

**ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ**  
**ΤΜΗΜΑ ΟΙΚΟΝΟΜΙΚΗΣ ΕΠΙΣΤΗΜΗΣ**



**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ**  
**ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΔΗΜΟΣΙΑ**  
**ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΠΟΛΙΤΙΚΗ**

**ΚΑΙΝΟΤΟΜΕΣ ΥΠΗΡΕΣΙΕΣ ΗΛΕΚΤΡΟΝΙΚΗΣ**  
**ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΚΑΙ**  
**ΕΝΗΜΕΡΩΣΗ ΤΩΝ ΠΟΛΙΤΩΝ**

**ΔΗΜΟΥΛΑΚΗΣ ΙΩΑΝΝΗΣ**

Διπλωματική Εργασία υποβληθείσα στο Τμήμα Οικονομικών Επιστημών του Πανεπιστημίου Πειραιώς ως  
μέρος των απαιτήσεων για την απόκτηση Μεταπτυχιακού Διπλώματος στην Εφαρμοσμένη Δημόσια  
Οικονομική και Πολιτική

**Πειραιάς, Απρίλιος 2025**



**UNIVERSITY OF PIRAEUS**  
**DEPARTMENT OF ECONOMICS**



**MASTER PROGRAM IN**  
**APPLIED PUBLIC ECONOMICS AND POLICY**

**INNOVATIVE E-GOVERNMENT SERVICES FOR THE**  
**SECURITY AND INFORMATION OF CITIZENS**

**By**

**DIMOULAKIS IOANNIS**

Master Thesis submitted to the Department of Economics of the University of Piraeus in partial fulfillment of the requirements for the degree of Master of Science in Applied Public Economics and Policy

**Piraeus, Greece, April 2025**



ΤΜΗΜΑ  
ΟΙΚΟΝΟΜΙΚΗΣ ΕΠΙΣΤΗΜΗΣ  
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

## ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

«Δηλώνω υπεύθυνα ότι το έργο που εκπονήθηκε και παρουσιάζεται στην υποβαλλόμενη διπλωματική εργασία, για τη λήψη του μεταπτυχιακού τίτλου σπουδών, στην «Εφαρμοσμένη Δημόσια Οικονομική και Πολιτική» με τίτλο:

«Καινοτόμες Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης για την ασφάλεια και την ενημέρωση των πολιτών»

---

έχει γραφτεί από εμένα αποκλειστικά στο σύνολό της. Δεν έχει υποβληθεί ούτε εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών στην Ελλάδα ή στο εξωτερικό, ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

Δηλώνω επίσης υπεύθυνα ότι οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης εργασίας αναφέρονται στο σύνολό τους, κάνοντάς πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου.»

Υπογραφή Μεταπτυχιακού Φοιτητή

Ονοματεπώνυμο

Ιωάννης ΔΗΜΟΥΛΑΚΗΣ

*Την εργασία αυτή την αφιερώνω  
στην μητέρα μου, η οποία είναι  
αρωγός σε κάθε μου βήμα.*



## **Ευχαριστίες**

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή κύριο ΣΜΥΡΛΗ Ιωάννη για την καθοδήγηση και την υποστήριξη που μου προσέφερε κατά την εκπόνηση αυτής της εργασίας.



## Περίληψη

Η παρούσα μελέτη διερευνά τον ρόλο των καινοτόμων υπηρεσιών ηλεκτρονικής διακυβέρνησης στην ενίσχυση της ασφάλειας και της πρόσβασης των πολιτών στις πληροφορίες, εστιάζοντας στον ψηφιακό μετασχηματισμό των υπηρεσιών επιβολής του νόμου. Η ηλεκτρονική διακυβέρνηση περιλαμβάνει την εφαρμογή ψηφιακών τεχνολογιών για τη βελτίωση της παροχής δημόσιων υπηρεσιών, την προώθηση της διαφάνειας και την αύξηση της συμμετοχής των πολιτών. Εξετάζοντας τις ηλεκτρονικές υπηρεσίες της Ελληνικής Αστυνομίας και συγκριτικές πρακτικές από άλλες χώρες, η έρευνα αναδεικνύει τις σημαντικές προόδους που επιτυγχάνονται μέσω αυτών των τεχνολογιών.

Βασικές πρωτοβουλίες, όπως η «Police on Line» της Ελλάδας, τα συστήματα CAR-PC, οι ψηφιακές υπηρεσίες GOV.GR και το κουμπί πανικού, καταδεικνύουν πώς τα ψηφιακά εργαλεία εξορθολογίζουν τις επιχειρήσεις, βελτιώνουν την επικοινωνία και προστατεύουν τις ευάλωτες ομάδες. Οι προσπάθειες αυτές συμπληρώνονται από παρόμοιες καινοτομίες στο εξωτερικό, όπως ο ελεγκτής παραβίασης ηλεκτρονικού ταχυδρομείου της ολλανδικής αστυνομίας, η πλατφόρμα Single Online Home του Ηνωμένου Βασιλείου, η εφαρμογή AlertCops της Ισπανίας και οι ψηφιακές υπηρεσίες του Καναδά που επικεντρώνονται στην κοινότητα. Μέσω μιας ανάλυσης SWOT, η μελέτη εντοπίζει τα δυνατά σημεία, τις αδυναμίες, τις ευκαιρίες και τους κινδύνους που συνδέονται με την εφαρμογή υπηρεσιών ηλεκτρονικής διακυβέρνησης, τονίζοντας την ανάγκη αντιμετώπισης προκλήσεων όπως η προστασία της ιδιωτικής ζωής των δεδομένων και η τεχνολογική υιοθέτηση.

Τα ευρήματα υπογραμμίζουν το μετασχηματιστικό δυναμικό της ηλεκτρονικής διακυβέρνησης στην αστυνόμευση, προωθώντας ασφαλέστερες και πιο συνδεδεμένες κοινωνίες. Επενδύοντας σε προηγμένες τεχνολογίες και διεθνή συνεργασία, οι υπηρεσίες επιβολής του νόμου μπορούν να διασφαλίσουν υπηρεσίες δημόσιας ασφάλειας χωρίς αποκλεισμούς, αποτελεσματικές και επικεντρωμένες στον πολίτη σε έναν ολοένα και πιο ψηφιακό κόσμο.

### Λέξεις κλειδιά

Ηλεκτρονική Διακυβέρνηση, ψηφιακός μετασχηματισμός, δημόσια ασφάλεια, αστυνομία.

## **Abstract**

This study explores the role of innovative e-government services in enhancing citizens' security and access to information, focusing on the digital transformation of law enforcement services. E-government involves the application of digital technologies to improve the delivery of public services, promote transparency and increase citizen participation. By examining the e-government services of the Hellenic Police and comparative practices from other countries, the research highlights the significant advances achieved through these technologies.

Key initiatives, such as Greece's Police on Line, CAR-PC systems, GOV.GR digital services and the panic button, demonstrate how digital tools streamline operations, improve communication and protect vulnerable groups. These efforts are complemented by similar innovations abroad, such as the Dutch police's email breach checker, the UK's Single Online Home platform, Spain's AlertCops app and Canada's community-focused digital services. Through a SWOT analysis, the study identifies the strengths, weaknesses, opportunities and risks associated with the implementation of e-government services, highlighting the need to address challenges such as data privacy and technology adoption.

The findings highlight the transformative potential of e-government in policing, promoting safer and more connected societies. By investing in advanced technologies and international cooperation, law enforcement agencies can ensure inclusive, efficient and citizen-centric public safety services in an increasingly digital world.

### **Keywords**

eGovernment, digital transformation, public security, police.

## Περιεχόμενα

Περίληψη.....	ix
Abstract.....	x
ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ.....	
ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ.....	
ΚΕΦΑΛΑΙΟ 1: Ηλεκτρονική Διακυβέρνηση .....	1
1.1. Εισαγωγή .....	1
1.2. Ορισμοί και διαστάσεις Ηλεκτρονικής Διακυβέρνησης.....	2
1.3. Γενικές αρχές ηλεκτρονικής διακυβέρνησης .....	5
1.4. Κατηγορίες Ηλεκτρονικής Διακυβέρνησης .....	8
1.5. Στάδια ηλεκτρονικής διακυβέρνησης.....	10
1.6. Οφέλη ηλεκτρονικής διακυβέρνησης.....	12
1.7. Κίνδυνοι εφαρμογής ηλεκτρονικής διακυβέρνησης .....	13
1.8. Σκοπός .....	14
ΚΕΦΑΛΑΙΟ 2: Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης στην Ελληνική Αστυνομία.....	16
2.1. Police on Line .....	16
2.1.1. Ηλεκτρονική Αλληλογραφία.....	16
2.1.2. CAR-PC.....	17
2.2. Ψηφιακές υπηρεσίες GOV.GR.....	19
2.3. Smart Policing.....	21
2.4. Panic button .....	30

2.5. Ιστότοπος <a href="http://www.astynomia.gr">www.astynomia.gr</a> .....	34
<b>ΚΕΦΑΛΑΙΟ 3: Ανάλυση SWOT για τις Υπηρεσίες Η.Δ. στην Ελληνική Αστυνομία.....</b>	<b>36</b>
3.1. Δυνάμεις.....	36
3.2. Αδυναμίες .....	40
3.3. Ευκαιρίες.....	41
3.4. Κίνδυνοι – Απειλές .....	46
<b>ΚΕΦΑΛΑΙΟ 4: Πρακτικές από χώρες της Ε.Ε. και διεθνώς.....</b>	<b>50</b>
4.1. Εφαρμογή «Check Your Hack» – Ολλανδία.....	50
4.2. Εφαρμογή «Police.UK» - Ηνωμένο Βασίλειο.....	52
4.3. Εφαρμογή «AlertCops» - Ισπανία .....	54
4.4. Εφαρμογή «TPS Mobile» - Καναδάς .....	55
4.5. Εφαρμογή «Police@SG» – Δημοκρατία της Σιγκαπούρης.....	58
4.6. Εφαρμογή «My Police Department App (MyPD)» Ηνωμένες Πολιτείες Αμερικής .....	59
Συμπεράσματα, Προτάσεις .....	61
<b>ΒΙΒΛΙΟΓΡΑΦΙΑ.....</b>	<b>64</b>

## **ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ**

3.1 Ανάλυση SWOT	48
------------------	----

## **ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ**

Εικόνα 1 Τύποι Ηλεκτρονικής Διακυβέρνησης	8
Εικόνα 2 Στάδια Ηλεκτρονικής Διακυβέρνησης	10
Εικόνα 3 Επίδειξη συστήματος CAR PC	18
Εικόνα 4 Επίδειξη Ενιαίας Εφαρμογής Αναζητήσεων	25
Εικόνα 5 Επίδειξη Εφαρμογής Καταγραφής Περιστατικών	26
Εικόνα 6 Επίδειξη Εξοπλισμού – Εργασιών	28
Εικόνα 7 Στατιστικά στοιχεία	29
Εικόνα 8 menu εφαρμογής sky	33
Εικόνα 9 menu εφαρμογής checkyouhack	51
Εικόνα 10 menu εφαρμογής police.uk	53
Εικόνα 11 menu εφαρμογής alertcops	55
Εικόνα 12 menu εφαρμογής Police@SG	58
Εικόνα 13 menu εφαρμογής mypd	61



# ΚΕΦΑΛΑΙΟ 1: Ηλεκτρονική Διακυβέρνηση

## 1.1. Εισαγωγή

Οι τελευταίες δεκαετίες χαρακτηρίζονται από την εκθετική ανάπτυξη του Διαδικτύου και των δυνατοτήτων του καθώς και την ραγδαία ανάπτυξη των Τεχνολογιών Πληροφορίας και Επικοινωνιών (ΤΠΕ) – (Information and Communication Technologies – ICTs), οδηγώντας τις κυβερνήσεις στο αναπόφευκτο συμπέρασμα ότι το Διαδίκτυο (Internet), που είχε ήδη αξιοποιηθεί στην ιδιωτική σφαίρα, θα μπορούσε να χρησιμοποιηθεί αναλογικά και από τους κρατικούς φορείς, με αντικειμενικό σκοπό την βελτίωση των παρεχόμενων υπηρεσιών. Πλέον οι φορείς άσκησης Δημόσιας Διοίκησης, χρησιμοποιούν καθημερινά το διαδίκτυο και τις διαδικτυακές εφαρμογές τόσο στο στάδιο των εσωτερικών λειτουργιών τους όσο και στις συναλλαγές τους με πολίτες, με επιχειρήσεις και με άλλους φορείς. Η διάθεση από την δημοσία διοίκηση ψηφιακών υπηρεσιών ενημέρωσης καθώς και οι ηλεκτρονικές συναλλαγές με τους πολίτες αποτελούν έναν ταχύτατα αναπτυσσόμενο τομέα καθώς ο σύγχρονος τρόπος ζωής έχει αυξήσει τις απαιτήσεις για ψηφιακές υποδομές.

Με την ανάπτυξη εφαρμογών ηλεκτρονικής διακυβέρνησης τα κοινωνικοοικονομικά οφέλη είναι πολλαπλά. Ο ρόλος που παίζουν οι ΤΠΕ στην αύξηση της διαφάνειας, την ενίσχυση των δημοκρατικών θεσμών, διαμέσου της εξ αποστάσεως συμμετοχής των πολιτών στην δημόσια διοίκηση, συνδυαστικά με την παροχή δημοσίων υπηρεσιών προς τους πολίτες της χώρας είναι κομβικός και αδιαμφισβήτητος. Όσον αφορά την βελτίωση της σχέσης μεταξύ κράτους και πολιτών, η υλοποίηση πολιτικών ηλεκτρονικής διακυβέρνησης ουσιαστικά μεταβάλλει και επαναπροσδιορίζει τον τρόπο λειτουργίας του κράτους, καθώς συμβάλει στην παροχή υπηρεσιών αυξημένης ποιότητας, στην καλύτερη αξιοποίηση του ανθρώπινου δυναμικού και των διαθέσιμων πόρων και στη μείωση του χρόνου και του κόστους που απαιτείται για την ολοκλήρωση σχετικών υποθέσεων.

Λαμβάνοντας υπόψη τις αυξανόμενες προκλήσεις, στο διαρκώς μεταβαλλόμενο περιβάλλον ασφάλειας, καθίσταται σαφές σε όλους ότι η ελεύθερη κυκλοφορία προσώπων, η παγκοσμιοποίηση και ο ψηφιακός μετασχηματισμός συνθέτουν νέες προκλήσεις που

καλούνται να διαχειριστούν οι σύγχρονες Αρχές Επιβολής του Νόμου. Στην ψηφιακή εποχή εκμηδενίζονται τα γεωγραφικά όρια και καθίσταται πλέον δυσδιάκριτη η διαφοροποίηση μεταξύ της θεωρούμενης εσωτερικής και εξωτερικής ασφάλεια. Για την Ελληνική Αστυνομία, που αποτελεί τον κύριο πυλώνα πάνω στον οποίο οικοδομείται η ασφάλεια στο εσωτερικό της Χώρας σε εθνικό επίπεδο, γίνεται κατανοητή η σκοπιμότητα και η κοινωνική προσταγή να διατηρήσει την προληπτική της ισχύ, αναπροσαρμόζοντας το μοντέλο λειτουργίας της, έχοντας υπόψη τόσο τις αναδυόμενες προκλήσεις στο εγχώριο και διεθνές, περιβάλλον ασφάλειας, όσο και τις τεχνολογικές και καινοτόμες δυνατότητες που προσφέρει το πλαίσιο μετάβασης στην Ηλεκτρονική Διακυβέρνηση του δημόσιου τομέα, για βελτιωμένες Υπηρεσίες ασφάλειας και ενημέρωσης πολιτών.

## **1.2. Ορισμοί και διαστάσεις Ηλεκτρονικής Διακυβέρνησης**

Ο όρος ηλεκτρονική διακυβέρνηση έχει χρησιμοποιηθεί για να αποδώσει εννοιολογικά και να δώσει υπόσταση σε ένα ευρύ φάσμα ενεργειών, από τις «διαδικτυακές κυβερνητικές υπηρεσίες» έως και «την ανταλλαγή πληροφοριών και υπηρεσιών ηλεκτρονικά με πολίτες, επιχειρήσεις και έτερους κυβερνητικούς φορείς». Η Ηλεκτρονική Διακυβέρνηση δεν περιορίζεται απλά στην εφαρμογή υπολογιστικών συστημάτων και λογισμικών. Περιλαμβάνει και ουσιαστικές αλλαγές στις διαδικασίες διοίκησης του κράτους, οι οποίες μπορούν να προσφέρουν σημαντικά οφέλη, ενισχύοντας την αποδοτικότητα και την αποτελεσματικότητα της δημόσιας διοίκησης (Ronci, 2019). Με την εξέλιξη των ΤΠΕ η Η-Δ παύει πλέον να αντιμετωπίζεται ως ένα τεχνολογικό εργαλείο και λογίζεται ως μια ολοκληρωμένη πρακτική άσκησης δημόσιας διοίκησης. Καθώς πρόκειται για ένα φαινόμενο που εξελίσσεται δυναμικά δεν υπάρχει ένας καθολικός ορισμός της ηλεκτρονικής διακυβέρνησης αλλά ποικιλόμορφες προσεγγίσεις ανάλογα την οπτική γωνία που εξετάζεται αυτή (Halchin, 2004).

Η Ηλεκτρονική Διακυβέρνηση είναι η χρήση των τεχνολογιών της πληροφορικής και των επικοινωνιών (ΤΠΕ) στις δημόσιες διοικήσεις, σε συνδυασμό με οργανωτικές αλλαγές και νέες δεξιότητες του προσωπικού, για την βελτίωση των δημοσίων υπηρεσιών, των δημοκρατικών διαδικασιών και την ενίσχυση της στήριξης στις δημόσιες πολιτικές (Σμυρλής, 2022).

Έχουν διατυπωθεί αρκετοί ορισμοί για την έννοια της Ηλεκτρονικής Διακυβέρνησης, ορισμένοι από τους οποίους παραθέτονται ακολούθως:

Σύμφωνα με την Παγκόσμια Τράπεζα (2015), ο όρος «Ηλεκτρονική Διακυβέρνηση» αναφέρεται στην χρήση από τους κυβερνητικούς φορείς τεχνολογιών πληροφοριών (όπως δίκτυα ευρείας περιοχής, Διαδίκτυο και φορητοί υπολογιστές) που έχουν την δυνατότητα να αναδιαμορφώνουν τις σχέσεις με τους πολίτες, τις επιχειρήσεις και άλλους κρατικούς φορείς. Αυτές οι τεχνολογίες μπορούν να εξυπηρετήσουν ποικίλους διαφορετικούς σκοπούς: καλύτερες κυβερνητικές υπηρεσιών στους πολίτες, βελτίωση των συναλλαγών με τις επιχειρήσεις, ενδυνάμωση των πολιτών μέσω της πρόσβασης στην πληροφόρηση, μείωση της διαφθοράς και αύξηση διαφάνειας».

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (Ο.Ο.Σ.Α) κατά το έτος 2003 έδωσε τον εξής ορισμό: «η ηλεκτρονική διακυβέρνηση είναι η χρήση των τεχνολογιών πληροφοριών και επικοινωνίας, και ιδιαίτερα του Διαδικτύου, ως εργαλείο για την επίτευξη καλύτερη κυβέρνηση».

Ο Οργανισμός Ηνωμένων Εθνών (Ο.Η.Ε.), ορίζει ότι: «Ηλεκτρονική διακυβέρνηση είναι η χρήση των ΤΠΕ για την αποτελεσματικότερη και αποδοτικότερη παροχή κυβερνητικών υπηρεσιών στους πολίτες και τις επιχειρήσεις. Είναι η εφαρμογή των ΤΠΕ στις κυβερνητικές λειτουργίες, για την επίτευξη δημοσίων σκοπών με ψηφιακά μέσα».

Σύμφωνα με την Ευρωπαϊκή Ένωση ηλεκτρονική διακυβέρνηση (eGovernment) ορίζεται ως: «η χρήση των τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ) στις δημόσιες διοικήσεις, σε συνδυασμό με οργανωτικές αλλαγές και νέες δεξιότητες του προσωπικού. Σκοπός είναι η βελτίωση των δημόσιων υπηρεσιών, καθώς και η ενίσχυση των δημοκρατικών διαδικασιών και των διαδικασιών στήριξης των δημόσιων πολιτικών».

Η κυβέρνηση των Ηνωμένων Πολιτειών Αμερικής (Η.Π.Α.) ορίζει την ηλεκτρονική διακυβέρνηση ως: «την χρήση από την κυβέρνηση εφαρμογών Διαδικτύου ή άλλων τεχνολογιών πληροφοριών για την βελτίωση της πρόσβασης και της παροχής κυβερνητικών πληροφοριών και υπηρεσιών στο κοινό, σε άλλες υπηρεσίες και κρατικούς φορείς· ή για την βελτίωση στις κυβερνητικές λειτουργίες ως προς την αποτελεσματικότητα, την αποδοτικότητα, την ποιότητα υπηρεσιών ή τον μετασχηματισμό τους»

Στην Βικιπαίδεια αναφέρεται ότι: «ηλεκτρονική διακυβέρνηση, χαρακτηρίζεται γενικά η εισαγωγή των τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ), κυρίως του διαδικτύου, στη δημόσια διοίκηση και οι νέες διοικητικές πρακτικές, τις οποίες οι τεχνολογίες αυτές εισήγαγαν. Ο όρος αυτός δημιουργήθηκε με τις γενικότερες πρακτικές, σύμφωνα με τις οποίες τοποθετείται το επίθετο «ηλεκτρονικό-ή» (“e”) με σκοπό να δώσει έμφαση στον ηλεκτρονικό

τρόπο παραγωγής και διανομής των υπηρεσιών (ηλεκτρονικό εμπόριο, ηλεκτρονικό επιχειρείν, ηλεκτρονική μάθηση κλπ.). Υπάρχουν δύο διαφορετικά ρεύματα προσέγγισης της Ηλεκτρονικής Διακυβέρνησης. Σύμφωνα με την επιχειρηματική προσέγγιση, η ηλεκτρονική διακυβέρνηση είναι «η εφαρμογή εργαλείων και τεχνικών του ηλεκτρονικού εμπορίου στη λειτουργία της διακυβέρνησης» με σκοπό τη μείωση του κόστους και την αύξηση της αποδοτικότητας. Σύμφωνα με τη συμμετοχική προσέγγιση, η ηλεκτρονική διακυβέρνηση έχει τη δυναμική να «βελτιώσει τη δημοκρατική συμμετοχή» και να «υπερκεράσει τη πολιτική αποστασιοποίηση». Η αντίληψη αυτή εστιάζει σε πρωτοβουλίες που ενισχύουν την εμπιστοσύνη των πολιτών προς την κυβέρνηση με πολιτικές που προωθούν τη διαφάνεια, την υπευθυνότητα και τη συμμετοχικότητα».

Από τους παραπάνω ποικιλόμορφους ορισμούς που έχουν αναπτυχθεί για την Ηλεκτρονική Διακυβέρνηση σε συνδυασμό με τις αναφορές για αξιοποίηση των ΤΠΕ, για την υποστήριξη των κυβερνητικών λειτουργιών, την συμμετοχή των πολιτών και την παροχή κυβερνητικών υπηρεσιών, διακρίνονται τέσσερις βασικές διαστάσεις στην εφαρμογή της Η-Δ (Πομπόρτσας, 2017):

- Ηλεκτρονικές υπηρεσίες (e-services)
- Ηλεκτρονική Διαχείριση (e-management)
- Ηλεκτρονική Δημοκρατία (e-democracy)
- Ηλεκτρονικό Εμπόριο (e-commerce)

Η διάσταση των Ηλεκτρονικών Υπηρεσιών αναφέρεται στην διάθεση με ηλεκτρονικά μέσα κυβερνητικών πληροφοριών, προγραμμάτων και υπηρεσιών. Το σύνολο αυτών είναι προσβάσιμο καθ' όλο το εικοσιτετράωρο μέσω του διαδικτύου ή άλλων εφαρμογών.

Η διάσταση της Ηλεκτρονικής Διαχείρισης περιλαμβάνει τα πληροφοριακά συστήματα των δημόσιων υπηρεσιών και την αξιοποίηση της τεχνολογίας των πληροφοριών με στόχο την αναδιάρθρωση και βελτίωση της λειτουργίας τους. Προκειμένου να καταστεί επιτυχημένη μια στρατηγική ηλεκτρονικής διαχείρισης είναι απαραίτητη η οργανωτική αναδιάρθρωση της δημόσιας διοίκησης, με αναπροσαρμογή του τρόπου εκτέλεσης εργασιών στο εσωτερικό της.

Η διάσταση της Ηλεκτρονικής Δημοκρατίας αφορά την χρήση των ΤΠΕ για την υποστήριξη και ενίσχυση της δημοκρατίας, των δημοκρατικών θεσμών και των δημοκρατικών διαδικασιών, μέσω της ενημέρωσης και ενεργής συμμετοχής των πολιτών στα κοινά (CDDG 2020).

Η διάσταση του Ηλεκτρονικού Εμπορίου συνδέεται με την «εμπορική» πλευρά της κυβέρνησης καθώς προβαίνουν σε οικονομικές συναλλαγές με ιδιώτες είτε ως προμηθευτές είτε ως αγοραστές, μέσω διαδικτύου. Παράδειγμα τέτοιων συναλλαγών που εφαρμόζονται οι αρχές του ηλεκτρονικού εμπορίου είναι η πληρωμή φόρου εισοδήματος, λογαριασμών κοινής ωφελείας από τους πολίτες είτε η προμήθεια από τους δημόσιους φορείς με υλικά μέσω του συστήματος ηλεκτρονικής προμήθειας (Γιαννουκάκου 2011).

### **1.3. Γενικές αρχές ηλεκτρονικής διακυβέρνησης**

Η Διακήρυξη του Ταλίν για την ηλεκτρονική διακυβέρνηση του 2017 σηματοδότησε ένα ορόσημο για μια αξιόπιστη και καινοτόμο ηλεκτρονική διακυβέρνηση στην Ευρώπη (Ευρωπαϊκή Επιτροπή 2017). Παρόλα αυτά, η εδραίωση της ηλεκτρονικής διακυβέρνησης έχει ως απόρροια την ανάγκη εφαρμογής μεταβολών στην οργάνωση των διοικητικών φορέων αλλά και στο ρυθμιστικό πλαίσιο λειτουργίας αυτών. Ειδικότερα, οι γενικές αρχές που πρέπει να διέπουν την ψηφιακή διακυβέρνηση σύμφωνα με την προρρηθείσα Διακήρυξη είναι οι εξής:

- **Αρχή της χρηστής Διοίκησης**

Η δημόσια διοίκηση βασίζεται σε μια σειρά από αρχές οι οποίες διέπουν και νομιμοποιούν την δράση της. Οι αρχές αυτές βασίζονται στην νομική θεωρία, την νομολογία και τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (άρθρο 41). Στην προσπάθεια να μελετηθεί το περιεχόμενο αυτής της αρχής, πρέπει να επικεντρωθούμε στα παρακάτω:

Η αρχή της χρηστής διοίκησης επιβάλλει στα διοικητικά όργανα, να ασκούν τις αρμοδιότητές τους σύμφωνα με τις αρχές της χρηστής και καλόπιστης διοίκησης ώστε κατά την εφαρμογή των σχετικών διατάξεων να αποφεύγονται οι ανεπιεικείς ή και δογματικές ερμηνείες. Ουσιαστικά, όμως, η έννοια της χρηστής διοίκησης παραμένει μια πολύ γενική και αόριστη αρχή. Το Συμβούλιο της Επικρατείας την ορίζει αρνητικά, χαρακτηρίζοντας ορισμένες πράξεις ή παραλείψεις της διοίκησης ως αντικείμενες στην αρχή της χρηστής (ή εύρυθμης) διοίκησης. Η διακριτική ευχέρεια δεν επιτρέπει στη διοίκηση να ταλαιπωρεί χωρίς λόγο τον πολίτη. Αντιθέτως, σύμφωνα με την αρχή της χρηστής διοίκησης, ιδίως όταν η διοίκηση δρα στο πλαίσιο της διακριτικής της ευχέρειας, οφείλει να διαφυλάσσει τα έννομα συμφέροντα του πολίτη και να τον διευκολύνει στην άσκηση των δικαιωμάτων του.

