payment,» 2018.

[16] R. Krimmer, M. Volkamer, D. Duenas-Cid, P. Rønne, M. Germann, «Electronig Voting,» σε *7th International Joint Conference, E-Vote-ID 2022*, Bregenz, 2022.

[17] L. Li, «An Electronic Voting Scheme Based on ElGamal Homomorphic Encryption for Privacy Protection,» *J. Phys.: Conf. Ser. 1544 012036,* τόμ. 1544, αρ. 012036, 2020.

[18] P. Paillier, «Public-Key Cryptosystems Based on Composite Degree Residuosity Classes,» σε *International Conference on the Theory and Applications of Cryptographic Techniques*, Berlin, 1999.

[19] R. Suwandi, S. Nasution, F. Azmi, «Secure E-voting System by Utilizing Homomorphic Properties of the Encryption Algorithm,» *TELKOMNIKA,* τόμ. 16, pp. 862-867, 2013.

[20] C. Gentry, «Fully homomorphic encryption using ideal lattices,» σε *STOC '09: Proceedings of the forty-first annual ACM symposium on Theory of computing*, 2009.

[21] Ε. Μάγκος, Β. Χρυσικόπουλος, Ν. Αλεξανδράκης, Μ. Πούλος, «Ηλεκτρονική Ψηφοφορία μέσω Internet: Ουτοπία ή Πραγματικότητα;,» https://users.ionio.gr/~emagos/eDemocracy.PDF, 2012.

[22] M. Green, «Zero Knowledge Proofs: An illustrated primer,» 27 Nov 2017. [Ηλεκτρονικό]. Available: https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer.

[23] Chainlink, «Zero-Knowledge Proof: Applications and Use Cases,» 6 March 2023. [Ηλεκτρονικό]. Available: https://blog.chain.link/zero-knowledge-proof-use-cases/.

[24] Υ. Ε. Ε. Ένωσης, «Eur-Lex,» 1 2 2011. [Ηλεκτρονικό]. Available: https://eur-lex.europa.eu/legal-content/EL/LSU/?uri=celex:31995L0046.

[25] Δ. Τζέλλης, Μ. Μυλώση, Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων, Αθήνα: Νομική Βιβλιοθήκη, 2022.

[26] C. N. d. l. e. d. Libertés, «CNIL,» French Government, [Ηλεκτρονικό]. Available: https://www.cnil.fr/en/privacy-impact-assessment-pia.

[27] B. Adida, «Helios Voting,» [Ηλεκτρονικό]. Available: https://vote.heliosvoting.org/about.

[28] V. Cortier, D. Galindo, S. Glondu, M. Izabachène, «Distributed ElGamal `a la Pedersen - Application to Helios,» WPES'13, Berlin, 2013.

[29] I.Chillotti, N.Gama, M.Georgieva, M.Izabachène, «A Homomorphic LWE Based E-voting Scheme,» σε *International Workshop on Post-Quantum Cryptography*, 2016.

[30] A. Rodriguez-Perez, «My Vote, My (Personal) Data: Remote Electronic Voting and the General Data Protection Regulation,» σε *E-Vote-ID*, Barcelona, Spain, 2020.