Με την αρχή της νομιμότητας εκφράζεται η σχέση μεταξύ νομοθετικής εξουσίας και δημόσιας διοίκησης, σε ένα κράτος δικαίου. Η αρχή της νομιμότητας εκφράζει τις εξής δύο

πτυχές: α) ότι η δημόσια διοίκηση υπόκειται στο δίκαιο και οφείλει να σέβεται τις επιταγές και τις απαγορεύσεις του και β) ότι η δημόσια διοίκηση μπορεί να περιορίσει τα δικαιώματα και τις ελευθερίες καθώς και την ιδιοκτησία των πολιτών μόνο βάσει νόμου. Με την υπαγωγή της δημόσιας διοίκησης στους κανόνες δικαίου που ψηφίζονται από το όργανο που διαθέτει τη νομοθετική αρμοδιότητα, το Κοινοβούλιο, επιτυγχάνεται έμμεσα η υποταγή της διοίκησης στο εκλογικό σώμα, στο λαό με τη στενή έννοια, ως φορέα της λαϊκής κυριαρχίας. Συνδέεται άρρηκτα με την αρχή του κράτους δικαίου (άρθρο 25 §1 Σ) και κατά συνέπεια και με την αρχή της διάκρισης των λειτουργιών (άρθρο 26 Σ).

- Αρχή μόνον άπαξ

Η αρχή βάση της οποίας πολίτες και επιχειρήσεις υποβάλλουν μόνο μία φορά τις απαιτούμενες πληροφορίες κατά την αλληλεπίδρασή τους με την δημόσια διοίκηση. Ως εκ τούτου οι φορείς δημόσιας διοίκησης είναι υποχρεωμένοι να ανταλλάσσουν αυτές τις πληροφορίες μεταξύ τους και να επαναχρησιμοποιούν τα ήδη υπάρχοντα δεδομένα. Κατά αυτόν τον τρόπο αποδεσμεύονται από την υποχρέωση παροχής εκ νέου πληροφοριών ήδη γνωστών στην δημόσια διοίκηση ενώ εξαιρούνται οι περιπτώσεις που απαιτούν επικαιροποίηση. Στο πλαίσιο αυτό λαμβάνονται όλα τα απαραίτητα μέτρα τηρουμένων δεόντως των κανόνων που αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα.

Απαραίτητη προϋπόθεση για την καθολική εφαρμογή της, αποτελεί η επίτευξη υψηλού επιπέδου διαλειτουργικότητας των πληροφοριακών συστημάτων των δημόσιων φορέων. Με βάση το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας ως διαλειτουργικότητα ορίζεται η *«ικανότητα των οργανισμών να αλληλεπιδρούν προς την κατεύθυνση της επίτευξης αμοιβαίως ωφέλιμων στόχων, οι οποίοι αφορούν την ανταλλαγή πληροφοριών και γνώσεων μεταξύ των εν λόγω οργανισμών διά μέσου των επιχειρησιακών διαδικασιών που υποστηρίζουν, μέσω της ανταλλαγής δεδομένων μεταξύ των οικείων συστημάτων ΤΠΕ»* (Ευρωπαϊκή Επιτροπή 2017).

Η διαλειτουργικότητα στις δημόσιες υπηρεσίες στηρίζεται σε ένα μοντέλο τεσσάρων επιπέδων:

1) Θεσμικό επίπεδο: Αφορά στην εναρμόνιση των νομικών πλαισίων, που καθορίζουν τον τρόπο οργάνωσης και λειτουργίας των δημόσιων διοικήσεων

2) Οργανωτικό επίπεδο: Αναφέρεται στον καθορισμό των στόχων, τη διαμόρφωση διαδικασιών (κυρίως διοικητικών–οικονομικών) και την επίτευξη συνεργασίας των φορέων. Πολλές φορές για την επίτευξη τους απαιτούνται νομοθετικές ρυθμίσεις καθώς και συμφωνίες μεταξύ των εμπλεκόμενων.

3) Σημασιολογικό επίπεδο: Αναφέρεται στα περιεχόμενα της εφαρμογής που θα καλύψει η διαλειτουργικότητα. Διασφαλίζει ότι η ακριβής έννοια των ανταλλασσόμενων πληροφοριών είναι κατανοητή από όλους. Είναι η βάση για κοινή αντίληψη των οντοτήτων των εφαρμογών, βασικών εννοιών και απαιτούμενων βημάτων. Σημαντική δράση είναι η υιοθέτηση ενός κοινού λεξιλογίου-ορολογίας από όλα τα συστήματα και τις υπηρεσίες

4) Τεχνικό επίπεδο: Η ικανότητα μεταφοράς και χρησιμοποίησης της πληροφορίας με ομοιογενή και αποτελεσματικό τρόπο μεταξύ των συστημάτων πληροφορικής. Το επίπεδο αυτό αναφέρεται σε τεχνικές προδιαγραφές υλικού και λογισμικού.

Τα πληροφοριακά συστήματα κάθε οργανισμού οργανώνονται σύμφωνα με τις ανάγκες, τις απαιτήσεις και τους στόχους που έχει θέσει με αποτέλεσμα, να καθίσταται δυσχερής έως και ανέφικτη η αλληλεπίδραση μεταξύ αυτών. Η επίτευξη υψηλού επιπέδου διαλειτουργικότητας μεταξύ των πολιτών, των εμπλεκόμενων δημόσιων φορέων και των επιχειρήσεων αποτελεί απαραίτητη προϋπόθεση για αποτελεσματικές και πραγματικά ωφέλιμες ψηφιακές δημόσιες υπηρεσίες.

- Εξ ορισμού διασυνοριακός χαρακτήρας των υπηρεσιών

Οι δημόσιες υπηρεσίες θα πρέπει να εκτείνονται πέρα από τα εθνικά σύνορα και να συνδέονται με παρόμοιες υπηρεσίες σε επίπεδο Ευρωπαϊκής Ένωσης, καθιστώντας τις διαθέσιμες στο διαδίκτυο σε όλους τους πολίτες στην Ε.Ε. χωρίς διακρίσεις. Κατά τον τρόπο αυτό οικοδομείται μια ψηφιακή ενιαία αγορά, που διευκολύνει την κινητικότητα των πολιτών και των επιχειρήσεων, διασφαλίζοντας ένα ευνοϊκό κλίμα για όσους διαμένουν, σπουδάζουν και εργάζονται οπουδήποτε σε ολόκληρη την Ευρώπη. Στο πλαίσιο του μηχανισμού «Connecting Europe Facility - CEF» (Συνδέοντας την Ευρώπη) ενισχύεται η ψηφιακή συνδεσιμότητα και κατ' επέκταση διευκολύνεται η διασυνοριακή διαλειτουργικότητα μεταξύ των δημόσιων διοικήσεων.

- Εξ ορισμού ψηφιακός χαρακτήρας των υπηρεσιών:

Το Ελληνικό Κράτος και οι φορείς του θα πρέπει να αναδείξουν την παροχή υπηρεσιών μέσω ψηφιακών καναλιών ως την πρωτίστως προτιμώμενη ενέργεια για όσους αποφασίζουν να συνδιαλλαγούν μαζί τους, χωρίς ωστόσο να αποκλείονται από τις παρεχόμενες υπηρεσίες όσοι επιλέγουν την επικοινωνία με φυσικό τρόπο ή στερούνται προσβάσεων στο ψηφιακό περιβάλλον. Μέσα σε αυτό το πλαίσιο θα περιοριστεί η διακίνηση φυσικής αλληλογραφίας και θα ενισχυθεί η ανταλλαγή ήδη υπαρχόντων ψηφιακών δεδομένων μεταξύ των φορέων απαλλάσσοντας τους πολίτες από την υποβολή εγγράφων.

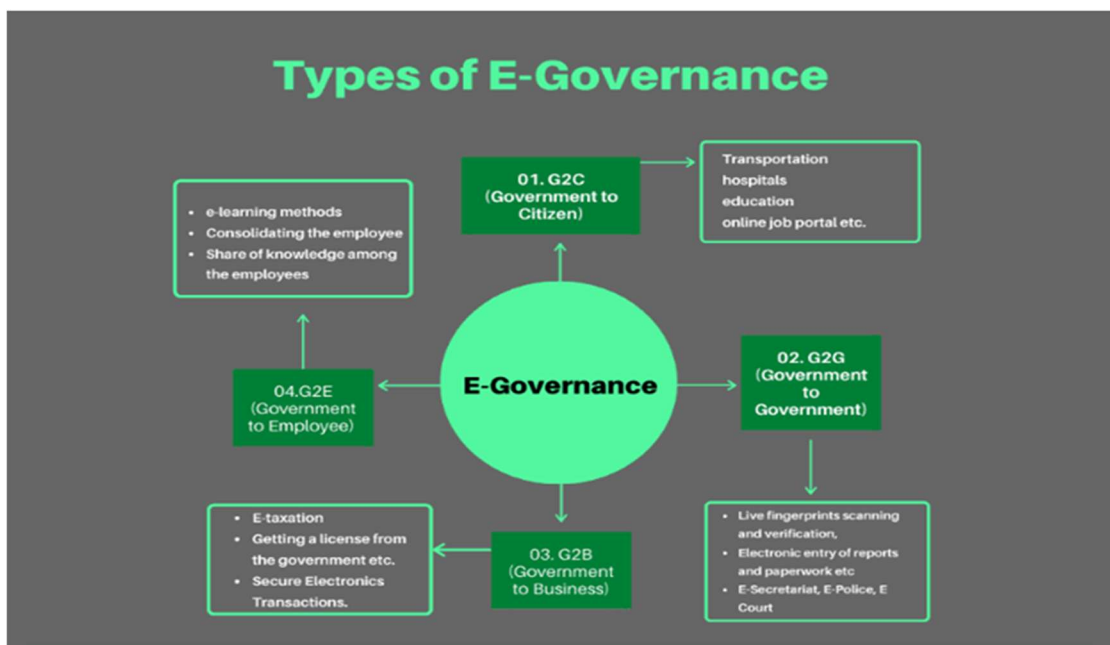
- Αξιοπιστία και ασφάλεια

Οι σχέσεις εμπιστοσύνης μεταξύ των πολιτών και των δημοσίων διοικήσεων αποτελούν ακρογωνιαίο λίθο για την αξιοποίηση των παρεχόμενων υπηρεσιών. Οι φορείς του δημόσιου τομέα που παρέχουν ψηφιακές δημόσιες υπηρεσίες θα πρέπει να σχεδιάζουν υποδομές και υπηρεσίες, ασφαλείς και αξιόπιστες, οι οποίες θα προστατεύουν τις πληροφορίες και τα δεδομένα που διακινούν ή με οποιονδήποτε τρόπο διαχειρίζονται. Πρόκειται για σημαντικές προϋποθέσεις για την ενίσχυση της εμπιστοσύνης και την υιοθέτηση των ψηφιακών υπηρεσιών.

#### 1.4. Κατηγορίες Ηλεκτρονικής Διακυβέρνησης

Οι εφαρμογές της ηλεκτρονικής διακυβέρνησης περιλαμβάνουν ένα ποικιλόμορφο φάσμα υπηρεσιών ωστόσο χαρτογραφώντας τις αλληλεπιδράσεις και τις σχέσεις μεταξύ των εμπλεκόμενων μερών, παρόχου και αποδέκτη, προκύπτουν τέσσερις κύριες κατηγορίες: κυβέρνηση προς πολίτη (G2C), κυβέρνηση προς επιχείρηση (G2B), κυβέρνηση προς κυβέρνηση (G2G) και κυβέρνηση προς υπάλληλο (G2E).

Οι υπηρεσίες Ηλεκτρονικής Διακυβέρνησης μπορούν να κατηγοριοποιηθούν και ως εξής:



Εικόνα 1 Τύποι Ηλεκτρονικής Διακυβέρνησης<sup>1</sup>

<sup>1</sup> <https://schoolofpoliticalscience.com/what-is-e-governance>

– Κυβέρνηση-προς-Πολίτες (Government to Citizen - G2C): Η κατηγοριοποίηση αυτή περιλαμβάνει όλες εκείνες τις διαδικασίες που αφορούν στις σχέσεις αλληλεπίδρασης μεταξύ των δημόσιων οργανισμών και των πολιτών με την πλειοψηφία των κρατικών υπηρεσιών να εμπίπτουν σε αυτήν την κατηγορία ηλεκτρονικής διακυβέρνησης. Κύριος στόχος είναι η εξυπηρέτηση των πολιτών η οποία επιτυγχάνεται διευκολύνοντας την πρόσβαση σε δημόσιες πληροφορίες και την αλληλεπίδρασή τους με την κυβέρνηση, αξιοποιώντας διαδικτυακούς ιστότοπους. Οι πολίτες αποκτούν άμεση πρόσβαση σε κρατικές πληροφορίες και υπηρεσίες από οπουδήποτε, ανά πάσα στιγμή, χρησιμοποιώντας πολλαπλούς διαύλους επικοινωνίας, μειώνοντας τον χρόνο αλλά και το κόστος που θα χρειάζονταν για την πραγματοποίηση συναλλαγής. Η συνεχής διεπαφή με τους πολίτες ενισχύει την λογοδοσία και βελτιώνει τις δημόσιες υπηρεσίες και ως εκ τούτου αυξάνει την συμμετοχή των πολιτών στις δημοκρατικές διαδικασίες και την εμπιστοσύνη στην κυβέρνηση. Παραδείγματα τέτοιων υπηρεσιών είναι η έκδοση πιστοποιητικών, η πληρωμή κρατικών τελών ή η αίτηση για απόκτηση αδειών (Alshehri & Drew, 2010).

– Κυβέρνηση-προς-Επιχειρήσεις (Government to Business - G2B): Στην κατηγορία αυτή συγκαταλέγονται οι υπηρεσίες των δημόσιων οργανισμών με τελικούς αποδέκτες τις ιδιωτικές επιχειρήσεις και αποτελούν συγκριτικά την δεύτερη κυριότερη κατηγορία ηλεκτρονικής διακυβέρνησης, εξασφαλίζοντας μεγιστοποιημένη αποτελεσματικότητα τόσο για τον κυβερνητικό όσο και για τον επιχειρηματικό τομέα. Σε αυτό το πλαίσιο εντάσσονται υπηρεσίες όπως η πρόσβαση σε τρέχουσες επιχειρηματικές πληροφορίες, νέους κανονισμούς, η λήψη εντύπων αίτησης, η υποβολή φόρων, η ανανέωση αδειών, η εγγραφή επιχειρήσεων, η απόκτηση αδειών κ.λπ. Ψηφιοποιώντας τις συναλλαγές του επιχειρηματικού τομέα με το κράτος, απλοποιούνται οι διοικητικές διαδικασίες, βελτιώνεται η ποιότητα και η αποτελεσματικότητα αφού περιορίζονται τα σχετικά κόστη και ο χρόνος για την επεξεργασία των αιτημάτων, δημιουργώντας ένα διαφανές επιχειρηματικό περιβάλλον.

– Κυβέρνηση-προς-Κυβέρνηση (Government to Government - G2G): Πρόκειται για τις διαδικασίες που αφορούν στις σχέσεις αλληλεπίδρασης μεταξύ των δημόσιων οργανισμών είτε οριζόντια μεταξύ υπηρεσιών είτε κάθετα σε διαφορετικά επίπεδα διακυβέρνησης. Οι διάφορες κυβερνητικές οντότητες μπορούν να επικοινωνούν διαδικτυακά αξιοποιώντας κοινές βάσεις δεδομένων, να μοιράζονται δεδομένα και πληροφορίες, βελτιώνοντας τον συντονισμό, την αποτελεσματικότητα και την αποδοτικότητα της δημόσιας διοίκησης.

– Κυβέρνηση-προς-εργαζόμενους (Government to Employees - G2E) Η κατηγορία αυτή περικλείει τις αλληλεπιδράσεις μεταξύ της κυβέρνησης και των υπαλλήλων της. Παρέχεται στους εργαζομένους η δυνατότητα να έχουν πρόσβαση μέσω διαδικτύου σε προσωποποιημένη πληροφόρηση όπως η μισθοδοσία, η υποβολή αίτησης για ετήσια άδεια κ.α. τους επιτρέπει δηλαδή να επικοινωνούν διαδικτυακά με την διοίκηση μέσω μιας εύκολης και γρήγορης φόρμας επικοινωνίας. Σκοπός αυτής της πολιτικής είναι να ενισχύσει την αποδοτικότητα, την παραγωγικότητα και την δέσμευση των υπαλλήλων παρέχοντας τους ψηφιακά εργαλεία φιλικά προς τον χρήστη για τον χειρισμό των υποθέσεων τους και την πρόσβαση σε σχετική πληροφόρηση. Η παροχή κατάρτισης και η ανάπτυξη των δεξιοτήτων του ανθρώπινου δυναμικού επιτυγχάνονται με τις προαναφερόμενες διαδικασίες.

## 1.5. Στάδια ηλεκτρονικής διακυβέρνησης

Σύμφωνα με έκθεση των Ηνωμένων Εθνών του 2002 σχετικά με το περιβάλλον ηλεκτρονικής διακυβέρνησης μιας Χώρας υφίστανται 5 στάδια τα οποία περιγράφουν την εξέλιξη και εφαρμογή της ηλεκτρονικής διακυβέρνησης από τις κυβερνήσεις και συγκεκριμένα:



Εικόνα 2 Στάδια Ηλεκτρονικής Διακυβέρνησης

## 1. Πληροφόρηση

Η παρουσία στο διαδίκτυο με κυβερνητικούς ιστότοπους είναι το πρώτο εξελικτικό στάδιο της ηλεκτρονικής διακυβέρνησης. Σε αυτή τη φάση, κάθε κρατικός φορέας παρέχει ξεχωριστά υπηρεσίες στους πολίτες μέσω του δικού του ιστότοπου λειτουργώντας επί της ουσίας ως «φυλλάδιο», υποδηλώνοντας ότι είναι το ηλεκτρονικό ισοδύναμο ενός έντυπου φυλλαδίου. Πρόκειται για μια παθητική παρουσίαση γενικών πληροφοριών, καθιστώντας την απλούστερη και λιγότερο δαπανηρή καθώς προσφέρει περιορισμένες επιλογές για τους πολίτες. Ένα τυπικό παράδειγμα είναι μια στατική ιστοσελίδα που παραθέτει συνοπτικές πληροφορίες σχετικά με μια υπηρεσία, όπως ώρες λειτουργίας, ταχυδρομική διεύθυνση ή/και αριθμούς τηλεφώνου, χωρίς να συμπεριλαμβάνει διαδραστικές δυνατότητες.

## 2. Απλή Διάδραση

Αυτό το στάδιο διακρίνεται από μια ενισχυμένη παρουσία στην οποία οι ιστότοποι των κυβερνητικών υπηρεσιών είναι δυναμικοί και οι πληροφορίες είναι ενημερωμένες. Επιτρέπει στους χρήστες να έχουν πρόσβαση σε πληθώρα πληροφοριών σε εξειδικευμένους ιστότοπους. Οι αλληλεπιδράσεις είναι σχετικά απλές και γενικά περιστρέφονται γύρω από την παροχή πληροφοριών με βελτιωμένες δυνατότητες, όπως η επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου ή οι ηλεκτρονικές φόρμες με δυνατότητα λήψης.

## 3. Αμφίδρομη Διάδραση

Αυτό το στάδιο διακρίνεται από διαδραστικές πύλες που επιτρέπουν στις πληροφορίες να ρέουν και προς τις δύο κατευθύνσεις, επιτρέποντας στους χρήστες να πραγματοποιούν αναζητήσεις σε εξειδικευμένες βάσεις δεδομένων, να αποθηκεύουν και να υποβάλλουν ηλεκτρονικά σχετικές φόρμες, να ανατροφοδοτούν με σχόλια ενώ κάνουν την εμφάνισή τους κωδικοί χρήσης και ασφαλείς συνδέσεις.

## 4. Ολοκληρωμένες Συναλλαγές

Σε αυτό το στάδιο, οι χρήστες μπορούν να εκτελούν ασφαλείς διαδικτυακές εργασίες και συναλλαγές με τους κρατικούς φορείς. Αυτές οι πρωτοβουλίες είναι πιο περίπλοκες από την απλή παροχή πληροφοριών και ενσωματώνουν τους τύπους δραστηριοτήτων που συνδέονται ευρέως με την ηλεκτρονική διακυβέρνηση, όπως ανανεώσεις αδειών, πληρωμή φόρων και τελών και υποβολή προσφορών για συμβάσεις προμηθειών. Το επίπεδο αλληλεπίδρασης σε

αυτό το στάδιο είναι υψηλότερο από το δεύτερο στάδιο ωστόσο οι δραστηριότητες εξακολουθούν να περιλαμβάνουν μια ροή πληροφοριών που είναι κυρίως μονόδρομη (είτε προς την κυβέρνηση είτε προς τον αποδέκτη, ανάλογα με τη δραστηριότητα).

## 5. Εξατομικευμένες Υπηρεσίες

Πρόκειται για το τελευταίο και πιο ολοκληρωμένο στάδιο ηλεκτρονικής διακυβέρνησης, στο οποίο οι κυβερνήσεις παρέχουν άμεση πρόσβαση σε όλες τις δημόσιες υπηρεσίες μέσω μιας ενιαίας ψηφιακής πύλης. Όλα τα είδη συναλλαγών που προσφέρονται από την κυβέρνηση είναι διαθέσιμα online χωρίς καμία οριοθέτηση μεταξύ των διαφόρων τμημάτων και υπηρεσιών.

Συμπερασματικά, η ηλεκτρονική διακυβέρνηση είναι ένας τρόπος για τις κυβερνήσεις να χρησιμοποιήσουν τις ΤΠΕ για να μεταμορφώσουν τις δομές, τις λειτουργίες και την κουλτούρα της κυβέρνησης. Η ανάπτυξη διαφόρων τύπων ηλεκτρονικής διακυβέρνησης αντικατοπτρίζει την ποικιλομορφία των αναγκών και των προτεραιοτήτων των χρηστών στις κυβερνητικές στρατηγικές. Η επιτυχής ανάπτυξη και εφαρμογή πρωτοβουλιών ηλεκτρονικής διακυβέρνησης εξαρτάται από διάφορους παράγοντες, συμπεριλαμβανομένου του εθνικού πλαισίου, των πολιτικών και θεσμικών παραγόντων, των κοινωνικοοικονομικών και πολιτιστικών παραγόντων και της τεχνικής υποδομής. Η ηλεκτρονική διακυβέρνηση έχει τη δυνατότητα να βελτιώσει την ποιότητα των υπηρεσιών, να ενισχύσει τις ευκαιρίες για δημοκρατική συμμετοχή και να υποστηρίξει τους στόχους λογοδοσίας και χρηστής διακυβέρνησης.

## 1.6. Οφέλη ηλεκτρονικής διακυβέρνησης

Η εφαρμογή της ηλεκτρονικής διακυβέρνησης αποτελεί έναν καθοριστικό παράγοντα μετασχηματισμού των δημόσιων φορέων, υπερβαίνοντας την στείρα χρήση της ηλεκτρονικής τεχνολογίας για την παροχή υπηρεσιών. Τα οφέλη από την χρήση της ηλεκτρονικής διακυβέρνησης γίνονται εμφανή τόσο εντός των φορέων διοίκησης όσο και στις σχέσεις τους με τους πολίτες και τις επιχειρήσεις, που είναι οι κύριοι αποδέκτες της. Αναφορικά με τις θετικές επιδράσεις της ηλεκτρονικής διακυβέρνησης στους κρατικούς φορείς και την εν γένει λειτουργία των κυβερνήσεων συγκαταλέγονται η ενίσχυση της διαφάνειας και ο περιορισμός της διαφθοράς, η μείωση του λειτουργικού κόστους για την παροχή υπηρεσιών και η αύξηση της παραγωγικότητας μέσω της μείωσης του απαιτούμενου χρόνου για την διεκπεραίωση των

υποθέσεων. Δημιουργούνται δηλαδή όλες εκείνες οι συνθήκες που εξασφαλίζουν την αύξηση της αποδοτικότητας και της αποτελεσματικότητας της δημόσιας διοίκησης.

Από την υιοθέτηση και ενσωμάτωση της ηλεκτρονικής διακυβέρνησης δεν επωφελείται μόνο η δημόσια διοίκηση αλλά και οι πολίτες καθώς πλέον εξασφαλίζεται μια σειρά από πλεονεκτήματα, που συνθέτουν μια βελτίωση στην ποιότητα των παρεχόμενων υπηρεσιών. Οι ηλεκτρονικές υπηρεσίες είναι προσβάσιμες χωρίς χρονικούς και γεωγραφικούς περιορισμούς, σε καθημερινή βάση, χωρίς να απαιτείται η αυτοπρόσωπη παρουσία των ενδιαφερόμενων στα καταστήματα των δημοσίων υπηρεσιών. Κατά αυτόν τον τρόπο επιτυγχάνεται εξοικονόμηση χρόνου και μείωση του κόστους συναλλαγής, αφού πλέον δεν είναι απαραίτητη η φυσική παρουσία τους. Επιπλέον, απλουστεύονται οι διαδικασίες και μειώνεται ο χρόνος διεκπεραίωσης των υποθέσεων, καθώς χρησιμοποιούνται προσυμπληρωμένα ηλεκτρονικά έντυπα ενώ με τις ενιαίες βάσεις δεδομένων οι δημόσιοι φορείς αντλούν τα απαραίτητα στοιχεία, απαλλάσσοντας τον συναλλασσόμενο από την σχετική υποχρέωση. Ο ίδιος ο πολίτης αποκτά πληρέστερη πρόσβαση και μπορεί να ασκεί έλεγχο των διαδικασιών συναλλαγής.

Η ηλεκτρονική διακυβέρνηση ενδυναμώνει τους δημοκρατικούς θεσμούς ενθαρρύνοντας την συμμετοχή των πολιτών στις δημοκρατικές διαδικασίες. Παρέχεται η δυνατότητα συμμετοχής στην ηλεκτρονική διαβούλευση που προηγείται της ψήφισης νόμων, εξασφαλίζεται η ουσιαστική ενημέρωση από την μελέτη επίσημων εγγράφων, προϋπολογισμών και πρακτικών συνεδριάσεων ομάδων ή έργου επιτροπών και εκφράζεται η προτίμηση μια επιλογής έναντι κάποιας εναλλακτικής με συμμετοχή σε online ψηφοφορίες ή έρευνες.

## **1.7. Κίνδυνοι εφαρμογής ηλεκτρονικής διακυβέρνησης**

Παρόλο που υπάρχουν εξαιρετικής σημασίας οφέλη που προκύπτουν από την εφαρμογή της ΗΔ, υπάρχουν επίσης διάφοροι παράγοντες που περιορίζουν την καθολική αποδοχή της (Παπαζήσης, 2008). Κατά αρχάς είναι γεγονός πως η εφαρμογή των ΤΠΕ επιβάλλει την διάθεση αυξημένων πόρων ένεκα του υψηλού κόστους εξοπλισμού. Οι οικονομικοί πόροι που πρέπει να διατεθούν για την προμήθεια του αναγκαίου εξοπλισμού σε αρκετές περιπτώσεις είναι ανέφικτοι. Ένας επιπλέον ουσιαστικός παράγοντας που δημιουργεί δυσχέρειες στην εφαρμογή της ηλεκτρονικής διακυβέρνησης είναι η ελλιπής εκπαίδευση του προσωπικού των δημοσίων υπηρεσιών. Οι εγγενείς αδυναμίες αυτές που απαντώνται τόσο στους δημόσιους

υπαλλήλους όσο και στους πολίτες εμποδίζουν την αποτελεσματική εφαρμογή της ηλεκτρονικής διακυβέρνησης (Abramson, M.A. & Means G, 2001).

Ωστόσο, η σημαντικότερη δυσκολία που ανακύπτει είναι ο κίνδυνος για την προστασία των δεδομένων προσωπικού χαρακτήρα. Τα περιστατικά αθέμιτης πρόσβασης σε δεδομένα προσωπικού χαρακτήρα συχνά δημιουργούν στους πολίτες αίσθημα ανασφάλειας όσον αφορά την χρήση διαδικτυακών υπηρεσιών. Ο τρόπος επεξεργασίας και διαχείρισης των δεδομένων προσωπικού χαρακτήρα διέπεται από ένα σύνολο κανόνων-αρχών, σύμφωνα με την παράγραφο 5 του Ευρωπαϊκού Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27<sup>ης</sup> Απριλίου 2016:

- Αρχή της νομιμότητας<sup>2</sup>.
- Αρχή της αντικειμενικότητας.
- Αρχή διαφάνειας.
- Αρχή του περιορισμού του σκοπού<sup>3</sup>.
- Αρχή της ελαχιστοποίησης των δεδομένων<sup>4</sup>.
- Αρχή της ακρίβειας των δεδομένων<sup>5</sup>.
- Αρχή του περιορισμού της αποθήκευσης.
- Αρχή της ασφάλειας των δεδομένων.
- Αρχή της λογοδοσίας<sup>6</sup>.

## 1.8. Σκοπός

Κατά την τελευταία τριετία η χώρα μας έχει χρησιμοποιήσει σε ικανοποιητικό βαθμό της ΤΠΕ για να περιορίσει την γραφειοκρατία που προκαλείται από υπηρεσίες κατηγορίας G2C

---

<sup>2</sup> Επεξεργασία με σύννομο, δίκαιο και διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («Νομιμότητα, αντικειμενικότητα και διαφάνεια»)

<sup>3</sup> Συλλέγονται για συγκεκριμένους, ρητούς και νόμιμους σκοπούς και δεν θα υποβάλλονται πλέον σε επεξεργασία κατά τρόπο ασυμβίβαστο με αυτούς τους σκοπούς. Οποιαδήποτε περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς δεν θεωρείται ασυμβίβαστη με τον αρχικό σκοπό σύμφωνα με το άρθρο 89 παράγραφος 1 («Περιορισμός του σκοπού»).

<sup>4</sup> Είναι επαρκής, συναφής και περιορίζεται σε ό,τι είναι απαραίτητο για τους σκοπούς της επεξεργασίας («ελαχιστοποίηση δεδομένων»).

<sup>5</sup> Είναι ακριβής και ενημερωμένη όπου είναι απαραίτητο. Πρέπει να λάβετε όλα τα εύλογα μέτρα για να διαγράψετε ή να διορθώσετε αμέσως τυχόν προσωπικά δεδομένα που είναι ανακριβή σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ακρίβεια»).

<sup>6</sup> Ο Υπεύθυνος επεξεργασίας είναι υπεύθυνος για τη συμμόρφωση με τη ρήτρα 1 («λογοδοσία») και πρέπει να είναι σε θέση να το αποδείξει.

(κυβέρνηση προς πολίτη) κυρίως σε συναλλαγές του τύπου front-office. Απλές αλλά πολύ αποτελεσματικές διαδικτυακές εφαρμογές έχουν ψηφιοποιήσει τις υπηρεσίες G2C που απαιτούσαν αυτοπρόσωπη παρουσία, αποδείξεις γνησιότητας, κατάθεση εγγράφων κ.λπ. Συμβάντα όπως η υγειονομική κρίση covid-19 και οι καταστροφές από ακραία φυσικά φαινόμενα που υπαγόρευαν την άμεση παροχή ενισχύσεων σε πολίτες και επιχειρήσεις και έκδοση ηλεκτρονικών εγγράφων επιτάχυναν τις προαναφερόμενες διαδικασίες.

Τέτοιες εφαρμογές δεν πραγματοποιούν ριζικές τομές στις γραφειοκρατικές διαδικασίες του δημόσιου τομέα και παρά την πρόοδο που συντελέστηκε οι φορείς της δημόσιας διοίκησης εξακολουθούν να χαρακτηρίζονται από χρονοβόρες, δαπανηρές, και απρόσωπες υπηρεσίες.

Τα στελέχη της ΕΛ.ΑΣ. και οι πολίτες αντιμετωπίζουν πλήθος καθημερινών δυσκολιών και δυσλειτουργιών, με αποτέλεσμα να υπάρχει μειωμένη εμπιστοσύνη για τις παραγόμενες υπηρεσίες και ιδιαίτερα για τις ηλεκτρονικές, αφού στις περισσότερες περιπτώσεις δεν είναι ολοκληρωμένες και απαιτούν τελικά επιπλέον αυτοπρόσωπη παρουσία των πολιτών.

Αυτή η εργασία επικεντρώνεται σε καινοτόμες εφαρμογές Ηλεκτρονικής Διακυβέρνησης, [G2C (κυβέρνηση προς πολίτη), G2G (κυβέρνηση προς κυβέρνηση) και G2E (κυβέρνηση προς εργαζομένους)] οι οποίες ενισχύουν το επίπεδο ασφάλειας και διευκολύνουν την ενημέρωση των πολιτών.

## **ΚΕΦΑΛΑΙΟ 2: Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης στην Ελληνική Αστυνομία**

### **2.1. Police on Line**

Το 1993 άρχισε η δημιουργία ενός δικτύου πληροφορικής που περιλάμβανε τρεις κεντρικούς υπολογιστές και τριακόσιους προσωπικούς υπολογιστές στις κεντρικές λειτουργίες του Σώματος. Το 2008, ολοκληρώθηκε το έργο «Συμμετοχή της Ελληνικής Αστυνομίας στον εκσυγχρονισμό της Δημόσιας Διοίκησης μέσω της Πληροφορικής (Police On Line)», το οποίο υλοποιήθηκε στο πλαίσιο του Τρίτου Κοινοτικού Πλαισίου Στήριξης και συγχρηματοδοτήθηκε από την Ευρωπαϊκή Ένωση. Το έργο αυτό διευκόλυνε τον εκσυγχρονισμό της Ελληνικής Αστυνομίας με τον εξοπλισμό όλων των υπηρεσιών με υλικό και την ανάπτυξη εφαρμογών λογισμικού για την ενίσχυση της εξυπηρέτησης του πολίτη, τη μείωση της γραφειοκρατίας και τη βελτίωση της αποτελεσματικότητας και της παραγωγικότητας των επιχειρήσεων της ΕΛ.ΑΣ. (Ελληνική Αστυνομία, 2009). Η εφαρμογή Police on Line (P.O.L.) περιλαμβάνει το «Ηλεκτρονικό ταχυδρομείο», το «Webmail Police» και πολλές επιμέρους εφαρμογές που λειτουργούν ως βάσεις δεδομένων (π.χ. Εφαρμογή Δαπανών, Ταυτότητες Ελλήνων Πολιτών κ.λ.π.) (Ελληνική Αστυνομία, 2009).

#### **2.1.1. Ηλεκτρονική Αλληλογραφία**

Με την Ηλεκτρονική Αλληλογραφία δίνονται οι δυνατότητες:

- Προετοιμασία διοικητικών εγγράφων. Προετοιμασία διοικητικών εγγράφων με χρήση υποδειγμάτων σύμφωνα με τους ισχύοντες νομικούς κανονισμούς.
- Εισαγωγή και επικόλληση εγγράφων. Χρήση συσκευών εισόδου (π.χ. σαρωτή) για την εισαγωγή εγγράφων που δεν έχουν δημιουργηθεί εντός της εφαρμογής και επικόλλησή τους για μετέπειτα διαβίβαση και χρήση.
- Δρομολόγηση εγγράφων. Διαβίβαση εγγράφων σε άλλες υπηρεσίες ή ιεραρχικά επίπεδα για προώθηση εγγράφων.

- Αρχαιοθέτηση εγγράφων. Μετά την ολοκλήρωση της εργασίας για την οποία δημιουργήθηκε το έγγραφο, αρχαιοθετείται.
- Ανάκτηση εγγράφου. Ένα έγγραφο μπορεί να εντοπιστεί με βάση τον αριθμό πρωτοκόλλου του ή μέσω λεπτομερούς αναζήτησης, όπως με βάση την ημερομηνία, τις πληροφορίες αποστολέα ή παραλήπτη, το θέμα, τη λέξη-κλειδί ή τον αριθμό θέματος.
- Ηλεκτρονική υπογραφή εγγράφου. Για σκοπούς δρομολόγησης, κάθε έγγραφο πρέπει να περιλαμβάνει τις ψηφιακές υπογραφές τόσο του εφευρέτη όσο και του ιεραρχικά προϊσταμένου του, όπως ορίζει το ΠΔ 25/2014.

Όλα τα γραφειοκρατικά καθήκοντα ενοποιήθηκαν στην «Ηλεκτρονική Αλληλογραφία», η οποία, μέσω της ψηφιοποίησης, μείωσε τον χρόνο διεκπεραίωσης και την απόσταση εξυπηρέτησης.

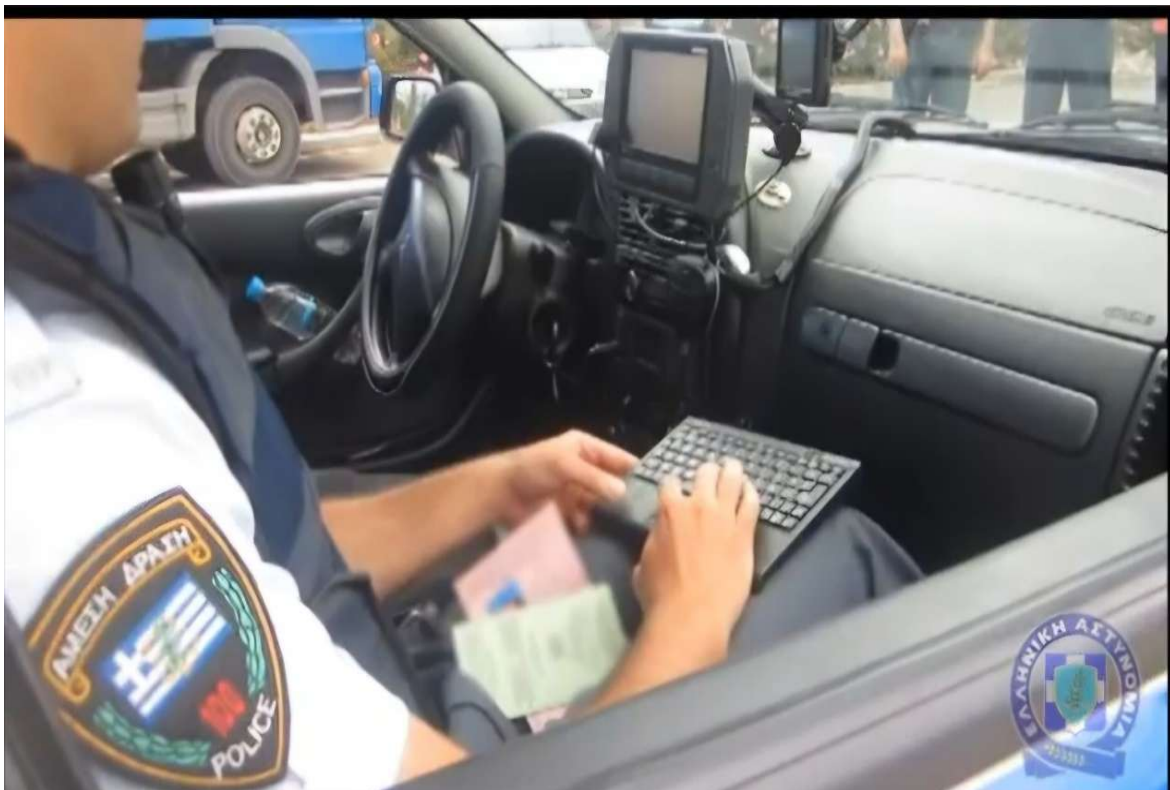
### **2.1.2. CAR-PC**

Τα περιπολικά οχήματα είναι εξοπλισμένα με υπολογιστές οχημάτων (Car-PC), οι οποίοι είναι απευθείας συνδεδεμένα με το σύστημα Police on Line και προσφέρουν άμεσα και ανά πάσα στιγμή στα πληρώματα, πληροφορίες σχετικές για τα υπό εξέταση άτομα και οχήματα. Έτσι δεν χρειάζεται να πραγματοποιούν όλες τις αναζητήσεις μέσω ασυρμάτου και αυτό να γίνεται μόνο σε περίπτωση που είναι αδύνατη η χρήση του. Ο αστυνομικός που βρίσκεται στο όχημα μπορεί να επαληθεύσει ανεξάρτητα τα στοιχεία των οχημάτων και των ατόμων που ελέγχονται. Έτσι, ενημερώνεται αμέσως για τυχόν διωκτικά έγγραφα που αφορούν το αντικείμενο ή το υποκείμενο του ελέγχου, επιτρέποντάς του να εκπληρώσει αποτελεσματικά το ρόλο του για την προστασία των πολιτών.

Η εφαρμογή Car PC δύναται να χρησιμοποιηθεί από όλους τους αστυνομικούς, ενώ οι υπηρεσίες που πραγματοποιούν επιτόπιους ελέγχους στο πεδίο την αξιοποιούν καθημερινά, μεταξύ των οποίων συμπεριλαμβάνονται τα πληρώματα των οχημάτων της Άμεσης Δράσης, περιπολίες ασφάλειας, σταθμοί Τροχαίας και εποχούμενες περιπολίες των Αστυνομικών Τμημάτων. Η εφαρμογή αυτή παρέχει πρόσβαση σε σημαντικό αριθμό βασικών πληροφοριών, όπως :

- εάν τα έγγραφα ενός Έλληνα πολίτη (ταυτότητα, διαβατήριο, άδεια οδήγησης, έγγραφο ιδιοκτήτη ζώων συντροφιάς) είναι σε ισχύ.

- εάν τα έγγραφα ενός αλλοδαπού πολίτη, που έχουν εκδοθεί από τις Ελληνικές Αρχές (ειδικό δελτίο ταυτότητας ομογενούς, δελτία αιτούντων διεθνούς προστασίας, άδειες παραμονής) είναι σε ισχύ.
- εάν η πινακίδα κυκλοφορίας ενός οχήματος εγείρει ανησυχίες (κλοπή, πλαστογραφία, απουσία ασφαλιστικής κάλυψης),
- εάν ένα άτομο απασχολεί τις Αρχές Επιβολής του Νόμου σε ευρωπαϊκό ή διεθνές επίπεδο,
- εάν διαθέτει άδεια κατοχής κυνηγετικού όπλου σε ισχύ ή μη,
- εάν κατέχει νόμιμα ιδιωτικό όπλο.
- εάν του έχει απαγορευτεί η είσοδος ή η έξοδος από το κράτος,
- εάν υπάρχει εν εξελίξει δικαστική διαδικασία κατά του εν λόγω ατόμου,
- εάν το microchip ζώου συντροφιάς είναι έγκυρο.



*Εικόνα 3 Επίδειξη συστήματος CAR PC*

## 2.2. Ψηφιακές υπηρεσίες GOV.GR

Η Ελληνική Αστυνομία προσφέρει διάφορες ψηφιακές υπηρεσίες στους κατοίκους και τις επιχειρήσεις μέσω της ψηφιακής πύλης GOV.GR. Κάθε χρήστης αποστέλλεται στον ιστότοπο [www.astynomia.gr](http://www.astynomia.gr) και, αφού εισάγει τα προσωπικά του διαπιστευτήρια για την ενιαία ψηφιακή πύλη της δημόσιας διοίκησης, μπορεί να υποβάλει αίτημα προς τις αρμόδιες αστυνομικές υπηρεσίες, το οποίο στη συνέχεια προωθείται στο γραμματοκιβώτιο της αστυνομικής υπηρεσίας. Ακολούθως, το εξειδικευμένο προσωπικό της Ελληνικής Αστυνομίας, έχοντας πρόσβαση στο σύστημα με τη χρήση κωδικών δημόσιας διοίκησης, χειρίζεται και επεξεργάζεται το αίτημα, ενημερώνοντας στη συνέχεια τον πολίτη. Οι ψηφιακές υπηρεσίες που είναι μέχρι σήμερα διαθέσιμες είναι:

- Άδεια άσκησης επαγγέλματος κατασκευαστών / επισκευαστών κλειδαριών,
- Άδεια άσκησης επαγγέλματος παλαιοπωλών, ενεχυροδανειστών,
- Άδεια εργασίας προσωπικού για ιδιωτικές υπηρεσίες ασφάλειας,
- Άδεια κατοχής κυνηγετικού όπλου,
- Άδεια οπλοφορίας,
- Αντίγραφο από το Βιβλίο Αδικημάτων και Συμβάντων,
- Αντίγραφο δελτίου οδικού τροχαίου ατυχήματος υλικών ζημιών,
- Αντίγραφο ημερήσιου δελτίου οχήματος,
- Αντίγραφο πράξης βεβαίωσης παράβασης,
- Αντίγραφο τηλεφωνικής κλήσης στην Άμεση Δράση,
- Αντίγραφο φακέλου απόστρατων αστυνομικών,
- Βεβαίωση δακτυλοσκόπησης,
- Βεβαίωση εγγραφής αλλοδαπών για λόγους σπουδών,
- Γνωστοποίηση καταχώρισης στο σύστημα πληροφοριών ΣΕΝΓΚΕΝ,
- Δηλώσεις κλοπής / ανεύρεσης κλαπέντων οχημάτων,
- Εθελοντική προεγγραφή ηλεκτρονικής αναγνώρισης,
- Ειδικό ταξιδιωτικό έγγραφο (T.D.V.) της Σύμβασης της Γενεύης του 1951,
- Έκδοση / ανανέωση άδειας παραμονής αλλοδαπού σε καθεστώς διεθνούς προστασίας,
- Έκδοση / ανανέωση προσωρινής άδειας εισόδου στη χώρα για λόγους έκτακτης ανάγκης,
- Ένσταση για πράξη βεβαίωσης παράβασης,
- Καταγγελία για οικονομικά εγκλήματα,

- Καταστροφή στοιχείων σημάνσεως,
- Προέλεγχο επιβατών κρουαζιερόπλοιων για την είσοδό τους στην Ελλάδα,

#### Άδειες κυκλοφορίας:

- Ανανέωση άδειας κυκλοφορίας μοτοποδηλάτου,
- Πρώτη άδεια κυκλοφορίας μοτοποδηλάτου,

#### Δελτίο ταυτότητας Ελλήνων πολιτών:

- Δήλωση απώλειας δελτίου ταυτότητας Ελλήνων πολιτών,
- Ραντεβού για την έκδοση δελτίου ταυτότητας Ελλήνων πολιτών,

#### Εγκλήματα κυβερνοχώρου:

- Καταγγελία για αδικήματα τελούμενα σε βάρος ανηλίκων μέσω διαδικτύου,
- Καταγγελία σχετικά με τα οικονομικά κυβερνοεγκλήματα στα οποία εμπλέκονται ηλεκτρονικά/ψηφιακά νομίσματα,
- Καταγγελία για παραβίαση του απορρήτου των ηλεκτρονικών και τηλεφωνικών επικοινωνιών,
- Καταγγελία για παράνομη διακίνηση οπτικοακουστικών έργων μέσω διαδικτύου,
- Καταγγελία για παράνομη πρόσβαση σε ηλεκτρονικό υπολογιστή,
- Καταγγελία για περιπτώσεις απάτης με υπολογιστή

#### Ομογενείς:

- Άδεια Διαμονής Ενιαίου Τύπου σε ομογενείς από Τουρκία,
- Ειδικό Δελτίο Ταυτότητας Ομογενούς (ΕΔΤΟ) από Αλβανία,
- Ειδικό Δελτίο Ταυτότητας Ομογενούς (ΕΔΤΟ) από Τουρκία,
- Ειδικό Δελτίο Ταυτότητας Ομογενούς (ΕΔΤΟ) από χώρες της τ. ΕΣΣΔ,
- Πολίτες κράτους μέλους της Ε.Ε.,
- Βεβαίωση εγγραφής μελών οικογένειας πολίτη κράτους μέλους της Ε.Ε.,
- Βεβαίωση εγγραφής πολιτών κράτους μέλους της Ε.Ε. για λοιπούς λόγους,
- Πιστοποίηση μόνιμης διαμονής πολίτη κράτους μέλους της Ε.Ε.,

#### Πολίτες τρίτων χωρών:

- Παράταση χρόνου βραχείας διαμονής πολιτών τρίτης χώρας,

Η διαδικτυακή πύλη gov.gr αποτελεί σημαντικό πόρο για τους πολίτες, προσφέροντας ένα σημαντικό φάσμα υπηρεσιών της Ελληνικής Αστυνομίας σε ασφαλή και ομοιόμορφη ψηφιακή μορφή. Οι υπηρεσίες βελτιώνονται και επικαιροποιούνται συνεχώς με τη συνεργασία όλων των

κυβερνητικών φορέων, ενώ ταυτόχρονα επιτρέπουν στους πολίτες να παρέχουν ανατροφοδότηση για τον ανασχεδιασμό και τη βελτίωση της όλης διαδικασίας. Επί του παρόντος, διάφορες υπηρεσίες προσφέρονται μέσω ανακατεύθυνσης από το gov.gr σε προϋπάρχουσες δομές και συστήματα ωστόσο, ο μακροπρόθεσμος στόχος είναι η ανακατασκευή ολόκληρου του πλαισίου ώστε να παρέχεται απευθείας από το gov.gr μόλις ολοκληρωθεί πλήρως και τεθεί σε λειτουργία (Gov.gr 2025).

Ορισμένα σημαντικά ψηφιακά έργα που βρίσκονται σε εξέλιξη και αναμένεται να ολοκληρωθούν το επόμενο χρονικό διάστημα και θα συνδράμουν την Ελληνική Αστυνομία στην διαχείριση των ανθρωπίνων πόρων της με ψηφιακό τρόπο είναι οι εξής:

- Νέες ψηφιακές ταυτότητες

Μια σημαντική πρωτοβουλία που αποσκοπεί στη βελτίωση της καθημερινής ζωής των κατοίκων είναι η έκδοση ψηφιακών δελτίων ταυτότητας για σύγχρονους σκοπούς ταυτοποίησης. Η αρχική εφαρμογή θα αφορά την πιστοποίηση της ταυτότητας, ενώ στη συνέχεια θα διευκολύνει την πρόσβαση σε ψηφιακές υπηρεσίες με αυξημένη ασφάλεια.

- Κεντρικό Σύστημα Διαχείρισης Ανθρώπινου Δυναμικού

Μία από τις πρωτοβουλίες που πρόκειται να εκτελεστούν στον ελληνικό δημόσιο τομέα, η οποία θα αφορά και την Ελληνική Αστυνομία, είναι η κεντρική διαχείριση του ανθρώπινου δυναμικού. Το σύστημα αυτό θα επιβλέπει όλες τις διαδικασίες από τον διορισμό ενός ατόμου στο δημόσιο μέχρι τη συνταξιοδότησή του. Θα διαφυλάσσει όλα τα προσωπικά και υπηρεσιακά δεδομένα και θα τα παρέχει στους κατάλληλους φορείς για την αντιμετώπιση συγκεκριμένων απαιτήσεων, τηρώντας παράλληλα αυστηρά πρότυπα ασφαλείας και τηρώντας όλες τις αρχές της ορθής επεξεργασίας (ΥΠ.ΕΣ. 2023).

### **2.3. Smart Policing**

Κατόπιν έγκρισης χρηματοδότησης της Δράσης «Προμήθεια Συστημάτων για Έξυπνη Αστυνόμευση (Smart Policing)» από το Εθνικό Πρόγραμμα του Ευρωπαϊκού Ταμείου Εσωτερικής Ασφάλειας / Τομέας Αστυνομικής Συνεργασίας 2014-2020, διενεργήθηκε ανοιχτός διεθνής διαγωνισμός ανάθεσης προμήθειας και η Ελληνική Αστυνομία προέβη στην σύναψη σύμβασης με την εταιρεία «Intracom Telecom SA», κατά το πρώτο εξάμηνο του 2019. Την 13/09/2021 πραγματοποιήθηκε η οριστική παραλαβή του έργου από την Επιτροπή Παρακολούθησης και Παραλαβής (ΕΠΠΕ).

Το πρόγραμμα αυτό παρέχει στην αστυνομία έξυπνες συσκευές εξοπλισμένες με λογισμικό για τη σάρωση πινακίδων κυκλοφορίας οχημάτων, την συλλογή δακτυλικών αποτυπωμάτων και τη λήψη εικόνων προσώπου. Τα βιομετρικά δεδομένα των ατόμων μπορούν να συγκριθούν άμεσα με πληροφορίες που είναι ήδη αποθηκευμένες σε 20 βάσεις δεδομένων που διατηρούνται από εθνικούς και διεθνείς φορείς. Τουλάχιστον μία από τις προαναφερθείσες βάσεις δεδομένων και μεθόδους είναι ικανή να συλλέγει σημαντικά βιομετρικά δεδομένα σε δημόσιους χώρους. Οι τεχνικές προδιαγραφές αναφέρουν ότι το σύστημα θα καταστρέφει αμέσως τις σαρώσεις δακτυλικών αποτυπωμάτων χωρίς ταύτιση, ενώ θα διατηρεί τις φωτογραφίες για διάρκεια επτά ημερών. Εάν το σύστημα αναγνωρίσει ένα άτομο από δακτυλικά αποτυπώματα, φωτογραφίες ή σαρώσεις προσώπου, τα δεδομένα θα διατηρούνται επ' αόριστον.

Η πρωτοβουλία «Smart Policing» δίνει έμφαση στην παροχή σύγχρονου κινητού ηλεκτρονικού εξοπλισμού στην Ελληνική Αστυνομία, που θα χρησιμεύσει για την πρόληψη και καταστολή διαφόρων μορφών εγκληματικότητας. Οι ηλεκτρονικές συσκευές συνδέονται με τις τρέχουσες εθνικές και ευρωπαϊκές βάσεις δεδομένων και μπορούν να λαμβάνουν βιομετρικές πληροφορίες, συμπεριλαμβανομένων των αριθμών πινακίδων κυκλοφορίας και των δεδομένων τεκμηρίωσης. Αυτό επιτρέπει στην Ελληνική Αστυνομία να διεξάγει ταχείες και ασφαλείς έρευνες και ταυτοποιήσεις ατόμων, οχημάτων και άλλων αντικειμένων. Επιπλέον, οι συσκευές διευκολύνουν τη μετάδοση δεδομένων μεταξύ των χρηστών και παρέχουν μια πλατφόρμα για την τεκμηρίωση περιστατικών.

Η ασφάλεια των συσκευών διασφαλίζεται από μια εξειδικευμένη πλατφόρμα για την απομακρυσμένη διαχείριση των κινητών συσκευών, η οποία ενσωματώνει λειτουργίες για την κρυπτογράφηση δεδομένων και την εποπτεία των δικαιωμάτων πρόσβασης εφαρμογών. Η Ελληνική Αστυνομία συμβάλλει καθοριστικά στην προσπάθεια αυτή, δίνοντας έμφαση στην οργάνωση και τον συντονισμό της τεχνολογίας. Στόχος της Ελληνικής Αστυνομίας είναι η ενίσχυση των επιχειρησιακών δυνατοτήτων της και η παροχή εξαιρετικών υπηρεσιών ασφάλειας, τηρώντας παράλληλα τη νομιμότητα, τη διαφάνεια και το σεβασμό των ατομικών δικαιωμάτων. Η ενσωμάτωση έξυπνων συσκευών στις λειτουργίες της Ελληνικής Αστυνομίας θα βελτιώσει την αποτελεσματικότητα των μοντέλων διαχείρισής της, οχυρώνοντας έτσι τις υπηρεσίες της. Επιπλέον, η συλλογή δεδομένων καθίσταται πιο ακριβής και σκόπιμη, ιδίως κατά τη διάρκεια των συνήθων και ολοκληρωμένων αξιολογήσεων. Έτσι, η αποτελεσματική αξιοποίηση των δεδομένων βοηθά στην πρόληψη, τον εντοπισμό και την καταστολή του

σοβαρού, επικίνδυνου και οργανωμένου εγκλήματος. Αυτό επιτρέπει την άμεση ανίχνευση και ταυτοποίηση ύποπτων οχημάτων, ατόμων ή αντικειμένων που σχετίζονται με διάφορες εγκληματικές δραστηριότητες (Opengon , 2017).

Η πρωτοβουλία για την έξυπνη αστυνόμευση έδωσε στην Ελληνική Αστυνομία τη δυνατότητα να χρησιμοποιεί αποτελεσματικά τις έξυπνες κινητές συσκευές για την αξιολόγηση περιστατικών και εγκλημάτων σε πραγματικό χρόνο, καθώς και για την ανεύρεση ατόμων, αυτοκινήτων και αντικειμένων. Η πρόσβαση σε πολλές βάσεις δεδομένων επέτρεψε την παρακολούθηση υπηκόων τρίτων χωρών που παραβίασαν τη νόμιμη διάρκεια παραμονής στη χώρα. Το έργο ενισχύει την εθνική ασφάλεια, προς όφελος των Ελλήνων πολιτών, της Ευρωπαϊκής Κοινότητας και των υπηκόων τρίτων χωρών.

Η οδηγία 2016/680 της ΕΕ, η οποία αναφέρεται ως οδηγία για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης ή ως οδηγία για την επιβολή του νόμου (LED), είναι νομοθεσία ανάλογη με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR), η οποία διέπει την επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς επιβολής του νόμου εντός του πλαισίου της ΕΕ για την προστασία των δεδομένων και της ιδιωτικής ζωής. Το άρθρο 8 της οδηγίας ορίζει ότι τα δεδομένα προσωπικού χαρακτήρα συλλέγονται και τυγχάνουν νόμιμης επεξεργασίας. Τα κράτη μέλη υποχρεούνται να νομοθετούν σχετικά με τη συλλογή και την επεξεργασία των δεδομένων, ορίζοντας «τους σκοπούς της επεξεργασίας, τα προς επεξεργασία δεδομένα προσωπικού χαρακτήρα και τους στόχους της επεξεργασίας» (Τσιρώνης, 2022).

Στόχος του έργου είναι η ενσωμάτωση σύγχρονων τεχνολογιών έξυπνων φορητών συσκευών σε πεζές και επιτόπιες περιπολίες, παρέχοντας λύσεις για την ταυτοποίηση και την επαλήθευση των ατόμων που υπόκεινται σε επιτόπιο έλεγχο, ενισχύοντας έτσι το αίσθημα ασφάλειας και μειώνοντας τον κίνδυνο διαφυγής των παραβατών. Η πρωτοβουλία διευκολύνει την αποτελεσματική επιβολή του νόμου με την άμεση και ασφαλή ταυτοποίηση ατόμων, οχημάτων και αντικειμένων. Στο πλαίσιο αυτό, για την ενίσχυση της αποτελεσματικότητας των αστυνομικών αντιδράσεων στο πεδίο ή κατά τη διάρκεια επιτόπιων ελέγχων, έχει αποκτηθεί σύγχρονος εξοπλισμός, βοηθώντας σημαντικά στη διενέργεια ελέγχων «περιστατικών» για την ταυτοποίηση ατόμων, οχημάτων και αντικειμένων σε πραγματικό χρόνο. Ταυτόχρονα, η προσέγγιση αυτή έχει ενισχύσει την ασφάλεια των αστυνομικών, έχει μειώσει σημαντικά την αναπόφευκτη ταλαιπωρία των κατοίκων και έχει οδηγήσει στην εξοικονόμηση ανθρώπινων και υλικών πόρων, καθώς και στην αποδοτικότητα του χρόνου.

Συγκεκριμένα, λαμβάνοντας υπόψη την αυξημένη ενσωμάτωση των αστυνομικών με έξυπνες κινητές συσκευές, την ικανότητά τους στην αξιοποίηση των νέων τεχνολογιών και την πρόοδο της κεντρικής υποδομής της Ελληνικής Αστυνομίας, η ενίσχυση των παρεχόμενων υπηρεσιών είναι προφανής. Το έργο επικεντρώθηκε στην παροχή σύγχρονων φορητών ηλεκτρονικών συσκευών που χαρακτηρίζονται ως «έξυπνα κινητά τηλέφωνα», τα οποία χρησιμοποιούν μια ενιαία εφαρμογή/διεπαφή για την αναζήτηση σε υπάρχουσες βάσεις δεδομένων (εθνικές και ευρωπαϊκές) και την απόκτηση βιομετρικών χαρακτηριστικών (μέσω σάρωσης), αριθμών πινακίδων κυκλοφορίας και δεδομένων τεκμηρίωσης, διευκολύνοντας έτσι την ταχεία και ασφαλή ταυτοποίηση οχημάτων, ατόμων και αντικειμένων. Το σύστημα διευκολύνει τη μετάδοση δεδομένων, συμπεριλαμβανομένης της μεταφοράς αρχείων και των τηλεφωνικών κλήσεων μεταξύ των χρηστών, και ενσωματώνει μια εφαρμογή για την τεκμηρίωση «περιστατικών ελέγχου» εντός της διεπαφής της συσκευής, ενισχύοντας έτσι την επιχειρησιακή επισκόπηση σε πραγματικό χρόνο για την κεντρική και περιφερειακή διοίκηση.

Το έργο περιλαμβάνει τις εξής, κατά κύριο λόγο, δυνατότητες:

#### 1. Προμήθεια 1000 συσκευών τύπου Smartphone.

Στο πλαίσιο του έργου, χορηγήθηκαν συνολικά 1000 συσκευές smartphone, μαζί με προεγκατεστημένες εφαρμογές και λογισμικό που αναπτύχθηκε στο πλαίσιο της πρωτοβουλίας. Επιπλέον, οι συσκευές διαθέτουν τη δυνατότητα να «φιλοξενούν» όλες τις τρέχουσες εφαρμογές της Ελληνικής Αστυνομίας, επιτρέποντας τη λειτουργία σε κινητό περιβάλλον. Μετά από διαβουλεύσεις προκρίθηκε η επιλογή συσκευών smartphone μάρκας Samsung S10e dual sim πιο πρόσφατης κυκλοφορίας. Όλες οι συσκευές παραδόθηκαν με τα απαραίτητα εξαρτήματα για άμεση λειτουργική χρήση.

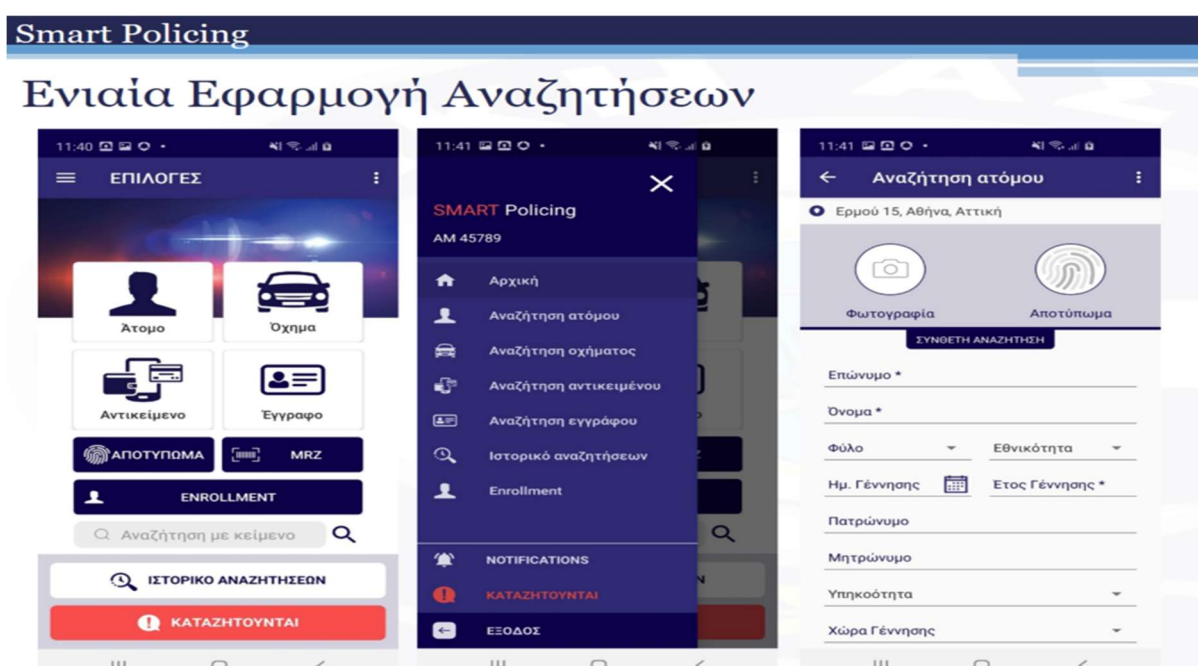
#### 2. Λογισμικό ασφαλούς διασύνδεσης - διαχείρισης έξυπνων φορητών συσκευών.

Για να διασφαλιστεί η απρόσκοπτη λειτουργία και προστασία των δεδομένων σε όλες τις φορητές συσκευές που σχετίζονται με το έργο, εκτελέστηκε η εγκατάσταση και η διαμόρφωση διεθνώς αναγνωρισμένου λογισμικού από τον κατασκευαστή VMWare, σε πλήρη συμμόρφωση με τους ισχύοντες κανονισμούς και την πολιτική ασφαλείας του Φορέα, ενώ παράλληλα αντιμετωπίστηκαν όλες οι περιπτώσεις χρήσης. Επιπλέον, η παροχή 3000 αδειών χρήσης του εν λόγω λογισμικού επιτρέπει την ενσωμάτωση των εξελιγμένων λειτουργιών του στις υπάρχουσες φορητές συσκευές που χρησιμοποιεί η Ελληνική Αστυνομία (tablets,

smartphones και φορητούς υπολογιστές), οι οποίες διαθέτουν τα απαιτούμενα χαρακτηριστικά συμβατότητας. Η προκαθορισμένη προμήθεια και διαμόρφωση του λογισμικού διευκολύνει τη μελλοντική επέκταση μόνο με την παροχή πρόσθετων αδειών, εξαλείφοντας την ανάγκη για ανάλογο κεντρικό εξοπλισμό (περίπου 10.000 συσκευές).

### 3. Κεντρική εφαρμογή αναζητήσεων.

Η εφαρμογή αναζήτησης του έργου προσφέρει μια ολοκληρωμένη πλατφόρμα για την αναζήτηση σε όλες σχεδόν τις τρέχουσες βάσεις δεδομένων της Ελληνικής Αστυνομίας, που περιλαμβάνουν επιχειρησιακά και εγκληματολογικά δεδομένα. Εκτελέστηκε με διπλή μεθοδολογία, προσφέροντας τόσο ένα περιβάλλον για κινητά όσο και για ηλεκτρονικούς υπολογιστές. Λαμβάνοντας υπόψη τα προαναφερθέντα κριτήρια, οι εφαρμογές μπορούν να χρησιμοποιηθούν από όλους τους τρέχοντες υπολογιστές εντός του δικτύου Police On Line χωρίς την ανάγκη χρήσης επιπλέον λογισμικού. Η ιδιαιτερότητα της εφαρμογής χαρακτηρίζεται από την αυστηρή τήρηση των δικαιωμάτων πρόσβασης του χρήστη στις υπάρχουσες βάσεις δεδομένων, διασφαλίζοντας ότι μη εξουσιοδοτημένοι χρήστες δεν μπορούν να έχουν πρόσβαση στα δεδομένα. Ο μηχανισμός συντήρησης που προβλέπεται για το πρόγραμμα επιτρέπει στο εξειδικευμένο προσωπικό της Διεύθυνσης Πληροφορικής να διευκολύνει τη μελλοντική σύνδεση νέων βάσεων δεδομένων ή πηγών πληροφοριών.



Εικόνα 4 Επίδειξη Ενιαίας Εφαρμογής Αναζητήσεων



υπάρχουσες βάσεις δεδομένων: ΔΕΕ Ευρετήρια, Μητρώο Αλλοδαπών και Ταυτότητες Ελλήνων Πολιτών. Προσφέρει εξειδικευμένο λογισμικό για την αξιοποίηση της δυνατότητας αναγνώρισης προσώπου σε φορητές συσκευές, με στόχο την ενίσχυση της ικανότητας ενός αστυνομικού να αναγνωρίζει ένα άτομο (είτε διώκεται είτε όχι) που δεν διαθέτει έγγραφα αναγνώρισης κατά τη διάρκεια αστυνομικών ελέγχων ή διαδικαστικών ερευνών. Η μέθοδος αυτή εκτελείται χωρίς τη διατήρηση στοιχείων βιομετρικών δεδομένων στο σύστημα. Ταυτόχρονα, τρεις προηγμένοι σταθμοί εργασίας είναι εξοπλισμένοι για την εκ νέου εξαγωγή βιομετρικών δεδομένων από ψηφιακό υλικό, αυξάνοντας έτσι την επιστημονική-επιχειρησιακή ικανότητα του Τμήματος Εγκληματολογικών Ερευνών και του Τμήματος Διαχείρισης και Ανάλυσης Πληροφοριών.

#### 6. Αναβάθμιση Εθνικού Συστήματος AFIS

Το σύστημα AFIS, το οποίο λειτουργεί από τον Δεκέμβριο του 2016, χρησιμοποιείται καθημερινά για την εκπλήρωση των απαιτήσεων των δεκαδικών ταυτοποιήσεων που διενεργούνται από 225 σταθμούς εργασίας σε όλη την Ελλάδα. Η βάση δεδομένων δεκαδικών δακτυλικών αποτυπωμάτων του συστήματος χρησιμεύει ως το εθνικό αποθετήριο δακτυλικών αποτυπωμάτων της εγκληματολογικής υπηρεσίας, το οποίο περιλαμβάνει τις κάρτες δεκαδικών δακτυλικών αποτυπωμάτων ατόμων που έχουν δακτυλοσκοπηθεί σε όλη την επικράτεια. Κατά την παρούσα φάση λειτουργίας του έργου, ο τυπικός ημερήσιος όγκος αναζητήσεων κυμαίνεται από 450 έως 550 αναζητήσεις δακτυλικών αποτυπωμάτων. Στόχος της αναβάθμισης που εκτελείται στο πλαίσιο του παρόντος έργου είναι η βελτίωση του εθνικού AFIS ώστε να διευκολύνεται η ταυτοποίηση και η αναζήτηση δακτυλικών αποτυπωμάτων από τουλάχιστον δύο (2) δάκτυλα. Η εγκατάσταση ενός εξειδικευμένου προγράμματος για την αποτύπωση δακτυλικών αποτυπωμάτων, με τη χρήση ενός smartphone εξοπλισμένου με ειδικό δέκτη δακτυλικών αποτυπωμάτων, έχει ολοκληρωθεί για τη διευκόλυνση των αναζητήσεων για ατομική ταυτοποίηση.

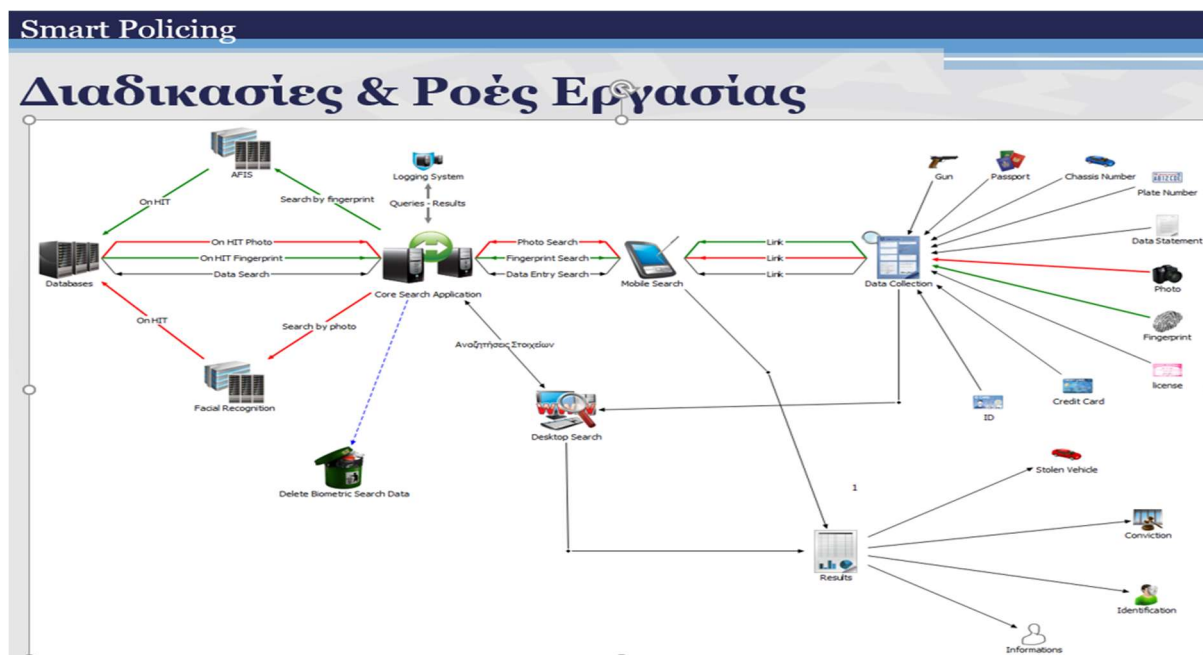
#### 7. Λογισμικό Γεωγραφικής Απεικόνισης.

Η συμβατικά καθορισμένη εφαρμογή του λογισμικού γεωγραφικής απεικόνισης περιγράφει τη δημιουργία ενός νέου συστήματος ΓΣΠ που απεικονίζει τα γεωγραφικά σημεία των αναζητήσεων, τα αντίστοιχα αποτελέσματα και τα καταγεγραμμένα περιστατικά, χρησιμοποιώντας σχετικά κριτήρια όπως η γεωγραφική περιοχή, η ομάδα χρηστών, ο τύπος

αναζήτησης (π.χ., άτομα/οχήματα, βιομετρικές αναζητήσεις) και το αποτέλεσμα της αναζήτησης (με συμμετοχή ατόμων/οχημάτων ή όχι). Ο Ανάδοχος παρέδωσε με επιτυχία την πλήρη λειτουργικότητα του CrimeView μέσω της νέας υποδομής λογισμικού, εκπληρώνοντας τη συμβατική υποχρέωση, ενώ παράλληλα φιλοξένησε 86 ταυτόχρονους χρήστες, ξεπερνώντας την προηγούμενη χωρητικότητα των 10 χρηστών.

## 8. Κεντρικό Εξοπλισμός-Υπηρεσίες ΤΠΕ

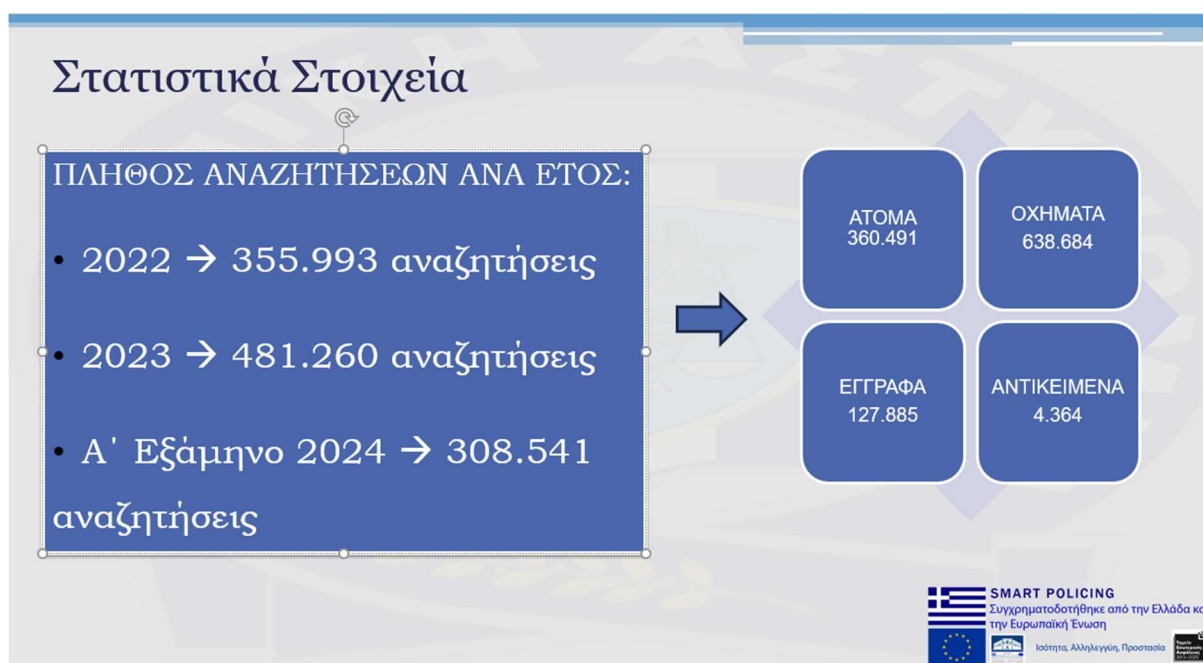
Για την φιλοξενία και λειτουργία συσκευών και λογισμικών, πραγματοποιήθηκε παραμετροποίηση κεντρικού εξοπλισμού εξυπηρετητών και δικτυακών υποδομών. Παράλληλα καλύπτονται τα τηλεπικοινωνιακά έξοδα χρήσης υποδομής δικτύου κινητής τηλεφωνίας για την ένταξη των smartphone στην υφιστάμενη υποδομή της Ελληνικής Αστυνομίας και την επικοινωνία τους με τα κεντρικά συστήματα ΤΠΕ αυτής.



Εικόνα 6 Επίδειξη Εξοπλισμού - Εργασιών

Η Ελληνική Αστυνομία συμμετείχε στον Διαγωνισμό Βραβείων Ψηφιακής Διακυβέρνησης (Digital Gov Awards) για το έτος 2022 που διοργανώθηκε με στόχο τον ψηφιακό μετασχηματισμό των κρατικών υποδομών, με το έργο «Εξυπνη Αστυνόμευση (Smart

Policing)», αποσπώντας το πρώτο βραβείο στην κατηγορία «Καλύτερη Εφαρμοσμένη Ιδέα» στην θεματική ενότητα «Ασφάλεια του Πολίτη». Η επιτυχία του έργου στηρίχθηκε στα κοινά στελέχη στις Επιτροπές σε κάθε φάση της δράσης (Επιτροπή τεχνικών προδιαγραφών, Επιτροπή τεχνικής αξιολόγησης και Επιτροπή Παρακολούθησης και Παραλαβής), στην ολοκλήρωση της Διακήρυξης στους προβλεπόμενους χρόνους, στις Ειδικές προβλέψεις σύμβασης για συνεχή ανάπτυξη νέων δυνατοτήτων κατά τη διάρκεια της περιόδου εγγύησης (Ανάπτυξη δυνατότητας στατιστικών στοιχείων, Αντικατάσταση προβληματικών συσκευών χωρίς κόστος για την Αναθέτουσα, Ενσωμάτωση νέων υπηρεσιών στην εφαρμογή αναζητήσεων, Βελτιστοποίηση εφαρμογής καταγραφής περιστατικών) και στην δυνατότητα Επέκτασης



Εικόνα 7 Στατιστικά στοιχεία

## 2.4. Panic button

Με το αρ. 19 του Ν. 4995/2022, θεσπίστηκε η πιλοτική λειτουργία του προγράμματος «Κομβίον Πανικού» (Panic Button), και τέθηκε σε επιχειρησιακή λειτουργία την Πέμπτη 23 Μαρτίου 2023 στην Αττική και τη Θεσσαλονίκη για την αντιμετώπιση περιστατικών ενδοοικογενειακής βίας. Πρόκειται για μια δωρεάν ψηφιακή εφαρμογή σχεδιασμένη για θύματα ενδοοικογενειακής βίας, που τους δίνει τη δυνατότητα να ειδοποιούν άμεσα και με ασφάλεια την Ελληνική Αστυνομία μέσω των smartphones τους σε περιπτώσεις ενδοοικογενειακής βίας που συνιστούν απειλή για τη ζωή ή τη σωματική τους ακεραιότητα (Ελληνική Αστυνομία, 2023).

Το θύμα ενεργοποιεί το πρόγραμμα αγγίζοντας και κρατώντας πατημένη την καθορισμένη ένδειξη στην οθόνη του κινητού του τηλεφώνου, η οποία μεταδίδει αυτόματα ένα γραπτό μήνυμα (SMS) στο Επιχειρησιακό Κέντρο της Διεύθυνσης Άμεσης Δράσης Αττικής που περιλαμβάνει βασικές πληροφορίες αναγνώρισης. Με το πάτημα ενός μόνο κουμπιού στην κινητή συσκευή της, το θύμα που βρίσκεται σε άμεσο κίνδυνο μπορεί να ειδοποιήσει άμεσα και με ασφάλεια τις αστυνομικές αρχές. Η εφαρμογή λειτουργεί ως κρυφός συναγερμός, καθώς ο δράστης παραμένει ανυποψίαστος για το θύμα που ειδοποιεί την Ελληνική Αστυνομία. Η αξιοποίηση του κουμπιού πανικού ελαχιστοποιεί τη διάρκεια που απαιτείται για την ενημέρωση των αρχών σχετικά με το περιστατικό. Σε αυτό το πρώιμο στάδιο, η εφαρμογή χορηγούνταν από τα Αστυνομικά Τμήματα και τα Γραφεία Αντιμετώπισης Ενδοοικογενειακής Βίας σε Αττική και Θεσσαλονίκη και τα Συμβουλευτικά Κέντρα που υπάγονται στο Δίκτυο Δομών της Γενικής Γραμματείας Ισότητας και Ανθρωπίνων Δικαιωμάτων του Υπουργείου Κοινωνικής Συνοχής και Οικογένειας (Ελληνική Αστυνομία, 2023).

Σύμφωνα με νεότερες Κοινές Υπουργικές Αποφάσεις [υπ' αριθμό ΥΚΟΙΣΟ/ 32276 Κ.Υ.Α. (Φ.Ε.Κ. Β' 2922/ 23-5-2024) και υπ' αριθμό ΥΚΟΙΣΟ/ 32277 Κ.Υ.Α. (Φ.Ε.Κ. Β' 2921/ 23-5-2024)], επεκτάθηκε η δυνατότητα χορήγησης της εφαρμογής "Panic Button" σε όλα τα ενήλικα θύματα ενδοοικογενειακής βίας και για όλη την ελληνική επικράτεια, ανεξαρτήτως φύλου. Όσον αφορά στη χορήγηση από Υπηρεσίες της Ελληνικής Αστυνομίας, "Η εφαρμογή «Κομβίον Πανικού» (Panic Button) χορηγείται στους δικαιούχους από: α) τα Επιχειρησιακά Γραφεία Αντιμετώπισης Ενδοοικογενειακής Βίας, β) τα Αστυνομικά Τμήματα των εκάστοτε Αστυνομικών Διευθύνσεων και γ) τις Υποδιευθύνσεις Ασφαλείας και τα Τμήματα Ασφαλείας. Μετά την επιτυχή ολοκλήρωση της διαδικασίας εγγραφής στην εφαρμογή, το εγγεγραμμένο

πρόσωπο έχει την δυνατότητα να ειδοποιεί την Διεύθυνση Άμεσης Δράσης Αττικής («100»), με την επιλογή της οικείας ένδειξης στην οθόνη του κινητού τηλεφώνου του, σε περίπτωση περιστατικού ενδοοικογενειακής βίας, που συνδέεται με άμεσο κίνδυνο ή με απειλή κινδύνου της ζωής του ή της σωματικής ακεραιότητάς του. Η Διεύθυνση Άμεσης Δράσης Αττικής ενημερώνει άμεσα την αντίστοιχη Υπηρεσία της οικείας Διεύθυνσης Αστυνομίας (Υπουργείο Προστασίας Πολίτη, 2024).

Η εφαρμογή του κουμπιού πανικού λειτουργεί στο πλαίσιο της βάσης δεδομένων της Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης (ΓΓΠΣΔΔ) του υπουργείου Ψηφιακής Διακυβέρνησης βάση δεδομένων με ονομασία «ΚΟΜΒΙΟΝ ΠΑΝΙΚΟΥ (Panic Button)». Οι πληροφορίες αποθηκεύονται σε κρυπτογραφημένη μορφή εντός της βάσης δεδομένων «ΚΟΥΜΠΙ ΠΑΝΙΚΟΥ (Panic Button)» είναι τα εξής (ΥΚΟΙΣΟ/32276/17.5.2024):

- α. Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ)
- β. Ονοματεπώνυμο
- γ. Αριθμός Κινητού Τηλεφώνου
- δ. Διεύθυνση κατοικίας (με αριθμό και Ταχυδρομικό Κώδικα σε διακριτά πεδία)
- ε. Όνομα που αναγράφεται στο κουδούνι της κατοικίας
- στ. Όροφος Κατοικίας
- ζ. Ύπαρξη ιστορικού περιστατικών κακοποίησης
- η. Ένδειξη κατοχής όπλου
- θ. Ένδειξη ύπαρξης τέκνων
- ι. Ένδειξη ύπαρξης ιστορικού εξαρτήσεων από ουσίες
- ια. Ένδειξη ύπαρξης ιστορικού ψυχολογικών διαταραχών
- ιβ. Ένδειξη εγκυμοσύνης (σε περίπτωση που η εγκατάσταση αφορά γυναίκα)
- ιγ. Κωδικός χρήσης της εφαρμογής που αποδίδεται στο χρήστη

Εκτός από την αντιμετώπιση της συζυγικής βίας, το κουμπί πανικού έχει σχεδιαστεί για την καταπολέμηση του εκφοβισμού και των περιπτώσεων βίας κατά των παιδιών. Η εφαρμογή θα τοποθετηθεί στα κινητά τηλέφωνα των εφήβων, δίνοντάς τους τη δυνατότητα να εκπέμπουν σήμα κινδύνου όταν βρίσκονται σε κίνδυνο. Η αστυνομία θα λαμβάνει γνώση της θέσης του παιδιού και θα μπορεί να βοηθήσει άμεσα (ΥΚΟΙΣΟ/32276/17.5.2024).

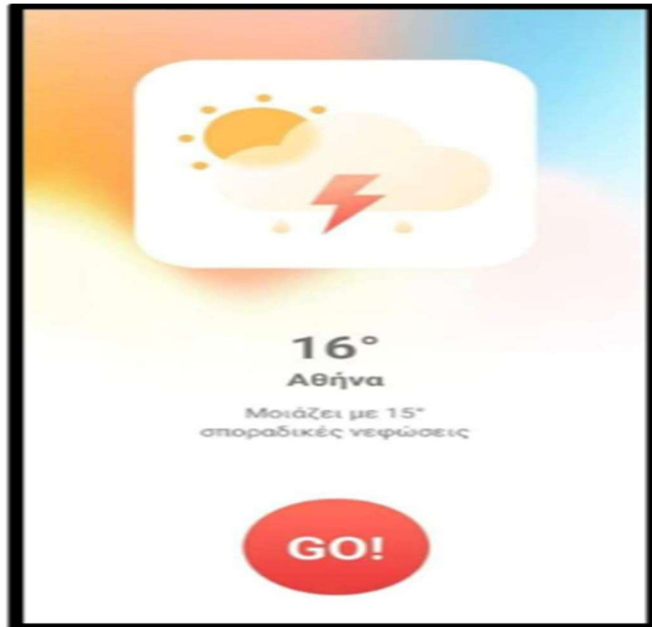
Το «Panic Button» είναι μια ψηφιακή εφαρμογή που έχει σχεδιαστεί για την κάλυψη των αναγκών έκτακτης ανάγκης που σχετίζονται με την ενδοοικογενειακή βία, σύμφωνα με την ελληνική νομοθεσία, συγκεκριμένα το άρθρο 19 του νόμου 4995/2022. Το πρόγραμμα «Panic

Button» διέπεται από συγκεκριμένες νομοθετικές και κανονιστικές διατάξεις, με τη βασική νομική δομή του να βασίζεται στο ελληνικό εθνικό δίκαιο και να συμμορφώνεται με τα ευρωπαϊκά πρότυπα προστασίας δεδομένων (GDPR, Κανονισμός ΕΕ 2016/679). Τροποποιήσεις στη λειτουργία του έχουν υλοποιηθεί με διαδοχικές αποφάσεις (π.χ. Φ.Ε.Κ. Β' 2922/2024), που εγγυώνται αυξημένη προσβασιμότητα και ασφαλή αξιοποίηση για τα θύματα ενδοοικογενειακής βίας (ΥΚΟΙΣΟ/32276/17.5.2024).

Η εφαρμογή είναι προσβάσιμη σε ενήλικα θύματα ενδοοικογενειακής βίας, όπως ορίζεται στο νόμο 3500/2006. Η ανάπτυξη δίνει προτεραιότητα στη συνεργασία μεταξύ των υπηρεσιών επιβολής του νόμου, των κέντρων κοινωνικής υποστήριξης και των κυβερνητικών φορέων. Τα θύματα εγγράφονται απευθυνόμενα σε εξουσιοδοτημένο προσωπικό σε αστυνομικά τμήματα, συμβουλευτικά κέντρα ή άλλους καθορισμένους φορείς. Μετά την εγκατάσταση, οι χρήστες μπορούν να ειδοποιήσουν την αστυνομία ενεργοποιώντας την εφαρμογή. Η ενέργεια αυτή μεταδίδει SMS σε πραγματικό χρόνο με βασικά προσωπικά δεδομένα και δεδομένα θέσης στις αρμόδιες υπηρεσίες επιβολής του νόμου, επιτρέποντας την ταχεία ανταπόκριση. Σε περιοχές που δεν διαθέτουν άμεση μονάδα αντιμετώπισης έκτακτης ανάγκης, οι ειδοποιήσεις προωθούνται στο πλησιέστερο αστυνομικό τμήμα. Το πρόγραμμα καταδεικνύει την αφοσίωση στην ασφάλεια των θυμάτων, τη βελτίωση των αντιδράσεων των αρχών επιβολής του νόμου και την ενσωμάτωση της τεχνολογίας στην κοινωνική προστασία. Οι συνεχείς ενημερώσεις και τα σχόλια των χρηστών είναι απαραίτητα για την ανάπτυξη και την αποτελεσματικότητα του προγράμματος, αναδεικνύοντας την σημασία του για την κοινωνική ασφάλεια (ΥΚΟΙΣΟ/32276/17.5.2024).

Συνοπτικά η λειτουργία της εφαρμογής έχει ως εξής:

- Υπάρχουν δύο κατηγορίες κινητών τηλεφώνων, στα οποία εγκαθίσταται η εφαρμογή: α) κινητά τηλέφωνα που λειτουργούν με λογισμικό “Android” και β) κινητά τηλέφωνα που λειτουργούν με λογισμικό “iOS”. Ανάλογα με τον τύπο συσκευής που έχει στην κατοχή του ο χρήστης ακολουθεί τα αντίστοιχα βήματα για την εγκατάσταση. Μετά την εγκατάσταση της εφαρμογής στο κινητό τηλέφωνο του τελικού χρήστη, θα εμφανιστεί το εικονίδιο της εφαρμογής υπό την ονομασία “SKY”.



Εικόνα 8 menu εφαρμογής sky

Στην οθόνη της εφαρμογής υπάρχουν τα παρακάτω «κουμπιά» με τις αντίστοιχες λειτουργικότητες ως εξής:

1) Εικονίδιο «καιρού»

- Απλό/γρήγορο πάτημα εικονιδίου καιρού: Δεν έχει καμία λειτουργικότητα.
- Παρατεταμένο πάτημα (για τουλάχιστον 6 δευτερόλεπτα): εμφανίζεται οθόνη επεξεργασίας / διαγραφής των στοιχείων του/της εγγεγραμμένου/ης χρήστη/ριας.

2) «Πληροφορίες για τον καιρό»

- Με απλό/γρήγορο πάτημα πάνω στις πληροφορίες για τον καιρό εμφανίζεται σελίδα με πληροφορίες για τον καιρό στο σημείο που βρίσκεται ο/η τελικός/ή χρήστης/ρια.
- Παρατεταμένο πάτημα: Καμία λειτουργικότητα.

3) Κουμπί «Go»

- Απλό/γρήγορο πάτημα του κουμπιού “GO”: εμφανίζει πληροφορίες για τον καιρό του σημείου που βρίσκεται ο/η τελικός/ή χρήστης/ρια.
- Παρατεταμένο πάτημα του κουμπιού “GO” για τουλάχιστον τρία δευτερόλεπτα (3 sec): αποστέλλεται SMS στην Άμεση Δράση (100).

- Το 100 θα εντοπίσει το στίγμα της τοποθεσίας του/της τελικού/ής χρήστη/ριας, όπως αυτό εμφανίζεται τη στιγμή της αποστολής του αυτοματοποιημένου μηνύματος. Για τον λόγο αυτό, θα είναι υποχρεωτικό, κατά την πρώτη λειτουργία της εφαρμογής, να συναινέσει ο/η

ενδιαφερόμενος/η στα αντίστοιχα μηνύματα αποδοχής της ενεργοποίησης της ρύθμισης εντοπισμού τοποθεσίας, όπως περιγράφεται παραπάνω. Σε περίπτωση μεταγενέστερης απενεργοποίησης της ρύθμισης εντοπισμού τοποθεσίας, η εφαρμογή δεν θα μπορεί να λειτουργεί και θα εμφανίζει μήνυμα ότι πρέπει να ενεργοποιηθεί η ρύθμιση εντοπισμού της τοποθεσίας.

- Ο χρήστης τουλάχιστον μια φορά το μήνα, πρέπει να μπαίνει στην εφαρμογή και να λαμβάνει τυχόν ενημερώσεις. Μπορεί να διαγράψει την εφαρμογή από το κινητό του, όποτε επιθυμεί, χωρίς να πρέπει να το δηλώσει κάπου.

## 2.5. Ιστότοπος [www.astynomia.gr](http://www.astynomia.gr)

Η Ελληνική Αστυνομία αποτελείται από κεντρικές και περιφερειακές υπηρεσίες. Το αρχηγείο της Ελληνικής Αστυνομίας λειτουργεί ως η υπέρτατη αρχή αυτών των Υπηρεσιών. Οι προσπάθειές τους επικεντρώνονται στην επίτευξη του στόχου της Δύναμης σύμφωνα με την πολιτική του Υπουργείου Εσωτερικών. Κατά συνέπεια, προγραμματίζει, κατευθύνει, εποπτεύει και ελέγχει τη δράση των Υπηρεσιών της, εξασφαλίζοντας τις απαιτούμενες προϋποθέσεις για την άσκηση της εξουσίας της. Στο πλαίσιο της διαρκούς δέσμευσής της για την εξυπηρέτηση και την προστασία των πολιτών, η Ελληνική Αστυνομία έχει αντιμετωπίσει τις σύγχρονες ανάγκες και προβλήματα με την ενίσχυση της εκπαίδευσης, την εφαρμογή μιας σύγχρονης στρατηγικής πρόληψης του εγκλήματος, τη βελτιστοποίηση της χρήσης της επιστήμης και της τεχνολογίας και την αξιοποίηση της διεθνούς συνεργασίας στον τομέα της επιβολής του νόμου (Hellenic Police, 2022). Ο ιστότοπος προσφέρει εμπειριστατωμένες πληροφορίες σχετικά με τη δομή και τις λειτουργίες της Ελληνικής Αστυνομίας, συμπεριλαμβανομένης της αποστολής, του οράματος και των υπηρεσιών της. Παρέχει μια επισκόπηση των επιχειρήσεων, των μονάδων και της δικαιοδοσίας της αστυνομίας. Ο επίσημος ιστότοπος της Ελληνικής Αστυνομίας, [astynomia.gr](http://astynomia.gr), λειτουργεί ως μια ολοκληρωμένη πύλη για πληροφορίες και υπηρεσίες που σχετίζονται με την ασφάλεια. Τα βασικά χαρακτηριστικά περιλαμβάνουν:

- **Οδηγός του πολίτη:** Εδώ, οι χρήστες λαμβάνουν πρακτικές συμβουλές για διάφορα θέματα ασφάλειας, όπως η ενδοοικογενειακή βία, η οδική ασφάλεια, η πρόληψη κλοπών και οι πρακτικές ασφαλούς διαδικτύου.

- **Στοιχεία επικοινωνίας:** Ο ιστότοπος παραθέτει στοιχεία επικοινωνίας για διάφορα αστυνομικά τμήματα και υπηρεσίες, γεγονός που διευκολύνει την άμεση επικοινωνία για βοήθεια ή αναφορά περιστατικών.
- **Ειδικές υπηρεσίες:** Διατίθενται πληροφορίες σχετικά με τις εξειδικευμένες υπηρεσίες, συμπεριλαμβανομένης της Διεύθυνσης Διαχείρισης και Ανάλυσης Πληροφοριών της Ελληνικής Αστυνομίας και της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, όπου περιγράφονται λεπτομερώς οι ρόλοι και τα στοιχεία επικοινωνίας τους.
- **Τύπος και Μέσα Μαζικής Ενημέρωσης:** Για την ενημέρωση των πολιτών σχετικά με τη δημόσια ασφάλεια και τις αστυνομικές επιχειρήσεις παρέχονται ενημερώσεις για πρόσφατες δραστηριότητες, δελτία τύπου και στατιστικά στοιχεία.

Ο ιστότοπος έχει σχεδιαστεί για να ενισχύσει τη δημόσια ασφάλεια προσφέροντας προσβάσιμες πληροφορίες και διευκολύνοντας την επικοινωνία μεταξύ των πολιτών και των υπηρεσιών επιβολής του νόμου. Το [astynomia.gr](http://astynomia.gr) μπορεί να κατευθύνει τους χρήστες σε άλλες κυβερνητικές πύλες για πιο εξειδικευμένες υπηρεσίες (π.χ. πληροφορίες για την άδεια οδήγησης, αναφορά περιστατικών κ.λπ.). Μέσω του δικτυακού τόπου, τα άτομα μπορούν να αναφέρουν εγκλήματα, τροχαία συμβάντα ή αγνοούμενα άτομα. Περιλαμβάνει επιλογές για την επικοινωνία με τα τοπικά αστυνομικά τμήματα και την υποβολή αναφορών για διάφορους τύπους περιστατικών. Μπορούν επίσης να αναρτηθούν ειδοποιήσεις σχετικά με εν εξελίξει έρευνες ή απειλές για την ασφάλεια.

Ο ιστότοπος προσφέρει πληροφορίες σχετικά με τρέχουσες ή επερχόμενες εκδηλώσεις που σχετίζονται με την αστυνομία, όπως προγράμματα προσέγγισης της κοινότητας, εκστρατείες ασφάλειας και πρωτοβουλίες δημόσιας εκπαίδευσης. Η αστυνομία συχνά συνεργάζεται με άλλους κυβερνητικούς και μη κυβερνητικούς οργανισμούς για την προώθηση της ασφάλειας και της κοινωνικής ευημερίας. Ο ιστότοπος παρέχει περιοδικά στατιστικά στοιχεία σχετικά με τις τάσεις της εγκληματικότητας, την αποτελεσματικότητα της επιβολής του νόμου και τους δείκτες δημόσιας ασφάλειας.

## **ΚΕΦΑΛΑΙΟ 3: Ανάλυση SWOT για τις Υπηρεσίες Η.Δ. στην Ελληνική Αστυνομία**

### **3.1. Δυνάμεις**

Η Ελληνική Αστυνομία έχει αναπτύξει μια ισχυρή βάση για το σχέδιό της για την ηλεκτρονική διακυβέρνηση, κυρίως λόγω της ανθεκτικής υποδομής πληροφορικής. Η υποδομή αυτή είναι απαραίτητη για την επιχειρησιακή τους αποτελεσματικότητα, προσφέροντας την τεχνολογική υποστήριξη που απαιτείται για τη σύγχρονη επιβολή του νόμου σε ένα προοδευτικά ψηφιοποιημένο περιβάλλον. Το δίκτυο «Police On Line» είναι σημαντικό για την υποδομή αυτή, αλλάζοντας σημαντικά τις μεθόδους εσωτερικής και εξωτερικής επικοινωνίας στο εσωτερικό του οργανισμού. Αυτή η προηγμένη τεχνολογία επιτρέπει την ομαλή μεταφορά πληροφοριών μεταξύ διαφόρων τμημάτων, ενισχύοντας τη συνεργασία και τη λειτουργική αποτελεσματικότητα (Dimitreliou & Fouskas, 2023). Ως αποτέλεσμα, οι διαδικασίες λήψης αποφάσεων επιταχύνονται, επιτρέποντας στην αστυνομία να ανταποκρίνεται γρήγορα στις αναδυόμενες καταστάσεις και να κατανέμει αποτελεσματικά τους πόρους. Η ενισχυμένη επικοινωνία που επιτρέπει το δίκτυο «Police On Line» έχει γεφυρώσει τα κενά που υπήρχαν προηγουμένως στις παραδοσιακές ροές εργασίας, βελτιώνοντας σημαντικά τη συνολική λειτουργικότητα του οργανισμού (Sarifudin & Damanik, 2024).

Η χρήση εξελιγμένων μέσων, όπως το σύστημα «Ηλεκτρονική Αλληλογραφία», έχει ενισχύσει την αποτελεσματικότητα της λειτουργίας της Ελληνικής Αστυνομίας. Η μέθοδος αυτή έχει μειώσει σημαντικά τις αναποτελεσματικότητες που συνδέονται με τις συμβατικές εργασίες σε χαρτί μέσω της ψηφιοποίησης της διαχείρισης εγγράφων. Πριν από την ανάπτυξή του, οι αστυνομικές υπηρεσίες αντιμετώπιζαν σημαντικές καθυστερήσεις στην επικοινωνία λόγω της χειροκίνητης ανταλλαγής εγγράφων, με αποτέλεσμα λάθη, λανθασμένη τοποθέτηση αρχείων και παρατεταμένες περιόδους λήψης αποφάσεων. Το σύστημα «Ηλεκτρονική Αλληλογραφία» βελτιστοποίησε αυτές τις διαδικασίες, διευκολύνοντας την άμεση αποστολή και λήψη βασικών εγγράφων. Αυτή η αυτοματοποίηση έχει βελτιώσει την αποτελεσματικότητα και την ακρίβεια των εσωτερικών διαδικασιών, ενώ παράλληλα προωθεί μια πιο διαφανή και υπεύθυνη οργανωτική κουλτούρα. Τα στελέχη και οι διοικητικοί υπάλληλοι μπορούν πλέον να

παρακολουθούν την κατάσταση της αλληλογραφίας, ελαχιστοποιώντας τον κίνδυνο εσφαλμένης επικοινωνίας ή παράβλεψης. Η λύση αυτή έχει μειώσει σημαντικά τις γραφειοκρατικές αναποτελεσματικότητες, έχει επιταχύνει τις ροές εργασίας και έχει ενισχύσει την ανταπόκριση του τμήματος επιβολής του νόμου (Yamin et al., 2020).

Ένα σημαντικό πλεονέκτημα στην ατζέντα της Ελληνικής Αστυνομίας για την ηλεκτρονική διακυβέρνηση είναι η εφαρμογή συστημάτων Car-PC στα περιπολικά οχήματα. Τα εργαλεία αυτά μεταμορφώνουν σημαντικά τις επιχειρήσεις των αστυνομικών πεδίου, παρέχοντας πρόσβαση σε πραγματικό χρόνο σε βασικές πληροφορίες που βελτιώνουν την επίγνωση της κατάστασης και τη λήψη αποφάσεων. Με αυτά τα φορητά τερματικά δεδομένων, οι αστυνομικοί μπορούν να έχουν άμεση πρόσβαση σε πληροφορίες σχετικά με τις εγγραφές αυτοκινήτων, τις βάσεις δεδομένων ποινικών υποθέσεων και άλλα σχετικά έγγραφα. Για παράδειγμα, κατά την αντιμετώπιση ενός ισχυρισμού για ένα ύποπτο αυτοκίνητο, οι αρχές μπορούν να εξακριβώσουν αμέσως την κατάσταση ταξινόμησής του, τις πληροφορίες ιδιοκτησίας και τυχόν διαπιστωμένες συνδέσεις με εγκληματικές δραστηριότητες. Η δυνατότητα αυτή βελτιώνει αισθητά την ικανότητά τους να λαμβάνουν τεκμηριωμένες αποφάσεις σε πραγματικό χρόνο, ενισχύοντας έτσι τόσο την ασφάλεια των αστυνομικών όσο και την αποτελεσματικότητα των ενεργειών τους. Σε σενάρια υψηλής πίεσης, όπου ο χρόνος είναι κρίσιμος, η ικανότητα ανάκτησης πληροφοριών απευθείας από το περιπολικό όχημα μπορεί να καθορίσει την επιτυχία ή την αποτυχία μιας επιχείρησης (Sarifudin & Damanik, 2024).

Η ενσωμάτωση εθνικών και διεθνών βάσεων δεδομένων προσθέτει ένα ακόμη επίπεδο πολυπλοκότητας στα συστήματα Car-PC της Ελληνικής Αστυνομίας. Η πρόσβαση σε βάσεις δεδομένων, όπως αυτές που τηρούνται από την Interpol και την Europol, επιτρέπει στους αστυνομικούς να συμμετέχουν απρόσκοπτα σε διασυνοριακές ποινικές έρευνες. Αυτή η ικανότητα είναι ιδιαίτερα κρίσιμη σε μια εποχή όπου εγκλήματα όπως η εμπορία ανθρώπων, το λαθρεμπόριο ναρκωτικών και το έγκλημα στον κυβερνοχώρο υπερβαίνουν τα εθνικά σύνορα. Συνεργαζόμενη με διεθνείς υπηρεσίες επιβολής του νόμου και αξιοποιώντας τις κοινές πληροφορίες, η Ελληνική Αστυνομία μπορεί να εντοπίζει υπόπτους, να ανακτά κλεμμένα περιουσιακά στοιχεία και να εξαρθρώνει αποτελεσματικότερα εγκληματικά δίκτυα. Η δυνατότητα πρόσβασης σε παγκόσμιες βάσεις δεδομένων σε πραγματικό χρόνο όχι μόνο ενισχύει την επιχειρησιακή αποτελεσματικότητα της Ελληνικής Αστυνομίας αλλά και την

αξιοπιστία της ως αξιόπιστου εταίρου στις διεθνείς προσπάθειες επιβολής του νόμου (Sarifudin & Damanik, 2024).

Οι τεχνολογίες βιομετρικής ταυτοποίησης έχουν εκσυγχρονίσει σημαντικά τις λειτουργίες της Ελληνικής Αστυνομίας. Οι τεχνολογίες που περιλαμβάνουν την αναγνώριση προσώπου, τη σάρωση δακτυλικών αποτυπωμάτων και την αναγνώριση φωνής έχουν μεταμορφώσει τις μεθόδους επαλήθευσης της ταυτότητας. Ιστορικά, η επιβεβαίωση της ταυτότητας ενός ατόμου απαιτούσε συχνά επίπονες χειροκίνητες διαδικασίες επιρρεπείς σε ανακρίβειες. Τα βιομετρικά μέσα έχουν βελτιστοποιήσει αυτές τις διαδικασίες, επιτρέποντας στους αστυνομικούς να επαληθεύουν τις ταυτότητες γρήγορα και με ακρίβεια. Κατά τη διάρκεια τακτικών στάσεων κυκλοφορίας ή ελέγχων ασφαλείας, οι αρχές μπορούν να χρησιμοποιούν φορητούς βιομετρικούς σαρωτές για να σαρώνουν το δακτυλικό αποτύπωμα ή τα χαρακτηριστικά του προσώπου ενός υπόπτου, διασταυρώνοντας αμέσως τις πληροφορίες με τα ποινικά μητρώα. Αυτή η λειτουργία όχι μόνο επιταχύνει τις επιτόπιες επιχειρήσεις, αλλά και βελτιώνει την ασφάλεια, καθώς εγγυάται ότι δεν παραλείπεται καμία βασική πληροφορία (Sarifudin & Damanik, 2024).

Οι ψηφιακές υπηρεσίες που απευθύνονται στο κοινό αποτελούν σημαντικό πλεονέκτημα στο σχέδιο ηλεκτρονικής διακυβέρνησης της Ελληνικής Αστυνομίας. Μέσω πλατφορμών όπως το GOV.GR, η αστυνομία έχει βελτιώσει σημαντικά τον τρόπο με τον οποίο αλληλεπιδρά με τους πολίτες, καθιστώντας τις υπηρεσίες πιο προσιτές και φιλικές προς το χρήστη. Η στροφή αυτή ευθυγραμμίζεται με τις ευρύτερες τάσεις στην ψηφιακή διακυβέρνηση, όπου οι δημόσιοι οργανισμοί αξιοποιούν την τεχνολογία για να βελτιώσουν τη διαφάνεια, την αποτελεσματικότητα και την ικανοποίηση των πολιτών. Προσφέροντας υπηρεσίες όπως η έκδοση ποινικού μητρώου, η αναφορά απολεσθέντων αντικειμένων και η υποβολή καταγγελιών μέσω διαδικτύου, η Ελληνική Αστυνομία έχει απλοποιήσει διαδικασίες που κάποτε απαιτούσαν φυσικές επισκέψεις στα αστυνομικά τμήματα. Για παράδειγμα, οι πολίτες που αναζητούν ποινικό μητρώο για λόγους απασχόλησης μπορούν πλέον να ολοκληρώσουν τη διαδικασία ηλεκτρονικά, εξοικονομώντας χρόνο και μειώνοντας την επιβάρυνση του αστυνομικού προσωπικού (Dimitrelou & Fouskas, 2023).

Αυτή η έμφαση στην ψηφιακή προσβασιμότητα όχι μόνο βελτιώνει την ευκολία για τους πολίτες αλλά και ανακουφίζει τις διοικητικές ευθύνες εντός του αστυνομικού τμήματος. Η μείωση των ατόμων που προσέρχονται στα αστυνομικά τμήματα για πεζά ζητήματα επιτρέπει στους αστυνομικούς να επικεντρωθούν σε πιο επείγουσες αρμοδιότητες, όπως η διερεύνηση

εγκλημάτων και η διατήρηση της δημόσιας τάξης. Επιπλέον, οι ψηφιακές υπηρεσίες που παρέχονται μέσω του GOV.GR αποτελούν παράδειγμα αφοσίωσης στη διαφάνεια και τη λογοδοσία. Η Ελληνική Αστυνομία έχει ενισχύσει την εμπιστοσύνη στις δραστηριότητές της δίνοντας στους κατοίκους τη δυνατότητα να παρακολουθούν την κατάσταση των αιτημάτων τους ηλεκτρονικά (Dimitrelou & Fouskas, 2023).

Η συμμόρφωση με τον Γενικό Κανονισμό της Ευρωπαϊκής Ένωσης για την Προστασία Δεδομένων (GDPR) αποτελεί έναν ακόμη ακρογωνιαίο λίθο των προσπαθειών της Ελληνικής Αστυνομίας για την ηλεκτρονική διακυβέρνηση. Το εν λόγω κανονιστικό πλαίσιο επιβάλλει αυστηρά πρωτόκολλα προστασίας δεδομένων, εξασφαλίζοντας την ασφαλή διαχείριση των προσωπικών πληροφοριών των πολιτών και του αστυνομικού προσωπικού. Με την τήρηση των προτύπων του GDPR, η Ελληνική Αστυνομία όχι μόνο διασφαλίζει τα ευαίσθητα δεδομένα, αλλά και σηματοδοτεί τη δέσμευσή της για σεβασμό της ιδιωτικής ζωής και ηθική διακυβέρνηση. Η συμμόρφωση αυτή ενισχύει την εμπιστοσύνη του κοινού στα ψηφιακά συστήματα του οργανισμού, καθώς οι πολίτες διαβεβαιώνονται ότι οι πληροφορίες τους προστατεύονται από κακή χρήση ή μη εξουσιοδοτημένη πρόσβαση (Sarifudin & Damanik, 2024).

Η ενσωμάτωση έξυπνων συσκευών και εφαρμογών για κινητά τηλέφωνα έχει ενισχύσει την αποτελεσματικότητα της λειτουργίας της Ελληνικής Αστυνομίας. Οι αξιωματικοί που χρησιμοποιούν smartphones, tablets και άλλες κινητές συσκευές μπορούν να εκτελούν ένα ευρύ φάσμα δραστηριοτήτων εξ αποστάσεως. Για παράδειγμα, μπορούν να οριστικοποιούν αναφορές περιστατικών, να ανακτούν βασικά δεδομένα και να συμμετέχουν σε ασφαλή επικοινωνία με τους συναδέλφους τους ενώ βρίσκονται στο πεδίο. Αυτές οι λειτουργίες εγγυώνται ότι οι αστυνομικοί παραμένουν συνδεδεμένοι και αποτελεσματικοί, ακόμη και όταν λειτουργούν σε απομακρυσμένες ή δύσκολες τοποθεσίες. Η ενσωμάτωση της κινητής τεχνολογίας στις τακτικές επιχειρήσεις βελτίωσε την αποτελεσματικότητα και επέτρεψε στην Ελληνική Αστυνομία να ανταποκρίνεται πιο προσαρμοστικά στις εξελισσόμενες συνθήκες (Sarifudin & Damanik, 2024).

Η προσέγγιση της Ελληνικής Αστυνομίας για την ηλεκτρονική διακυβέρνηση στηρίζεται σε μια σταθερή υποδομή πληροφορικής, τεχνολογίες αιχμής και υπηρεσίες με επίκεντρο τον πολίτη. Το δίκτυο «Police On Line», τα καινοτόμα συστήματα Car-PC και οι τεχνολογίες βιομετρικής ταυτοποίησης έχουν φέρει επανάσταση στις λειτουργίες του οργανισμού, ενισχύοντας την αποτελεσματικότητα, τη διαφάνεια και την ανταπόκριση. Αξιοποιώντας αυτά

τα περιουσιακά στοιχεία, η Ελληνική Αστυνομία είναι κατάλληλα εξοπλισμένη για να αντιμετωπίσει τα προβλήματα της σύγχρονης επιβολής του νόμου και να καλλιεργήσει περαιτέρω την εμπιστοσύνη με τις κοινότητες που υπηρετεί (Yamin et al., 2020).

### 3.2. Αδυναμίες

Παρά τις δυνατότητες αυτές, ορισμένα εσωτερικά εμπόδια εμποδίζουν την πλήρη αξιοποίηση του δυναμικού της ηλεκτρονικής διακυβέρνησης στην Ελληνική Αστυνομία. Ένα αξιοσημείωτο τρωτό σημείο είναι η εξάρτηση από ξεπερασμένη τεχνολογία για συγκεκριμένες υπηρεσίες και βάσεις δεδομένων. Ένα πλήθος από αυτά τα παλαιά συστήματα είναι ασύμβατα με τις σύγχρονες πλατφόρμες, με αποτέλεσμα να δημιουργούνται συμφόρηση και λειτουργικές ανεπάρκειες. Για παράδειγμα, αν και η πλειονότητα των υπηρεσιών προς τους πολίτες είναι διαθέσιμες μέσω της πύλης GOV.GR, ορισμένες δυνατότητες στέλνουν τους χρήστες σε παρωχημένα συστήματα, προκαλώντας απογοήτευση τόσο στους χρήστες όσο και στο εσωτερικό προσωπικό. Η συνέχιση αυτών των παλαιών συστημάτων παρεμποδίζει την ομαλή ενσωμάτωση που αναμένουν οι πρωτοβουλίες ηλεκτρονικής διακυβέρνησης (Dimitrelou & Fouskas, 2023).

Μια άλλη σημαντική ανησυχία είναι η περιορισμένη υιοθέτηση των νέων τεχνολογιών από το προσωπικό. Μια κουλτούρα αντίστασης στην αλλαγή, σε συνδυασμό με ανεπαρκή προγράμματα κατάρτισης, εμποδίζει την αποτελεσματική αξιοποίηση των προηγμένων εργαλείων. Πολλοί αξιωματικοί, ιδίως εκείνοι που είναι συνηθισμένοι στις παραδοσιακές ροές εργασίας, δυσκολεύονται να προσαρμοστούν στις ψηφιακές μεθόδους. Για παράδειγμα, η ελλιπής αξιοποίηση προηγμένων εφαρμογών, όπως η προγνωστική ανάλυση ή τα εργαλεία που βασίζονται στην τεχνητή νοημοσύνη, αντανακλά το έλλειμμα δεξιοτήτων εντός του οργανισμού. Χωρίς ολοκληρωμένα προγράμματα κατάρτισης και διαχείρισης αλλαγών, τα οφέλη αυτών των τεχνολογιών παραμένουν ανεκμετάλλευτα (Abhay et al., 2023).

Η εξάρτηση από τον προμηθευτή αποτελεί ευπάθεια που θέτει τον οργανισμό σε πιθανούς κινδύνους. Η Ελληνική Αστυνομία εξαρτάται σημαντικά από ξένους προμηθευτές τεχνολογίας, συμπεριλαμβανομένων των Intracom Telecom και VMware, για βασικά συστήματα πληροφορικής και συντήρηση. Η εξάρτηση αυτή αυξάνει τον κίνδυνο εγκλωβισμού σε προμηθευτές, κατά τον οποίο η εταιρεία εξαρτάται από συγκεκριμένους παρόχους για

ενημερώσεις, αντιμετώπιση προβλημάτων και τεχνολογικές βελτιώσεις. Αυτή η εξάρτηση μπορεί να οδηγήσει σε αυξημένες δαπάνες και περιορισμένη προσαρμοστικότητα στην εφαρμογή εναλλακτικών λύσεων (Abhay et al., 2023).

Η ευαισθητοποίηση του κοινού για τις σημαντικές προσπάθειες εξακολουθεί να αποτελεί εμπόδιο. Η εφαρμογή «Panic Button» αποτελεί βασικό πόρο για την καταπολέμηση της ενδοοικογενειακής κακοποίησης- ωστόσο, η αποτελεσματικότητά της περιορίζεται από την ανεπαρκή γνώση των μελλοντικών χρηστών. Ένα σημαντικό τμήμα του πληθυσμού εξακολουθεί να αγνοεί την ύπαρξή της ή την εφαρμογή της σε καταστάσεις έκτακτης ανάγκης. Τελικά, παρά τη συμμόρφωσή τους με τον ΓΚΠΔ και άλλα μέτρα ασφαλείας, ο κίνδυνος παραβίασης δεδομένων και επιθέσεων παραμένει. Μια παραβίαση ευαίσθητων δεδομένων της αστυνομίας ή των πολιτών θα μπορούσε να υπονομεύσει σημαντικά την εμπιστοσύνη του κοινού και τη φήμη της Ελληνικής Αστυνομίας (Abhay et al., 2023).

### **3.3. Ευκαιρίες**

Το εξελισσόμενο τεχνολογικό τοπίο προσφέρει διάφορες ευκαιρίες στην Ελληνική Αστυνομία να βελτιώσει τις υπηρεσίες ηλεκτρονικής διακυβέρνησης και να ενσωματωθεί αποτελεσματικότερα στις απαιτήσεις μιας σύγχρονης, ψηφιακά διασυνδεδεμένης κοινωνίας. Οι προοπτικές αυτές περιλαμβάνουν όχι μόνο την εσωτερική αποτελεσματικότητα, αλλά και την ενίσχυση της εμπλοκής των πολιτών, την ενίσχυση της δημόσιας εμπιστοσύνης και τη βελτίωση της γενικής ασφάλειας. Σημαντική ευκαιρία ανάπτυξης υπάρχει στην ενίσχυση των ψηφιακών υπηρεσιών που παρέχονται απευθείας μέσω της πλατφόρμας GOV.GR. Αυτός ο κυβερνητικός ιστότοπος λειτουργεί ως κεντρικό κέντρο για τις δημόσιες υπηρεσίες και η ενσωμάτωση όλων των υπηρεσιών που σχετίζονται με την αστυνομία σε αυτή την πλατφόρμα θα βελτιώσει σημαντικά την προσβασιμότητα και την ευκολία των χρηστών. Επί του παρόντος, πολλές υπηρεσίες της αστυνομίας είναι προσβάσιμες διαδικτυακά- ωστόσο, ορισμένες απαιτούν από τους πελάτες να εμπλακούν με απαρχαιωμένα συστήματα ή να επισκεφθούν φυσικούς χώρους για συγκεκριμένες διαδικασίες. Μια εκτεταμένη ενσωμάτωση θα βελτιστοποιήσει αυτές τις αλληλεπιδράσεις, παρέχοντας στους πολίτες μια συνεκτική, ενιαία εμπειρία (Dimitrelou & Fouskas, 2023).

Για παράδειγμα, υπηρεσίες όπως η καταγγελία μικροπαραβάσεων, η ανανέωση αδειών ή η υποβολή αιτήσεων για άδειες θα μπορούσαν να ψηφιοποιηθούν και να συνδεθούν απρόσκοπτα με το GOV.GR. Η ενέργεια αυτή όχι μόνο θα εξοικονομούσε χρόνο για τους πολίτες, αλλά και θα ανακούφιζε τις διοικητικές υποχρεώσεις των υπαλλήλων επιβολής του νόμου. Επιπλέον, η ενσωμάτωση εξελιγμένων μέτρων ασφαλείας σε αυτές τις ψηφιακές υπηρεσίες, όπως ο έλεγχος ταυτότητας δύο παραγόντων ή η επαλήθευση δεδομένων με βάση την αλυσίδα μπλοκ, θα μπορούσε να ενισχύσει την εμπιστοσύνη του κοινού στην ασφάλεια και την αξιοπιστία της πλατφόρμας. Αυτές οι αλλαγές θα προωθούσαν την αυξημένη χρήση των ψηφιακών υπηρεσιών, προωθώντας τους στόχους της Ελληνικής Αστυνομίας για την ηλεκτρονική διακυβέρνηση (Dimitrelou & Fouskas, 2023).

Η δημιουργία νέων ψηφιακών ταυτοτήτων προσφέρει μια πρόσθετη ευκαιρία για την ενίσχυση της προσβασιμότητας και της εμπιστοσύνης. Οι ψηφιακές ταυτότητες που περιλαμβάνουν ενισχυμένα πρωτόκολλα ασφαλείας -όπως βιομετρική επαλήθευση και κρυπτογραφημένη αποθήκευση- μπορούν να διευκολύνουν τις αλληλεπιδράσεις μεταξύ των ατόμων και των αρχών επιβολής του νόμου. Οι ταυτότητες αυτές θα μπορούσαν να λειτουργήσουν ως ασφαλής μέθοδος για την πρόσβαση των χρηστών στις αστυνομικές υπηρεσίες, την πιστοποίηση της ταυτότητάς τους κατά τη διάρκεια διαδικτυακών συνομιλιών ή τη συμμετοχή σε εικονικές δικαστικές διαδικασίες. Αξιοποιώντας αυτές τις εξελίξεις, η Ελληνική Αστυνομία μπορεί να καθιερωθεί ως πρωτοπόρος στον ψηφιακό μετασχηματισμό στον δημόσιο τομέα (Sarifudin & Damanik, 2024).

Η δημιουργία ενός κεντρικού συστήματος διαχείρισης ανθρώπινου δυναμικού (HRMS) στο εσωτερικό της παρουσιάζει σημαντικές ευκαιρίες για την ενίσχυση της διοικητικής αποτελεσματικότητας και τη βελτιστοποίηση της κατανομής των πόρων. Επί του παρόντος, πολυάριθμες λειτουργίες ανθρώπινου δυναμικού, συμπεριλαμβανομένης της επεξεργασίας μισθοδοσίας, του προγραμματισμού και των αξιολογήσεων επιδόσεων, διαχειρίζονται μέσω αποσπασματικών ή χειροκίνητων μεθόδων. Αυτή η αποκέντρωση οδηγεί συχνά σε αναποτελεσματικότητα, καθυστερήσεις και σφάλματα, τα οποία μπορούν να εμποδίσουν την επιχειρησιακή αποτελεσματικότητα της αστυνομικής δύναμης. Ένα ενοποιημένο HRMS θα αυτοματοποιούσε αυτές τις λειτουργίες, προσφέροντας μια συνεκτική πλατφόρμα για τη διαχείριση των δραστηριοτήτων που σχετίζονται με το προσωπικό. Οι αστυνομικοί μπορούν να χρησιμοποιούν το σύστημα για να υποβάλλουν αιτήσεις αδειών, να εξετάζουν τα ημερολόγια τους ή να έχουν πρόσβαση σε πόρους κατάρτισης, όλα από ένα ενιαίο περιβάλλον

εργασίας. Οι προϊστάμενοι θα μπορούσαν να χρησιμοποιούν την πλατφόρμα για να αξιολογούν την απόδοση της ομάδας, να παρακολουθούν την εξέλιξη της κατάρτισης και να δαπανούν τους πόρους με μεγαλύτερη σύνεση. Με την ελάφρυνση του διοικητικού φόρτου, ένα τέτοιο σύστημα θα επιτρέψει στην Ελληνική Αστυνομία να επικεντρωθεί περισσότερο στον πρωταρχικό της στόχο, δηλαδή τη διασφάλιση της δημόσιας ασφάλειας και τάξης. Επιπλέον, ένα HRMS μπορεί να συνδεθεί με τεχνολογίες προγνωστικής ανάλυσης για την ενίσχυση του προγραμματισμού της εργασίας. Μέσω της ανάλυσης των τάσεων των δεδομένων προσωπικού, συμπεριλαμβανομένων των ποσοστών συνταξιοδότησης και των μοτίβων αποχώρησης, η Ελληνική Αστυνομία θα μπορούσε να προβλέψει τις ανάγκες σε προσωπικό και να μετριάσει προληπτικά τυχόν ελλείψεις. Αυτή η δεξιότητα θα ήταν ιδιαίτερα επωφελής για τη διασφάλιση ότι η εταιρεία είναι επαρκώς στελεχωμένη για την αντιμετώπιση μελλοντικών δυσκολιών, όπως η αύξηση του εγκλήματος στον κυβερνοχώρο και οι αναδυόμενες απειλές για την ασφάλεια (Sarifudin & Damanik, 2024).

Οι τεχνολογικές βελτιώσεις δημιουργούν ένα βέλτιστο περιβάλλον για την ενίσχυση των προγραμμάτων «έξυπνης αστυνόμευσης» που χρησιμοποιούν μεθοδολογίες βασισμένες σε δεδομένα για την ενίσχυση της πρόληψης του εγκλήματος και της κατανομής των πόρων. Ένας πολλά υποσχόμενος τομέας είναι η ενσωμάτωση των συσκευών του Διαδικτύου των Πραγμάτων (IoT). Η τεχνολογία του Διαδικτύου των Πραγμάτων (IoT) μπορεί να φέρει επανάσταση στην παρακολούθηση και την ανταπόκριση της Ελληνικής Αστυνομίας σε περιστατικά. Για παράδειγμα, ευφυείς αισθητήρες που αναπτύσσονται σε δημόσιους χώρους θα μπορούσαν να εντοπίζουν ανώμαλη συμπεριφορά, όπως παράνομη είσοδο σε απαγορευμένες ζώνες ή απότομες αυξήσεις στα επίπεδα θορύβου, και να ειδοποιούν άμεσα τις αρχές (Yamin et al., 2020).

Η προγνωστική ανάλυση χρησιμεύει ως ένα τρομερό εργαλείο που μπορεί να ενισχύσει τις πρωτοβουλίες «έξυπνης αστυνόμευσης». Μέσω της ανάλυσης ποικίλων πηγών δεδομένων, συμπεριλαμβανομένων ιστορικών αρχείων εγκληματικότητας, κοινωνικοοικονομικών μεταβλητών και δεδομένων αισθητήρων σε πραγματικό χρόνο, τα μοντέλα πρόβλεψης μπορούν να εντοπίσουν τα μελλοντικά hotspots για εγκληματική δραστηριότητα. Οι πληροφορίες αυτές επιτρέπουν στην αστυνομία να κατανέμει τους πόρους πιο συνετά, εστιάζοντας σε περιοχές υψηλού κινδύνου. Για παράδειγμα, κατά τη διάρκεια σημαντικών δημόσιων εκδηλώσεων, οι αναλύσεις πρόβλεψης μπορούν να βοηθήσουν στον εντοπισμό των

περιοχών που απαιτούν μέτρα διαχείρισης του πλήθους, μειώνοντας έτσι την πιθανότητα διαταραχών ή ανησυχιών για την ασφάλεια (Yamin et al., 2020).

Η γεωχωρική χαρτογράφηση είναι μια τεχνική που έχει δυνατότητες βελτίωσης της επιχειρησιακής αποτελεσματικότητας. Μέσω της απεικόνισης των δεδομένων εγκληματικότητας σε διαδραστικούς χάρτες, η Ελληνική Αστυνομία μπορεί να διακρίνει μοτίβα και τάσεις που μπορεί να μην είναι άμεσα εμφανείς από μη επεξεργασμένα δεδομένα. Αυτή η ικανότητα μπορεί να αξιοποιηθεί για διάφορους σκοπούς, όπως ο σχεδιασμός των διαδρομών περιπολίας και ο σχεδιασμός προσαρμοσμένων παρεμβάσεων για συγκεκριμένες κοινότητες. Για παράδειγμα, εάν μια συγκεκριμένη περιοχή αντιμετωπίζει επίμονα υψηλή συχνότητα διαρρήξεων, η γεωχωρική ανάλυση θα μπορούσε να βοηθήσει στον εντοπισμό βέλτιστων τοποθεσιών για κάμερες ασφαλείας ή πρωτοβουλίες εμπλοκής της κοινότητας (Sarifudin & Damanik, 2024).

Η αυξανόμενη ανάγκη για ψηφιακές και αποτελεσματικές δημόσιες υπηρεσίες συμβαδίζει στενά με τους στόχους της ηλεκτρονικής διακυβέρνησης της Ελληνικής Αστυνομίας. Οι πολίτες προσδοκούν όλο και περισσότερο να αλληλεπιδρούν με τους δημόσιους φορείς μέσω διαισθητικών ψηφιακών καναλιών και η εκπλήρωση αυτών των προσδοκιών προσφέρει σημαντικές δυνατότητες για την Ελληνική Αστυνομία. Η εφαρμογή άλλων εφαρμογών με επίκεντρο τον πολίτη, όπως η αναφορά εγκλημάτων σε πραγματικό χρόνο και οι εικονικές υπηρεσίες διαβούλευσης, θα μπορούσαν να ενισχύσουν περαιτέρω τη συμμετοχή και την εμπιστοσύνη του κοινού. Οι εφαρμογές αναφοράς εγκλημάτων σε πραγματικό χρόνο θα επέτρεπαν στους χρήστες να αναφέρουν άμεσα περιστατικά από τα κινητά τους τηλέφωνα, παρέχοντας γεγονότα, φωτογραφίες ή βίντεο που θα μπορούσαν να βοηθήσουν τις έρευνες. Τα εργαλεία αυτά όχι μόνο δίνουν τη δυνατότητα στους πολίτες να ενισχύσουν τη δημόσια ασφάλεια αλλά και να αυξήσουν την αποτελεσματικότητα και την ακρίβεια των αστυνομικών αντιδράσεων. Αντίθετα, οι εικονικές υπηρεσίες διαβούλευσης μπορούν να επιτρέψουν στους πολίτες να λάβουν συμβουλές ή διευκρινίσεις για μη επείγοντα ζητήματα, όπως νομικές διατάξεις για συγκεκριμένες άδειες ή συμβουλές για την καταγγελία συγκεκριμένων αδικημάτων. Αυτές οι εικονικές επαφές μπορούν να πραγματοποιηθούν μέσω ασφαλών βιντεοκλήσεων ή chatbots, ελαχιστοποιώντας την ανάγκη για φυσικές επισκέψεις σε αστυνομικά τμήματα (Maliphol & Hamilton, 2022).

Η συνεργασία με προγράμματα και χρηματοδοτικά έργα της Ευρωπαϊκής Ένωσης (ΕΕ) αποτελεί σημαντική ευκαιρία για την ενίσχυση των προσπαθειών ψηφιακού μετασχηματισμού

της Ελληνικής Αστυνομίας. Η ΕΕ κατανέμει σταθερά οικονομικούς πόρους και τεχνικές γνώσεις στα κράτη μέλη για πρωτοβουλίες που αποσκοπούν στην ενίσχυση των δημόσιων υπηρεσιών και την προώθηση της καινοτομίας. Μέσω της ενεργού συμμετοχής σε αυτά τα προγράμματα, η Ελληνική Αστυνομία μπορεί να εξασφαλίσει χρήματα για δραστηριότητες όπως η βελτίωση της ασφάλειας στον κυβερνοχώρο, η έρευνα για την τεχνητή νοημοσύνη και η ενσωμάτωση έξυπνων πόλεων (Maliphol & Hamilton, 2022).

Εκτός από την οικονομική βοήθεια, η εταιρική σχέση της ΕΕ διευκολύνει την ανταλλαγή εμπειρογνομοσύνης και βέλτιστων πρακτικών μεταξύ των κρατών μελών. Η Ελληνική Αστυνομία θα μπορούσε να επωφεληθεί από τις εμπειρίες εθνών που έχουν εκτελέσει αποτελεσματικά ανάλογες πρωτοβουλίες ηλεκτρονικής διακυβέρνησης, παρακάμπτοντας έτσι πιθανές προκλήσεις και επιταχύνοντας την πρόοδό τους. Οι συνεργασίες με ερευνητικά ιδρύματα της ΕΕ μπορούν να ενισχύσουν τη δημιουργία προηγμένης τεχνολογίας ειδικά σχεδιασμένης για τις ιδιαίτερες απαιτήσεις της ελληνικής αστυνομίας (Maliphol & Hamilton, 2022).

Κοινωνικές ανησυχίες, όπως ο μετριασμός της ενδοοικογενειακής βίας και η προστασία των ευάλωτων πληθυσμών, παρουσιάζουν δυνατότητες για την Ελληνική Αστυνομία να ενισχύσει τη συμμετοχή της στην ασφάλεια της κοινωνίας. Ψηφιακά εργαλεία όπως η εφαρμογή «Panic Button», που προορίζεται να βοηθήσει τα θύματα ενδοοικογενειακής βίας, σηματοδοτούν μια ζωτική πρόοδο στον τομέα αυτό. Η αποτελεσματικότητα αυτών των τεχνολογιών εξαρτάται από την έκθεση και την προσβασιμότητά τους. Η ενίσχυση και η υποστήριξη της εφαρμογής «Panic Button» μέσω πρωτοβουλιών ευαισθητοποίησης του κοινού, συνεργασιών με ΜΚΟ και η ενσωμάτωση στις τρέχουσες κοινωνικές υπηρεσίες μπορεί να αυξήσει τη χρήση και την αποτελεσματικότητά της (Maliphol & Hamilton, 2022).

Ομοίως, η Ελληνική Αστυνομία μπορεί να αξιοποιήσει την τεχνολογία για τη βελτίωση των πρωτοβουλιών για την ασφάλεια των παιδιών. Η δημιουργία μιας εξειδικευμένης πλατφόρμας για την αναφορά και διερεύνηση περιστατικών κακοποίησης παιδιών θα μπορούσε να βελτιώσει την αποτελεσματικότητα και τα αποτελέσματα. Η πλατφόρμα αυτή μπορεί να ενσωματώσει λειτουργίες όπως η ανώνυμη αναφορά, η ασφαλής αποθήκευση δεδομένων και η επικοινωνία σε πραγματικό χρόνο μεταξύ των αρχών επιβολής του νόμου και της παιδικής πρόνοιας. Αντιμετωπίζοντας αυτές τις επείγουσες κοινωνικές προκλήσεις με καινοτόμες ψηφιακές λύσεις, η Ελληνική Αστυνομία μπορεί να ενισχύσει την αφοσίωσή της στην προστασία των πιο ευάλωτων τμημάτων της κοινωνίας (Sarifudin & Damanik, 2024).

Οι εξελίξεις στην τεχνολογία παρέχουν στην Ελληνική Αστυνομία μια ξεχωριστή ευκαιρία να βελτιώσει τις υπηρεσίες ηλεκτρονικής διακυβέρνησης και να ενισχύσει τη δέσμευση του κοινού. Οι δυνατότητες είναι εκτεταμένες και κυμαίνονται από την ενίσχυση των ψηφιακών υπηρεσιών μέσω του GOV.GR έως την αξιοποίηση σύγχρονων τεχνολογιών όπως το IoT και η προγνωστική ανάλυση. Αξιοποιώντας αυτές τις ευκαιρίες και ευθυγραμμίζοντας τις ενέργειές της με τα κοινωνικά συμφέροντα και τις οδηγίες της ΕΕ, η Ελληνική Αστυνομία μπορεί να τοποθετηθεί ως μια σύγχρονη, καινοτόμα και πολίτη-κεντρική υπηρεσία επιβολής του νόμου. Μέσω του στρατηγικού σχεδιασμού και της συνεχούς βελτίωσης, οι ευκαιρίες αυτές μπορούν να μετατραπούν σε συγκεκριμένα πλεονεκτήματα τόσο για τον οργανισμό όσο και για τις κοινότητες που υπηρετεί (Sarifudin & Damanik, 2024).

### **3.4. Κίνδυνοι – Απειλές**

Η εκτέλεση των υπηρεσιών ηλεκτρονικής διακυβέρνησης αντιμετωπίζει πολλά προβλήματα, καθώς τόσο εξωτερικοί όσο και εσωτερικοί κίνδυνοι θέτουν σε κίνδυνο τις πρωτοβουλίες ψηφιακού μετασχηματισμού της Ελληνικής Αστυνομίας. Μια σημαντική απειλή είναι η αυξανόμενη πολυπλοκότητα και το κόστος που σχετίζονται με τη συντήρηση εξελιγμένων συστημάτων ΤΠ. Καθώς οι τεχνολογίες εξελίσσονται ταχύτατα, η Ελληνική Αστυνομία πρέπει να διαθέσει πόρους για συνεχείς βελτιώσεις και συντήρηση για να διατηρήσει την αποτελεσματικότητά της. Οι επενδύσεις αυτές μπορεί να ασκήσουν πίεση στους οικονομικούς και ανθρώπινους πόρους, ιδίως σε περιόδους οικονομικής δυσπραγίας. Οι κίνδυνοι κυβερνοασφάλειας αποτελούν σημαντικό κίνδυνο. Παρά τις αυστηρές προφυλάξεις και την τήρηση του ΓΚΠΔ, προηγμένες κυβερνοεπιθέσεις με στόχο κρίσιμες βάσεις δεδομένων της αστυνομίας μπορεί να οδηγήσουν σε λειτουργικές διακοπές και βλάβη της φήμης. Αξιοσημείωτες παραβιάσεις δεδομένων, ιδίως εκείνες που αφορούν προσωπικές πληροφορίες, μπορεί να υπονομεύσουν την εμπιστοσύνη του κοινού και να έχουν σημαντικές νομικές και οικονομικές επιπτώσεις για την επιχείρηση (Yamin et al., 2020).

Ο σκεπτικισμός του κοινού όσον αφορά τις ανησυχίες για την προστασία της ιδιωτικής ζωής με τις βιομετρικές τεχνολογίες και τις τεχνολογίες επιτήρησης είναι μια άλλη πρόκληση. Ενώ τα εργαλεία αυτά ενισχύουν την ασφάλεια και την επιχειρησιακή αποτελεσματικότητα, εγείρουν επίσης ηθικά ζητήματα σχετικά με τη χρήση των δεδομένων και τα δικαιώματα των

πολιτών. Για παράδειγμα, οι επικριτές των τεχνολογιών αναγνώρισης προσώπου συχνά αναφέρουν ανησυχίες για πιθανή κατάχρηση, φυλετική προκατάληψη ή μη εξουσιοδοτημένη παρακολούθηση. Η οικοδόμηση και η διατήρηση της εμπιστοσύνης του κοινού μέσω διαφανών πολιτικών και μηχανισμών λογοδοσίας είναι απαραίτητη για την αντιμετώπιση αυτών των προκλήσεων (Yamin et al., 2020).

Η αντίσταση στην αλλαγή μεταξύ των αστυνομικών επιβολής του νόμου επιδεινώνει την εφαρμογή των νέων τεχνολογιών. Οι καθιερωμένοι πολιτισμικοί κανόνες και η εξάρτηση από συμβατικές διαδικασίες μπορεί να εμποδίσουν την απρόσκοπτη ενσωμάτωση ψηφιακών λύσεων. Ελλείψει κατάλληλων εκπαιδευτικών προγραμμάτων και κινήτρων για την υιοθέτηση, οι τεχνολογίες αυτές είναι πιθανό να μην αξιοποιηθούν επαρκώς ή ακόμη και να απορριφθούν (Yamin et al., 2020).

Τα νομικά και κανονιστικά εμπόδια μπορούν να θέσουν σε κίνδυνο την ομοιομορφία της χρήσης της τεχνολογίας μεταξύ των οργανισμών. Οι αποκλίσεις στα νομοθετικά πλαίσια μεταξύ περιφερειών ή οργανισμών μπορεί να δημιουργήσουν διαφορές, παρεμποδίζοντας τη συνεργασία και δυσχεραίνοντας την εκτέλεση πρωτοβουλιών ηλεκτρονικής διακυβέρνησης. Η εξάρτηση από εξωτερικούς προμηθευτές για βασικά συστήματα αυξάνει την ευαισθησία σε διακοπές της αλυσίδας εφοδιασμού. Καθυστερήσεις στις ενημερώσεις λογισμικού ή στην παράδοση υλικού μπορεί να οδηγήσουν σε λειτουργικές συμφορήσεις, θέτοντας σε κίνδυνο την αποτελεσματικότητα των αστυνομικών υπηρεσιών (Yamin et al., 2020).

**Πίνακας 3.1**  
**Ανάλυση SWOT**

	ΘΕΤΙΚΑ	ΑΡΝΗΤΙΚΑ
ΕΣΩΤΕΡΙΚΟ ΠΕΡΙΒΑΛΛΟΝ	<p>Δυνατά σημεία (Strengths)</p> <ul style="list-style-type: none"> <li>• Προηγμένη υποδομή ΤΠ (π.χ. δίκτυο Police On Line).</li> <li>• Ενσωμάτωση σύγχρονων εφαρμογών, όπως το σύστημα «Ηλεκτρονική Αλληλογραφία», που βελτιώνει τη διαχείριση εγγράφων και μειώνει τη γραφειοκρατία.</li> <li>• Δυνατότητες πραγματικού χρόνου των περιπολικών οχημάτων με συστήματα Car-PC.</li> <li>• Πρόσβαση σε πολλαπλές εθνικές και διεθνείς βάσεις δεδομένων για αποτελεσματική ανάκτηση δεδομένων.</li> <li>• Ανάπτυξη καινοτόμων υπηρεσιών όπως η «έξυπνη αστυνόμευση» και τα εργαλεία βιομετρικής ταυτοποίησης.</li> <li>• Εισαγωγή ψηφιακών υπηρεσιών με επίκεντρο τον πολίτη μέσω του GOV.GR.</li> <li>• Συμμόρφωση με τα ευρωπαϊκά πρότυπα προστασίας δεδομένων (GDPR).</li> <li>• Βελτίωση της επιχειρησιακής αποτελεσματικότητας και ενίσχυση της ασφάλειας των αστυνομικών με έξυπνες συσκευές.</li> </ul>	<p>Αδύναμα σημεία (Weaknesses)</p> <ul style="list-style-type: none"> <li>• Εξάρτηση από παλαιά συστήματα για ορισμένες υπηρεσίες και βάσεις δεδομένων.</li> <li>• Προκλήσεις όσον αφορά την υιοθέτηση από τους χρήστες και την εκπαίδευση για τις νέες τεχνολογίες από το προσωπικό.</li> <li>• Μεγάλη εξάρτηση από εξωτερικούς παρόχους τεχνολογίας (π.χ. Intracom Telecom, VMWare).</li> <li>• Περιορισμένη ευαισθητοποίηση και προσβασιμότητα του κοινού για προηγμένες υπηρεσίες όπως το «κουμπί πανικού».</li> <li>• Κίνδυνος παραβίασης δεδομένων παρά τα μέτρα ασφαλείας.</li> </ul>

### Πίνακας 3.1

#### Συνέχεια

ΕΞΩΤΕΡΙΚΟ ΠΕΡΙΒΑΛΛΟΝ	Ευκαιρίες (Opportunities)	Απειλές (Threats)
	<ul style="list-style-type: none"><li>• Επέκταση των ψηφιακών υπηρεσιών απευθείας μέσω του GOV.GR.</li><li>• Έκδοση νέων ψηφιακών ταυτοτήτων για τη βελτίωση της ασφάλειας και της ευκολίας χρήσης.</li><li>• Κεντρικό σύστημα διαχείρισης ανθρώπινου δυναμικού για εξορθολογισμό των διοικητικών διαδικασιών.</li><li>• Τεχνολογικές εξελίξεις για την ενίσχυση της έξυπνης αστυνόμευσης και των επιχειρήσεων πεδίου.</li><li>• Αυξανόμενη ζήτηση των πολιτών για ψηφιακές και αποτελεσματικές δημόσιες υπηρεσίες.</li><li>• Ενισχυμένη συνεργασία με προγράμματα της Ευρωπαϊκής Ένωσης και ευκαιρίες χρηματοδότησης.</li><li>• Κοινωνική εστίαση στην αντιμετώπιση της ενδοοικογενειακής βίας και της προστασίας των παιδιών μέσω εφαρμογών όπως το κουμπί πανικού.</li></ul>	<ul style="list-style-type: none"><li>• Αυξανόμενη πολυπλοκότητα και κόστος συντήρησης προηγμένων συστημάτων ΤΠ.</li><li>• Κίνδυνος κυβερνοεπιθέσεων με στόχο ευαίσθητα αστυνομικά δεδομένα.</li><li>• Σκεπτικισμός του κοινού όσον αφορά τις ανησυχίες για την προστασία της ιδιωτικής ζωής με τις βιομετρικές τεχνολογίες και τις τεχνολογίες επιτήρησης.</li><li>• Αντίσταση στην αλλαγή μεταξύ του προσωπικού που έχει συνηθίσει σε παραδοσιακές μεθόδους.</li><li>• Προκλήσεις στην εναρμόνιση των νομικών πλαισίων για τη χρήση της τεχνολογίας σε όλες τις υπηρεσίες.</li><li>• Οικονομικοί περιορισμοί που ενδεχομένως περιορίζουν περαιτέρω τεχνολογικές αναβαθμίσεις.</li><li>• Εξάρτηση από εξωτερικούς προμηθευτές για κρίσιμα στοιχεία και ενημερώσεις του συστήματος.</li></ul>

## ΚΕΦΑΛΑΙΟ 4: Πρακτικές από χώρες της Ε.Ε. και διεθνώς

Εξετάζονται διάφορες ψηφιακές εφαρμογές που έχουν αναπτυχθεί από τις υπηρεσίες επιβολής του νόμου παγκοσμίως για την ενίσχυση της δημόσιας ασφάλειας, τη βελτίωση της επικοινωνίας και τη διευκόλυνση της αναφοράς εγκλημάτων. Οι εφαρμογές αυτές χρησιμεύουν ως εργαλεία για τους πολίτες ώστε να επικοινωνούν με τις τοπικές αστυνομικές δυνάμεις, να αναφέρουν περιστατικά, να λαμβάνουν ειδοποιήσεις ασφαλείας και να έχουν πρόσβαση σε πηγές πρόληψης του εγκλήματος. Οι εφαρμογές που καλύπτονται σε αυτό το κεφάλαιο περιλαμβάνουν:

- Ολλανδία - *Check Your Hack*
- Ηνωμένο Βασίλειο - *Police.UK*
- Ισπανία - *AlertCops*
- Καναδά - *TPS Mobile*
- Σιγκαπούρη - *Police@SG*
- Ηνωμένες Πολιτείες - *MyPD*

### 4.1. Εφαρμογή «Check Your Hack» – Ολλανδία

Η Ολλανδική Αστυνομία προσφέρει ένα πολύτιμο διαδικτυακό εργαλείο με την ονομασία «Check Your Hack», το οποίο έχει σχεδιαστεί για να βοηθήσει τους πολίτες να προσδιορίσουν εάν οι διευθύνσεις ηλεκτρονικού ταχυδρομείου τους έχουν εκτεθεί σε εγκληματικές παραβιάσεις δεδομένων. Η πρωτοβουλία αυτή εντάσσεται στο πλαίσιο των ευρύτερων προσπαθειών των αστυνομικών αρχών για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και την προστασία των πολιτών από διαδικτυακές απειλές. Το εργαλείο λειτουργεί επιτρέποντας στους πολίτες να ελέγχουν τις διευθύνσεις ηλεκτρονικού ταχυδρομείου τους σε σχέση με συγκεκριμένα σύνολα κλεμμένων δεδομένων που έχουν κατασχεθεί από τις Ολλανδικές Αρχές στο πλαίσιο εξάρθρωσης εγκληματικών δικτύων που δραστηριοποιούνταν στον κυβερνοχώρο.

Επί του παρόντος, διάφορα σύνολα δεδομένων είναι αναζητήσιμα μέσω του εργαλείου, μεταξύ των οποίων (Politie.nl, 2025):

- Genesis Market (κατασχέθηκε στις 5 Απριλίου 2023),
- Qakbot (κατασχέθηκε στις 29 Αυγούστου 2023),
- Bank Help Desk Fraud (Ιανουάριος 2024), και
- Endgame (κατασχέθηκε στις 30 Μαΐου 2024).

Οι χρήστες μπορούν να έχουν πρόσβαση στην υπηρεσία εισάγοντας τη διεύθυνση ηλεκτρονικού ταχυδρομείου τους στο εργαλείο αναζήτησης. Σε περίπτωση που η διεύθυνση ηλεκτρονικού ταχυδρομείου βρεθεί σε κάποια από τις βάσεις δεδομένων, ο χρήστης θα λάβει ειδοποίηση μέσω ηλεκτρονικού ταχυδρομείου από την αστυνομία μέσα σε λίγα λεπτά. Το μήνυμα μπορεί να βρίσκεται στο φάκελο ανεπιθύμητης αλληλογραφίας - ως εκ τούτου, οι χρήστες ενθαρρύνονται να επαληθεύσουν και αυτή τη θέση. Εάν η διεύθυνση ηλεκτρονικού ταχυδρομείου απουσιάζει από οποιοδήποτε σύνολο δεδομένων, δεν θα αποσταλεί κανένα μήνυμα ηλεκτρονικού ταχυδρομείου.

### How it works

Enter your email address. If your e-mail address is included in one of the datasets, you will receive an e-mail from the police within a few minutes. To be sure whether or not you received an email, please also check your spam box. If your email address is not included in one of the datasets, you will not receive an email. For more information, please [read the FAQ](#).



« waakzaam en dienstbaar »



112

Εικόνα 9 menu εφαρμογής checkyouhack

Το εργαλείο αυτό επιτρέπει στους πολίτες να ενημερώνονται για πιθανές παραβιάσεις των προσωπικών τους δεδομένων και ενισχύει την ευαισθητοποίηση σχετικά με τις απειλές του εγκλήματος στον κυβερνοχώρο. Ο δικτυακός τόπος της ολλανδικής αστυνομίας διαθέτει μια περιοχή FAQ για περισσότερες πληροφορίες και λεπτομερείς οδηγίες. Το «Check Your Hack» δείχνει πώς οι προληπτικές ενέργειες των αρχών επιβολής του νόμου μπορούν να βοηθήσουν τις δημόσιες πρωτοβουλίες για την ασφάλεια στον κυβερνοχώρο (Politie.nl, 2025).

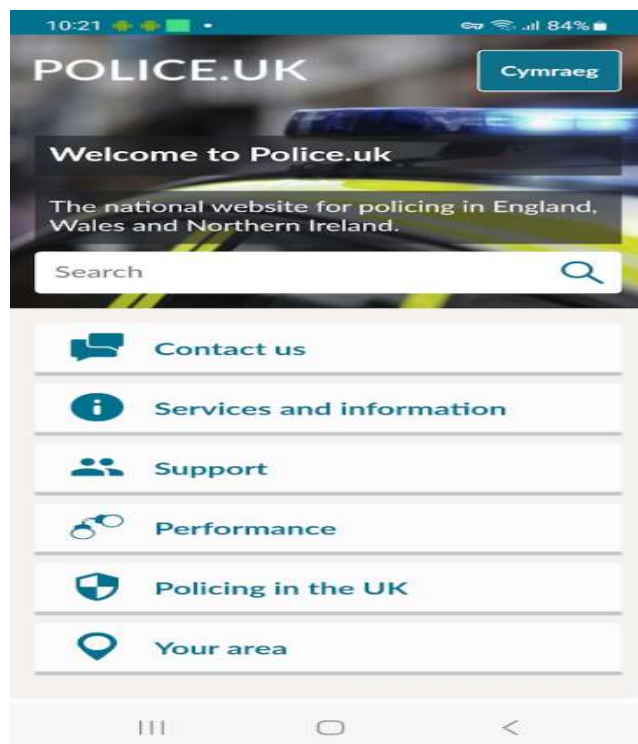
## **4.2. Εφαρμογή «Police.UK» - Ηνωμένο Βασίλειο**

Οι Αρχές Επιβολής του Νόμου στο Ηνωμένο Βασίλειο έχουν αναπτύξει μια νέα εφαρμογή αστυνόμευσης που επιτρέπει στο κοινό να καταγγέλλει εγκλήματα και περιστατικά, να λαμβάνει πληροφορίες σχετικά με τις τοπικές αστυνομικές μονάδες και να έχει πρόσβαση σε συμβουλευτική καθοδήγηση αλλά και βοήθεια για τα θύματα και τους μάρτυρες εγκληματικών ενεργειών. Η εφαρμογή, με την ονομασία «Police.UK», είναι προσβάσιμη μέσω των καταστημάτων εφαρμογών Google Play και iOS και είναι προϊόν του προγράμματος ψηφιακής επικοινωνίας με το κοινό (Digital Public Contact) του Εθνικού Συμβουλίου Αρχηγών Αστυνομίας (National Police Chief's Council).

Δίνει τη δυνατότητα στο κοινό να αναφέρει εγκλήματα και περιστατικά, να έχει πρόσβαση σε οδηγίες για την πρόληψη του εγκλήματος για ένα ευρύ φάσμα θεμάτων, όπως συμβουλές για την αποτροπή διαρρήξεων και κλοπών Ι.Χ. αυτοκινήτων οι οποίες παρουσιάζουν μεγάλη συχνότητα, να λαμβάνει πληροφορίες σχετικά με ομάδες που αστυνομεύουν τοπικά τις γειτονιές, να γνωρίζει τα μέλη των ομάδων αυτών, να λαμβάνει πληροφορίες σχετικά με την εγκληματικότητα στην περιοχή, τις προτεραιότητες και να ενημερώνεται για επικείμενες συναντήσεις εντός της κοινότητας.

Η εφαρμογή προσφέρει λειτουργίες οι οποίες είναι προσβάσιμες μέσω του δικτυακού τόπου «www.police.uk», που αποτελεί τον εθνικό ιστότοπο για υπηρεσίες και πληροφορίες αστυνόμευσης, καθώς και της διαδικτυακής πλατφόρμας «Single Online Home», η οποία περιλαμβάνει 38 από τους 43 δικτυακούς τόπους των αστυνομικών δυνάμεων. Στόχος αυτής της πρωτοβουλίας ήταν να καταστεί πιο εύκολη η επικοινωνία του κοινού με την Αστυνομία και να παρέχεται πρόσβαση σε πληροφορίες για να διαφυλάττουν την προσωπική τους

ασφάλεια, να προστατεύουν τις ιδιοκτησίες τους, καθώς και να ενημερώνονται σχετικά με τις τοπικές δραστηριότητες αστυνόμευσης. Η εφαρμογή «Police.UK» δίνει τη δυνατότητα στο κοινό να έχει τον έλεγχο και να αναφέρει περιστατικά κατά την κρίση του. Η διαθεσιμότητα μιας ψηφιακής επιλογής διευκολύνει τα άτομα να αναφέρουν περιστατικά που προηγουμένως δεν θα το έκαναν. Τα εγκλήματα και τα περιστατικά συχνά δεν καταγγέλλονται προς αποφυγήν της ταλαιπωρίας που συνεπάγεται η πραγματοποίηση ενός τηλεφωνήματος ή η επίσκεψη σε ένα αστυνομικό τμήμα. Ωστόσο, η δυνατότητα μιας ψηφιακής αναφοράς προστατεύει το θύμα ή τον μάρτυρα, καθώς πλέον δεν είναι απαραίτητο να εξιστορήσει εκ νέου τα τραυματικά γεγονότα αποφεύγοντας κατά αυτό τον τρόπο την επανάληψη δυσάρεστων συναισθημάτων. Οι ενδιαφερόμενοι πλέον ασκούν τον πλήρη έλεγχο χρησιμοποιώντας την εφαρμογή σύμφωνα με τις προτιμήσεις τους, δίνοντας φωνή σε ένα ευρύτερο κοινό. Παρόλα αυτά γίνεται σύσταση από τις Αρχές σε περιπτώσεις έκτακτης ανάγκης, το κοινό να καλεί για επείγοντα περιστατικά τον αντίστοιχο αριθμό έκτακτης ανάγκης (999) (Police.uk, 2025).



Εικόνα 10 menu εφαρμογής police.uk

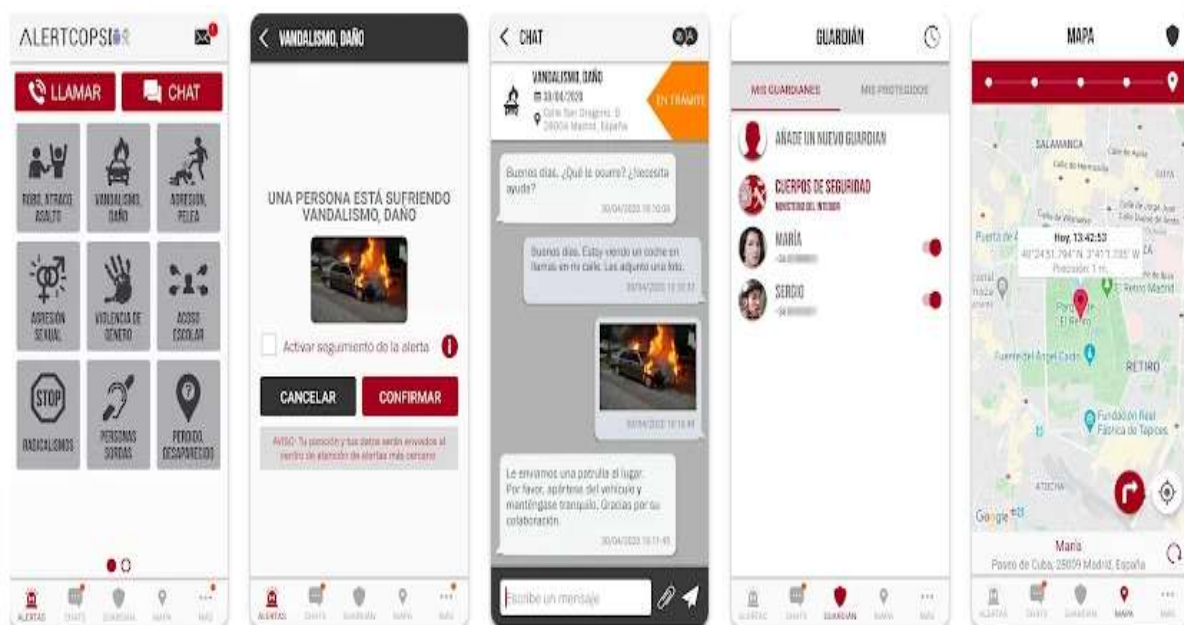
### 4.3. Εφαρμογή «AlertCops» - Ισπανία

Το Υπουργείο Εσωτερικών της Ισπανίας παρέχει μια ολοκληρωμένη ψηφιακή πλατφόρμα μέσω του προγράμματος «AlertCops», με στόχο τη βελτίωση της επικοινωνίας μεταξύ του κοινού και των υπηρεσιών επιβολής του νόμου. Η εφαρμογή διαθέτει πολυάριθμα χαρακτηριστικά που έχουν σχεδιαστεί για να ενισχύουν την ασφάλεια, να εγγυώνται την προσβασιμότητα και να διευκολύνουν τις γρήγορες αντιδράσεις κατά τη διάρκεια έκτακτων περιστατικών. Πρόκειται για μια ολοκληρωμένη τεχνολογία που έχει σχεδιαστεί τόσο για τον γενικό πληθυσμό όσο και για τις ομάδες κινδύνου, προωθώντας την ένταξη και την αποτελεσματική συνεργασία με τις Δυνάμεις και τα Σώματα Ασφαλείας (FFCCSE).

Πρωταρχικό στοιχείο του «AlertCops» είναι η δυνατότητα αναφοράς εγκλημάτων ή συμβάντων μέσω chat ή τηλεφώνου στο πλησιέστερο κέντρο εξυπηρέτησης. Αυτή η λειτουργία επιτρέπει σε οποιονδήποτε να ζητήσει γρήγορα και αβίαστα βοήθεια, ανεξάρτητα από το αν είναι θύμα ή μάρτυρας ενός εγκλήματος. Επιπλέον, οι εξειδικευμένες υπηρεσίες είναι προσβάσιμες για κωφά άτομα ή άτομα με προβλήματα ακοής και ομιλίας, επιτρέποντάς τους να ζητούν βοήθεια έκτακτης ανάγκης μέσω ενός ειδικού συστήματος συναγερμού. Το λογισμικό παρέχει προσβασιμότητα σε άτομα με διαταραχές του φάσματος του αυτισμού (ASD), χρησιμοποιώντας μια εικονογραφική και εικονική γλώσσα για την ενίσχυση της επικοινωνίας.

Η εφαρμογή ενσωματώνει τη λειτουργία «Guardian - Security Forces», επιτρέποντας στους χρήστες να μεταδίδουν τη θέση τους σε οργανισμούς επιβολής του νόμου, διευκολύνοντας έτσι την ταχεία και ακριβή διάσωση κατά τη διάρκεια καταστάσεων. Μια ανάλογη λειτουργία «Private Guardian» επιτρέπει στους χρήστες να αποκαλύπτουν την τοποθεσία τους σε έμπιστους άλλους, όπως η οικογένεια ή οι φίλοι, αυξάνοντας έτσι την προσωπική προστασία. Το «κουμπί SOS» είναι ένα άλλο βασικό εργαλείο, που προορίζεται ειδικά για πληθυσμούς που βρίσκονται σε κίνδυνο, συμπεριλαμβανομένων των θυμάτων έμφυλης βίας και των εργαζομένων στον τομέα της υγειονομικής περίθαλψης. Ενεργοποιώντας το κουμπί, οι χρήστες μπορούν να ειδοποιήσουν αμέσως τις πλησιέστερες υπηρεσίες επιβολής του νόμου, να καταγράψουν 10 δευτερόλεπτα ήχου και να τον μεταδώσουν ως συνημμένο στην ειδοποίηση.

Οι γεωγραφικά εντοπισμένες ειδοποιήσεις και ειδοποιήσεις ασφαλείας αποτελούν θεμελιώδη πτυχή της λειτουργικότητας της εφαρμογής. Οι χρήστες λαμβάνουν άμεσες ειδοποιήσεις από τις αρχές του νόμου σχετικά με κρίσεις ή συμβουλές ασφαλείας στην περιοχή τους, μαζί με ενημερώσεις κατά τη διάρκεια σημαντικών εκδηλώσεων όπως π.χ. η La Romería de El Rocío. Τα μηνύματα αυτά βοηθούν τους χρήστες να είναι ενημερωμένοι και να λαμβάνουν ασφαλέστερες αποφάσεις με βάση το περιβάλλον τους. Το AlertCops διακρίνεται για τη συμπερίληψή του, ιδίως μέσω των πόρων του που έχουν σχεδιαστεί για ευάλωτες κοινότητες. Ενσωματώνει την κοινή χρήση τοποθεσίας, τις ειδοποιήσεις σε πραγματικό χρόνο και την άνετη πρόσβαση σε υπηρεσίες έκτακτης ανάγκης στο πλαίσιο μιας μοναδικής, επικεντρωμένης στον χρήστη εφαρμογής. Αυτή η νέα στρατηγική υπογραμμίζει την αφοσίωση της Ισπανίας στην ενίσχυση της δημόσιας ασφάλειας και της προσβασιμότητας για όλους τους κατοίκους (AlertCops, 2025).



Εικόνα 11 menu εφαρμογής alertcops

#### 4.4. Εφαρμογή «TPS Mobile» - Καναδάς

Τον Αύγουστο του 2015, η Αστυνομική Υπηρεσία του Τορόντο στον Καναδά παρουσίασε το «TPS Mobile», μια εφαρμογή για συσκευές κινητών τηλεφώνων που έχει σχεδιαστεί για να ενισχύσει τη συνδεσιμότητα μεταξύ των κατοίκων του Τορόντο και της Αστυνομίας του μέσω

διαδραστικών λειτουργιών με επίκεντρο την υποστήριξη των θυμάτων/μαρτύρων. Η απόφαση για την κυκλοφορία μιας τέτοιας εφαρμογής για συσκευές δεν ελήφθη βιαστικά αλλά ήταν το αποτέλεσμα πολυετών διαβουλεύσεων.

Προτού η Αστυνομική Υπηρεσία του Τορόντο (Toronto Police Service – TPS) αναπτύξει την ψηφιακή της πλατφόρμα, είχαν προηγηθεί ορισμένα κομβικά γεγονότα που οδήγησαν σε αυτή την κατεύθυνση. Τον Ιούνιο του 2009 έλαβαν χώρα στο Τορόντο τα βραβεία μουσικών βίντεο «Much Music Video Awards», όπου μεταξύ των καλεσμένων ήταν και ένας επώνυμος μπλόγκερ και πρώιμος χρήστης της πλατφόρμας Twitter. Ο εν λόγω έτυχε να βρίσκεται παρόν σε μια επίθεση κατά την διάρκεια κοινωνικής εκδήλωσης σε ξενοδοχείο γεγονός που τον ώθησε να ζητήσει την βοήθεια των Αστυνομικών Αρχών μέσω της πλατφόρμας Twitter. Θαυμαστές του από όλο τον κόσμο άρχισαν να επικοινωνούν με το τηλεφωνικό κέντρο της Αστυνομίας προκειμένου να τους κινητοποιήσουν. Αυτό λειτούργησε ως ο αρχικός συναγερμός σχετικά με την σημαντική επιρροή των πλατφορμών κοινωνικής δικτύωσης σε πραγματικό χρόνο, όπως το «Twitter», στην αντίδραση της αστυνομίας και την δημόσια ασφάλεια.

Κατόπιν αυτών των γεγονότων, μέλη της Αστυνομικής Υπηρεσίας του Τορόντο, συμμετείχαν στο «SmileCon» (Social Media the Internet and Law Enforcement) στην Ουάσινγκτον, όπου ήρθαν σε επαφή με ομολόγους τους από διάφορες υπηρεσίες της Βόρειας Αμερικής και του Ηνωμένου Βασιλείου που ήδη χρησιμοποιούσαν τα μέσα κοινωνικής δικτύωσης και άλλες ψηφιακές πλατφόρμες. Εκείνη την εποχή, η TPS είχε αστυνομικούς στους δρόμους που χρησιμοποιούσαν το Twitter για να συνεργαστούν με την κοινότητα που υπηρετούσαν, αν και δεν είχε καθιερωμένες πολιτικές ή διαδικασίες σχετικά με τη χρήση των μέσων κοινωνικής δικτύωσης.

Ακολούθως, το 2012, έλαβαν χώρα δύο σημαντικά γεγονότα με ανταλλαγή πυροβολισμών, όπου τα γεγονότα που προηγήθηκαν των περιστατικών, τα ίδια τα περιστατικά αλλά και τα και τα επακόλουθα γεγονότα αποτυπώθηκαν σε δημοσιεύσεις στο Twitter.

Αυτό λειτούργησε ως μια καίρια αφύπνιση για την Αστυνομική Υπηρεσία του Τορόντο, ωθώντας την να χρησιμοποιήσει πλήρως τα διαδικτυακά μέσα κοινωνικής δικτύωσης και να εξετάσει το έγκλημα από όλες τις πιθανές οπτικές γωνίες. Κατά συνέπεια, η TPS ξεκίνησε την επιχείρηση Reboot, μια ομάδα εργασίας αφιερωμένη στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Η Επιχείρηση Επανεκκίνηση δημιουργήθηκε για να εξετάσει πώς η ανάλυση των κοινωνικών, κυβερνο- και ψηφιακών πλατφορμών θα μπορούσε να βοηθήσει τόσο στην εξιχνίαση όσο και, κυρίως, στην πρόληψη του εγκλήματος. Ένα βασικό συμπέρασμα της

επιχείρησης Reboot ήταν ότι για να μπορέσει η TPS να εμπλακεί ουσιαστικά στα μέσα κοινωνικής δικτύωσης, πρέπει να ενσωματώσει και το κοινό και να δώσει προτεραιότητα στην συνεργασία. Αναγνώρισαν ότι χωρίς την υποστήριξη και τη συνεργασία του κοινού δεν θα πετύχαιναν τον επιθυμητό στόχο. Παρόλο που οι συμβατικές στρατηγικές επικοινωνίας ήταν αποτελεσματικές, η TPS αναγνώρισε την ανάγκη διερεύνησης καινοτόμων προσεγγίσεων για τη συνεργασία με το κοινό.

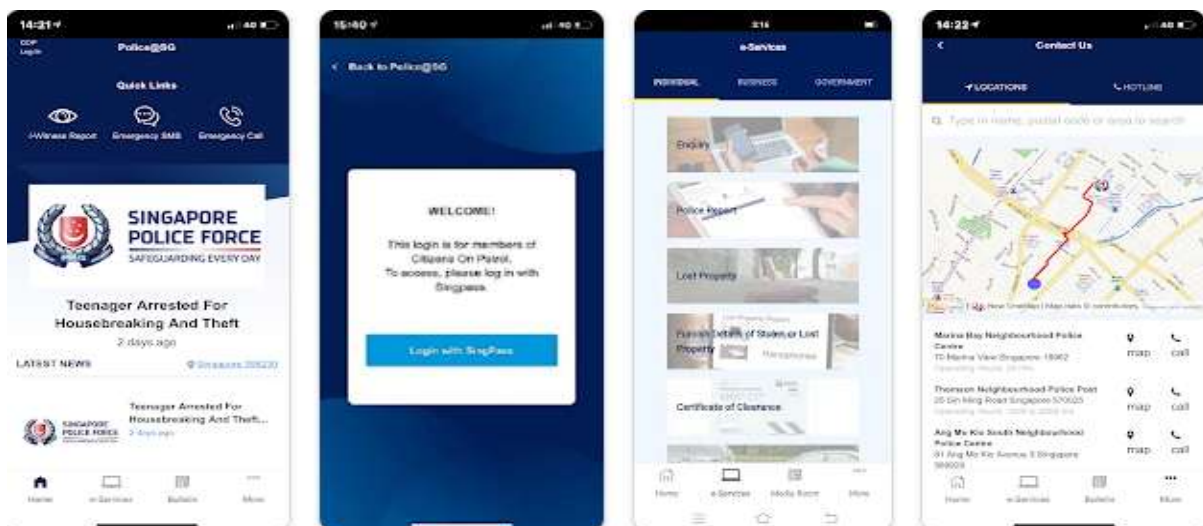
Η αστυνομία του Τορόντο συγκρότησε μια εσωτερική ομάδα για να καθορίσει πώς μια εφαρμογή μπορεί να ενισχύσει την επαφή με τους πολίτες του Τορόντο. Συμβουλευτήκαν άλλες κορυφαίες υπηρεσίες σε αυτόν τον τομέα, συμπεριλαμβανομένης της Αστυνομικής Διεύθυνσης της Βικτώριας, η οποία ήταν η πρώτη υπηρεσία στον Καναδά που εγκαινίασε μια εφαρμογή για κινητά τηλέφωνα. Στην προσπάθειά τους να αναπτύξουν μια κοινοτική εφαρμογή, ζήτησαν τη γνώμη της κοινότητας μέσω των μέσων κοινωνικής δικτύωσης, ρωτώντας για τα επιθυμητά χαρακτηριστικά χρησιμοποιώντας το hashtag #TPSApp. Αφού καθόρισαν τα κριτήριά τους, το TPS εξασφάλισε με επιτυχία χρήματα μέσω μιας επιχορήγησης που αποσκοπούσε στην υποστήριξη θυμάτων και μαρτύρων, με μια εφαρμογή να αναδεικνύεται ως η ιδανική επιλογή.

Σε διάστημα αρκετών μηνών, η Αστυνομική Υπηρεσία του Τορόντο και η εταιρεία «MobilePD» δημιούργησαν την αρχική έκδοση της εφαρμογής για κινητά TPS, η οποία διέθετε χαρακτηριστικά όπως ειδοποιήσεις της κοινότητας σε πραγματικό χρόνο, έναν εικονικό αστυνομικό, πρόσβαση σε αστυνομικούς της γειτονιάς και τη δυνατότητα υποβολής συγκεκριμένων αστυνομικών αναφορών μέσω της εφαρμογής (MobilePD, 2024). Η εφαρμογή παρουσιάστηκε τον Αύγουστο του 2015 και έτυχε ευρείας αποδοχής τόσο από τα μέσα ενημέρωσης όσο και από την κοινότητα. Στις επόμενες εκδόσεις, η TPS στοχεύει να επινοήσει νέες λύσεις που θα επιτρέψουν στην κοινότητα του Τορόντο να ενισχύσει συνεργατικά τη δημόσια ασφάλεια. Ένα πιθανό χαρακτηριστικό για μελλοντική έκδοση είναι η αναφορά Next-Gen-911, που επιτρέπει στα μέλη της κοινότητας να χρησιμοποιούν την εφαρμογή TPS για την αναφορά εγκλημάτων σε πραγματικό χρόνο και την άμεση επικοινωνία με το κέντρο. Θα επικεντρωθούν στην παροχή πληροφοριών σε πραγματικό χρόνο σε άτομα σχετικά με τις περιοχές τους, συμπεριλαμβανομένου ενός διαδραστικού χάρτη εγκληματικότητας που εμφανίζει την εγκληματική δραστηριότητα της γειτονιάς (Toronto Police, 2025).

#### 4.5. Εφαρμογή «Police@SG» – Δημοκρατία της Σιγκαπούρης

Το «Police@SG» είναι μια εφαρμογή που διατίθεται τόσο για συσκευές Android όσο και για iOS και αποτελεί μια πρωτοβουλία της Αστυνομίας της Σιγκαπούρης, η οποία παρέχει στο κοινό την δυνατότητα πρόσβασης σε χρήσιμες πληροφορίες εν κινήσει. Με την υπόψη εφαρμογή «Police@SG», οι πολίτες έχουν πρόσβαση στις ακόλουθες υπηρεσίες (SPF, 2025):

- Να ενημερώνονται σχετικά με τα τελευταία νέα για εγκλήματα, τις εκκλήσεις της αστυνομίας για παροχή πληροφοριών και για αγνοούμενα άτομα.
- Να μοιράζονται περιεχόμενο στις μέσα κοινωνικής δικτύωσης «Facebook» και το «X».
- Να εντοπίζουν το πλησιέστερο αστυνομικό τμήμα από την τρέχουσα θέση τους.
- Να συνδέονται με την αρχική σελίδα της ιστοτόπου της Αστυνομίας, αποκτώντας πρόσβαση σε πλήθος ηλεκτρονικών υπηρεσιών.
- Να υποβάλλει πληροφορίες ή να ανταποκρίνεται σε εκκλήσεις της Αστυνομίας μέσω της πύλης υποβολής πληροφοριών «i-Witness». Πρόκειται για ένα χαρακτηριστικό της εφαρμογής που δίνει την δυνατότητα στους πολίτες να παρέχουν πληροφορίες σχετικά με εγκληματικές και ύποπτες δραστηριότητες. Οι πληροφορίες μπορούν να χρησιμοποιηθούν για να βοηθήσουν τις συνεχιζόμενες έρευνες ή να αποκαλύψουν εγκλήματα που δεν έχουν καταγγελθεί.



Εικόνα 12 menu εφαρμογής Police@SG

## **4.6. Εφαρμογή «My Police Department App (MyPD)» Ηνωμένες Πολιτείες Αμερικής**

Η εφαρμογή My Police Department App (MyPD) αποτελεί μια δωρεάν εφαρμογή για κινητά που διατίθεται τόσο για συσκευές Android όσο και για iOS και έχει σχεδιαστεί για να διευκολύνει τους πολίτες να συνδέονται με το τοπικό αστυνομικό τμήμα. Πλήθος Αστυνομικών Υπηρεσιών στις Ηνωμένες Πολιτείες Αμερικής έχουν επιλέξει την εν λόγω εφαρμογή, καθώς το MyPD διαθέτει περίπου 40 παραμετροποιήσιμες λειτουργίες, επιτρέποντας σε κάθε αστυνομικό τμήμα να προσαρμόζει τη λειτουργικότητα της εφαρμογής με βάση τις ανάγκες της κοινότητάς του.

Τα βασικά χαρακτηριστικά του MyPD είναι τα εξής:

1. Ειδοποιήσεις push: Η εφαρμογή προβλέπει ενημερώσεις και ειδοποιήσεις σε πραγματικό χρόνο μέσω ειδοποιήσεων push, ενημερώνοντας τους χρήστες για σημαντικά θέματα ασφάλειας, έκτακτα περιστατικά ή ανακοινώσεις. Οι ειδοποιήσεις αποστέλλονται από το ταμπλό του τμήματος και οι χρήστες δεν χρειάζεται να δημιουργήσουν λογαριασμό για να τις λαμβάνουν.
2. Πηγές και πληροφορίες σχετικά με το έγκλημα: Το MyPD περιλαμβάνει πόρους και συνδέσμους για βασικά θέματα ασφάλειας, όπως δελτία τύπου, πληροφορίες επικοινωνίας για τους αστυνομικούς και πρόσβαση στο μητρώο σεξουαλικών παραβατών. Οι χρήστες έχουν τη δυνατότητα να σαρώνουν διάφορες οθόνες υποβάθρου, οι οποίες μπορεί να διαθέτουν ενημερώσεις σχετικά με αγνοούμενους, καταζητούμενα άτομα ή άλλες ανακοινώσεις.
3. Ανώνυμες συμβουλές: Η εφαρμογή επιτρέπει στους χρήστες να αναφέρουν εγκλήματα, ανησυχίες για την ποιότητα ζωής (π.χ. παραβιάσεις στάθμευσης ή δραστηριότητες που σχετίζονται με ναρκωτικά) ή να υποβάλλουν συμβουλές ανώνυμα. Στις αναφορές μπορούν επίσης να επισυνάπτονται φωτογραφίες και τοποθεσίες GPS χρησιμοποιώντας την κάμερα ή τη γκαλερί του τηλεφώνου.
4. Προσαρμογή και προαιρετική κοινή χρήση: Το MyPD επιτρέπει στους χρήστες να μοιράζονται προαιρετικά ανώνυμα δεδομένα σχετικά με την ηλικία, το φύλο ή τον τρόπο με τον οποίο ανακάλυψαν την εφαρμογή. Αυτό βοηθά τις υπηρεσίες να αναλύσουν τη χρήση της εφαρμογής χωρίς να απαιτούνται προσωπικές πληροφορίες. Πολύ σημαντικό είναι ότι δεν απαιτούνται λογαριασμοί ή προσωπικά δεδομένα για τη χρήση της εφαρμογής.

5. Χαρακτηριστικά δέσμευσης: Παρόλο που το MyPD δεν αποτελεί κοινωνικό δίκτυο, ενσωματώνει κοινωνικά στοιχεία, όπως η δυνατότητα "ξεκλειδώματος σημάτων" μέσω της συχνής αλληλεπίδρασης με την εφαρμογή. Αυτή η παιχνιδιοποίηση ενθαρρύνει τη μεγαλύτερη δέσμευση με το αστυνομικό τμήμα.

6. Χωρίς διαφημίσεις και με επίκεντρο την προστασία της ιδιωτικής ζωής: Η λήψη της εφαρμογής είναι εντελώς δωρεάν και δεν περιλαμβάνει διαφημίσεις. Οι χρήστες δεν υποχρεούνται να δημιουργήσουν λογαριασμούς ή να παράσχουν προσωπικές πληροφορίες, εκτός εάν το επιλέξουν.

Η εφαρμογή MyPD ενισχύει την επικοινωνία μεταξύ του αστυνομικού τμήματος και του κοινού, προσφέροντας μια προσιτή και βολική πλατφόρμα για τους πολίτες ώστε να ενημερώνονται και να μοιράζονται πληροφορίες. Οι κάτοικοι πόλεων μπορούν να χρησιμοποιούν την εφαρμογή για να στέλνουν ανώνυμες πληροφορίες, να αναφέρουν περιστατικά ή απλώς να ενημερώνονται για τις τελευταίες πληροφορίες ασφαλείας. Η δυνατότητα της εφαρμογής να επισυνάπτει φωτογραφίες, να μοιράζεται τοποθεσίες GPS και να προσαρμόζει χαρακτηριστικά ειδικά για την υπηρεσία την καθιστά πολύτιμο εργαλείο για την τοπική επιβολή του νόμου.

Οι πολίτες μπορούν να κατεβάσουν το MyPD αναζητώντας το στο κατάστημα εφαρμογών της συσκευής τους. Αφού επιλέξουν την τοπική τους υπηρεσία, όπως π.χ. το αστυνομικό τμήμα του Old Orchard Beach, η εφαρμογή θα ανοίγει πάντα απευθείας στους πόρους του συγκεκριμένου τμήματος. Αυτός ο προσεγμένος σχεδιασμός διασφαλίζει ότι οι χρήστες μπορούν να έχουν εύκολη πρόσβαση σε σχετικά εργαλεία και ενημερώσεις όποτε χρειάζεται. Το MyPD είναι μια καινοτόμος εφαρμογή που σέβεται το απόρρητο και απλοποιεί την επικοινωνία μεταξύ πολιτών και αστυνομίας, ενισχύει την ασφάλεια της κοινότητας και ενθαρρύνει την προληπτική εμπλοκή με την τοπική επιβολή του νόμου (Cambridge Police, 2024)



Εικόνα 13 menu εφαρμογής mypd

## Συμπεράσματα, Προτάσεις

Η εξέλιξη των υπηρεσιών ηλεκτρονικής διακυβέρνησης έχει μεταμορφώσει σε βάθος τον τρόπο με τον οποίο οι υπηρεσίες επιβολής του νόμου συνεργάζονται με τους πολίτες, δίνοντας έμφαση στην προσβασιμότητα, τη διαφάνεια και την αποτελεσματικότητα. Αξιοποιώντας τις ψηφιακές τεχνολογίες, οι αστυνομικές δυνάμεις σε όλο τον κόσμο όχι μόνο ενισχύουν τη δημόσια ασφάλεια αλλά και οικοδομούν ισχυρότερες, πιο αξιόπιστες σχέσεις με τις κοινότητές τους. Οι περιπτώσιολογικές μελέτες από την Ελλάδα, την Ολλανδία, το Ηνωμένο Βασίλειο, την Ισπανία, τον Καναδά, τη Σιγκαπούρη και τις Ηνωμένες Πολιτείες καταδεικνύουν πώς οι καινοτόμες λύσεις μπορούν να αντιμετωπίσουν τοπικές προκλήσεις, συμβάλλοντας παράλληλα στον παγκόσμιο στόχο της εκσυγχρονισμένης διακυβέρνησης με επίκεντρο τον πολίτη.

Ένα από τα πιο αξιοσημείωτα πλεονεκτήματα των υπηρεσιών ηλεκτρονικής διακυβέρνησης στην αστυνόμευση είναι η δυνατότητα παροχής επικοινωνίας σε πραγματικό χρόνο και πρόσβασης σε κρίσιμες πληροφορίες. Από το πρόγραμμα «Police on Line» της Ελλάδας και τα συστήματα CAR-PC μέχρι τον έλεγχο ηλεκτρονικής υποκλοπής της ολλανδικής αστυνομίας και την εφαρμογή AlertCops της Ισπανίας, οι λύσεις αυτές καταδεικνύουν πώς οι ψηφιακές πλατφόρμες μπορούν να βελτιώσουν την επιχειρησιακή αποτελεσματικότητα και να δώσουν στους πολίτες τη δυνατότητα να συμμετέχουν ενεργά στη διατήρηση της ασφάλειας. Επιπλέον,

πλατφόρμες όπως το *Police.UK* της Βρετανίας και το *Police@SG* της Σιγκαπούρης παρέχουν κεντρικούς κόμβους για αναφορές, συμβουλές πρόληψης του εγκλήματος και συμμετοχή, εξασφαλίζοντας απλοποιημένη πρόσβαση στις υπηρεσίες. Ταυτόχρονα, οι έξυπνες τεχνολογίες αστυνόμευσης, όπως η εφαρμογή στην Ελλάδα ενός «κουμπιού πανικού» για καταστάσεις έκτακτης ανάγκης, καταδεικνύουν τη σημασία εξατομικευμένων, καινοτόμων λύσεων που ανταποκρίνονται σε ευάλωτους πληθυσμούς και καταστάσεις υψηλού κινδύνου. Οι προσεγγίσεις αυτές δίνουν έμφαση στους διπλούς στόχους της προστασίας και της συμμετοχικότητας, διασφαλίζοντας ότι οι υπηρεσίες ηλεκτρονικής διακυβέρνησης ανταποκρίνονται στις ανάγκες όλων των πολιτών, συμπεριλαμβανομένων των ατόμων με αναπηρία ή εκείνων που κινδυνεύουν από βία.

Οι πρακτικές των διεθνών αστυνομικών δυνάμεων αποκαλύπτουν περαιτέρω τη δύναμη της συνεργασίας και της ανταλλαγής γνώσεων στην προώθηση της καινοτομίας. Μαθαίνοντας από τις επιτυχίες και τις προκλήσεις που αντιμετωπίζουν χώρες όπως ο Καναδάς, ο οποίος διαπρέπει στην εμπλοκή της κοινότητας, ή οι Ηνωμένες Πολιτείες, οι οποίες χρησιμοποιούν εφαρμογές για κινητά όπως το *MyPD* για επικοινωνία σε πραγματικό χρόνο, οι κυβερνήσεις μπορούν να υιοθετήσουν τις βέλτιστες πρακτικές, προσαρμόζοντάς τις παράλληλα στα δικά τους μοναδικά πλαίσια. Αυτή η παγκόσμια προοπτική διασφαλίζει ότι οι πρωτοβουλίες ηλεκτρονικής διακυβέρνησης παραμένουν σχετικές, προσαρμόσιμες και προοδευτικές.

Για τον εκσυγχρονισμό των υπηρεσιών επιβολής του νόμου και τη βελτίωση της δέσμευσης του κοινού, η Ελληνική Αστυνομία θα πρέπει να υιοθετήσει μια ολοκληρωμένη στρατηγική ψηφιακού μετασχηματισμού, εμπνευσμένη από παγκόσμιες βέλτιστες πρακτικές. Η Ελλάδα θα πρέπει να αναπτύξει μια κεντρική εφαρμογή για κινητά, παρόμοια με την *Police.UK* ή την *MyPD*, η οποία θα παρέχει αναφορά εγκλημάτων, ειδοποιήσεις σε πραγματικό χρόνο και άμεση επικοινωνία με τις τοπικές αστυνομικές μονάδες. Αυτή η εφαρμογή θα πρέπει να ενσωματώνει ένα κουμπί πανικού, εμπνευσμένο από το *AlertCops* της Ισπανίας, επιτρέποντας σε άτομα που βρίσκονται σε κίνδυνο (π.χ. θύματα ενδοοικογενειακής βίας) να ζητήσουν άμεση βοήθεια.

Η εφαρμογή ανώνυμης αναφοράς εγκλημάτων μέσω εφαρμογών για κινητά τηλέφωνα, όπως φαίνεται στο *TPS Mobile* του Καναδά, θα ενθάρρυνε περισσότερους πολίτες να αναφέρουν εγκλήματα χωρίς το φόβο αντιποίνων. Επιπλέον, χαρακτηριστικά όπως ενημερώσεις για την κοινοτική αστυνόμευση, πληροφορίες επικοινωνίας με τοπικούς αξιωματικούς και οδηγίες για την πρόληψη του εγκλήματος θα ενίσχυαν την εμπιστοσύνη του κοινού.

Με τις απειλές στον κυβερνοχώρο να αυξάνονται, η Ελλάδα θα πρέπει να δημιουργήσει ένα διαδικτυακό σύστημα «Check Your Hack», όπως η Ολλανδία, που θα επιτρέπει στους πολίτες να επαληθεύουν αν τα δεδομένα τους έχουν παραβιαστεί. Η ανάλυση εγκλημάτων με βάση την ΤΝ θα πρέπει επίσης να βοηθήσει την αστυνομία στον εντοπισμό της απάτης στον κυβερνοχώρο. Η εφαρμογή θα πρέπει να ενσωματώνει φωνητικές εντολές, μετατροπή κειμένου σε ομιλία, και εικονικές διεπαφές για άτομα με αναπηρίες, παρόμοια με τα φιλικά προς τα άτομα με ειδικές ανάγκες εργαλεία της *AlertCops*. Αυτό διασφαλίζει τη συμμετοχικότητα στα μέτρα δημόσιας ασφάλειας.

# ΒΙΒΛΙΟΓΡΑΦΙΑ

## Ελληνική

Τσιρώνης, Κ. (2022). “Ελλάδα: Το νέο πρόγραμμα αστυνόμευσης με βάση τα βιομετρικά στοιχεία συνιστά υπονόμευση δικαιωμάτων” <https://www.hrw.org/el/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights>

Γιαννουκάκου, Α., (2011). Ηλεκτρονική Διακυβέρνηση. Εθνικό Κέντρο Δημόσιας Διοίκησης και Αυτοδιοίκησης Περιφερειακό Ινστιτούτο Επιμόρφωσης Θεσσαλονίκης.

Παπαζήσης, Γ. (2008). *Ηλεκτρονική Δημόσια Διοίκηση: Οργάνωση, Τεχνολογία και Εφαρμογές*. Εκδόσεις Παπαζήση, Αθήνα.

Σμυρλής, Ι., Διαφάνειες Μαθήματος Καινοτομία, Οργανωσιακή Αλλαγή & Ηλεκτρονική Διακυβέρνηση ΠΜΣ «Εφαρμοσμένη Δημόσια Οικονομική και Δημόσια Πολιτική», ακαδημαϊκό έτος 2021 - 2022

Πομπόρτσος, Α., (2017). *Εισαγωγή στην Ηλεκτρονική Διακυβέρνηση*, Εκδόσεις Τζιόλα, Αθήνα.

## Ξένη

Ronchi, A. (2019). *e-Democracy Toward a New Model of (Inter)active Society*, Springer International Publishing, New York.

Abhay, D., S. Akash, Ashwin, K. R., Shenoy, A. G., and Prafullata Auradkar. (2023). Smart Policing: Using Geospatial Crime Data to Plan Patrol Routes. *2023 4th International Conference for Emerging Technology (INCET)* <https://ieeexplore.ieee.org/document/10170289>

Alshehri, M., and Drew, S. (2010). E-government fundamentals. *IADIS International Conference on ICT, Society and Human Beings* <https://www.iadisportal.org/digital-library/e-government-fundamentals>

Dimitrelou, Sotiria, and Konstantinos Fouskas. 2023. Digital Government Platforms in Greece. Current Trends: The Case of Gov.Gr. *KnE Social Sciences* 8 (1), 335–359. <https://doi.org/10.18502/kss.v8i1.12655>.

- Maliphol, S., and Hamilton, C. (2022). Smart Policing: Ethical Issues & Technology Management of Robocops. *IEEE Conference Publication*  
<https://ieeexplore.ieee.org/abstract/document/9882871/>
- Sarifudin, R., and Damanik, F. H. S. (2024). Enhancing transparency and accountability in public administration through information technology utilization. *Gema Wiralodra*, 15(1), 32–40. <https://doi.org/10.31943/gw.v15i1.661>
- Yamin, M. M., Shalaginov, A., and Katt, B. (2020). Smart Policing for a Smart World Opportunities, Challenges and Way Forward. *Advances in Intelligent Systems and Computing*, 532–549. [https://doi.org/10.1007/978-3-030-39445-5\\_39](https://doi.org/10.1007/978-3-030-39445-5_39)
- L. Elaine Halchin, Electronic government: Government capability and terrorist resource, *Government Information Quarterly*, Volume 21, Issue 4, 2004, <https://doi.org/10.1016/j.giq.2004.08.002>
- Abramson, M.A., & Means G (2001). *E-Government 2001*. Rowman and Littlefield Publishers, Maryland.

## Διαδικτυακοί Τόποι

- Παγκόσμια Τράπεζα (2015): <https://libguides.libraries.wsu.edu/c.php?g=294126&p=1959513>
- OECD (2003): <https://doi.org/10.1787/9789264101197-en>.
- Ο.Η.Ε.: <https://publicadministration.un.org/egovkb/en-us/Overview#whatis>
- Ε.Ε. (2003): <https://eur-lex.europa.eu/EL/legal-content/summary/egovernment.html>
- Η.Π.Α.: <https://www.usda.gov/ocio/centers/irmc/e-government>
- Βικιπαίδεια: [https://el.wikipedia.org/wiki/%CE%97%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CE%AE\\_%CE%B4%CE%B9%CE%B1%CE%BA%CF%85%CE%B2%CE%AD%CF%81%CE%BD%CE%B7%CF%83%CE%B7#cite\\_note-1](https://el.wikipedia.org/wiki/%CE%97%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CE%AE_%CE%B4%CE%B9%CE%B1%CE%BA%CF%85%CE%B2%CE%AD%CF%81%CE%BD%CE%B7%CF%83%CE%B7#cite_note-1)
- Council of Europe (2020): <https://rm.coe.int/11th-cddg-session-10-11-september-2020-e-democracy-handbook/16809f5a72>
- European Commission (2017): <https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration>
- Ε.Ε. (2016): <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A12016P%2FTXT>
- Ευρωπαϊκή Επιτροπή (2017) : [eif\\_brochure\\_final.pdf](#)

CEF: [https://hadea.ec.europa.eu/programmes/connecting-europe-facility/about\\_en](https://hadea.ec.europa.eu/programmes/connecting-europe-facility/about_en)

O.H.E. (2002): <https://www.un-ilibrary.org/content/books/9789210016322/read>  
<https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:32016R0679>

Ελληνική Αστυνομία. (2009): <https://www.astynomia.gr/2009/05/02/i-pliroforiki-stin-astynomia-police-on-line/>

Gov.gr (2025): <https://www.gov.gr/upourgeia/upourgeio-prostasias-tou-polite/ellenike-astunomia>

ΥΠ.ΕΣ.(2023):[https://www.ypes.gr/wp-content/uploads/2023/05/230419\\_GGDA\\_%CE%95Book-Apologismou-20230515.pdf](https://www.ypes.gr/wp-content/uploads/2023/05/230419_GGDA_%CE%95Book-Apologismou-20230515.pdf)

Ελληνική Αστυνομία (2019) : <https://www.astynomia.gr/file/2018/07/14122019anakoinosismartpolicing.pdf>

Opengov (2017): <https://www.opengov.gr/ypes/wp-content/uploads/2017/02/smart-policing.pdf>

Ελληνική Αστυνομία (2022): <https://www.astynomia.gr/2022/07/09/09-07-2022-me-dyo-vraveia-timithike-i-elliniki-astynomia-ston-diagonismo-vraveion-psifiakis-diakyvernisis-digital-gov-awards-gia-to-etos-2022/>

Panic Button: <https://www.taxheaven.gr/circulars/41474/111847-23-11-2022?nomobile=1>

Υπουργείο Προστασίας Πολίτη (2024) : <https://www.minocp.gov.gr/2024/05/20/20-05-2024-koino-deltio-tyrou-ton-ypourgeion-prostasias-tou-politi-ethnikis-oikonomias-kai-oikonomikon-psifiakis-diakyvernisis-kai-koinonikis-synochis-kai-oikogeneias/>

Ελληνική Αστυνομία. (2023): <https://www.astynomia.gr/2023/03/27/27-03-2023-xekinise-i-leitourgia-tou-panic-button-koubi-panikou-kata-tis-endooikogeneiakis-vias-se-attiki-kai-thessaloniki/>

MobilePD. (2024): <https://www.mobilepd.com/case-studies/vicpd.html>.

Police.uk (2025): <https://www.police.uk/pu/notices/2024/app/do-it-online>

Politie.nl (2025): <https://www.politie.nl/en/information/checkyourhack.html>

Singapore Police Force (SPF) (2025): <https://www.police.gov.sg>

Toronto Police (2025). <https://www.tps.ca/>.

AlertCops (2025): <https://alertcops.ses.mir.es/publico/alertcops/en/comoFunciona.html>.

Cambridge Police (2024)<https://www.cambridgema.gov/Departments/cambridgepolice/mydpapp>