ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Ανοιχτά δεδομένα και προστασία προσωπικών δεδομένων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της/του

Τσερέ Ευαγγελίας

Επιβλέπων : Αλεξόπουλος Χαράλαμπος

Μέλη εξεταστικής επιτροπής: Δ. Σαράντης, Β. Διαμαντοπούλου

Σάμος, [Ιούνιος 2025]

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο του μεταπτυχιακού προγράμματος σπουδών Ηλεκτρονική Διακυβέρνηση του τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών συστημάτων του Πανεπιστημίου Αιγαίου, με αντικείμενο τη διερεύνηση ζητημάτων που προκύπτουν από τη σύγκλιση της ψηφιακής διακυβέρνησης, της ανοιχτής πληροφορίας και της προστασίας της ιδιωτικότητας.

Το θέμα της εργασίας προέκυψε από τον προβληματισμό σχετικά με το πόσο η διαφάνεια μπορεί να συνυπάρξει με τη διαφύλαξη της ιδιωτικότητας των πολιτών στη σημερινή ψηφιακή εποχή, με την αξιοποίηση των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης από τους δημόσιους και ιδιωτικούς φορείς.

Επιχειρείται να συνδυαστεί θεωρητική ανάλυση, νομική τεκμηρίωση και πρακτικές περιπτώσεις με στόχο τη συμβολή στη συζήτηση για την υπεύθυνη και ισορροπημένη χρήση των δημόσιων δεδομένων.

Θα ήθελα να εκφράσω τις ευχαριστίες μου στον καθηγητή κ. Αλεξόπουλο Χαράλαμπο που με ενέπνευσε να ασχοληθώ με το παρόν θέμα, όπως επίσης και στους διδάσκοντες καθηγητές του προγράμματος για τις γνώσεις που μου προσέφεραν.

του/της
ΤΣΕΡΕ ΕΥΑΓΓΕΛΙΑ
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

Λίστα Πινάκων

Ακρωνύμια

ΤΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνίας
RTLD	Ready to Link Data
GDPR	General Data Protection Regulation
RDF	Resource Description Framework
API	Application Programming Interface
URI	Uniform Resource Identifier
DPIA	Data Protection Impact Assessment
BORTLD	Big Open Ready to Link Data

Περίληψη

Η διπλωματική εργασία εξετάζει τη σχέση μεταξύ διαφάνειας και προστασίας προσωπικών δεδομένων στο πλαίσιο των Συνδεδεμένων Προσωπικών Δεδομένων. Εστιάζει σε κινδύνους που εμφανίζονται από τη δημοσίευση και τη διασύνδεση δημόσιων συνόλων δεδομένων, όπως και στις δυνατότητες να υλοποιηθούν πολιτικές που θα επιτύχουν την ισορροπία μεταξύ της λογοδοσίας και της ιδιωτικότητας.

Παρουσιάζεται το θεωρητικό και νομικό πλαίσιο που διέπει τα Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης με αναφορές στον Γενικό Κανονισμό για την Προστασία Δεδομένων, γνωστό και ως GDPR, καθώς και στις αρχές της διαφάνειας, της ανωνυμοποίησης και της συγκατάθεσης. Στη συνέχεια καταγράφονται τεχνικές για την προστασία της ιδιωτικότητας και βέλτιστες πρακτικές για την προστασία των δεδομένων. Ακολουθεί συγκριτική μελέτη πέντε περιπτώσεων χωρών από την ΕΕ, όπου εξετάζονται εθνικές πολιτικές, ρυθμιστικές ελλείψεις και ο βαθμός συμμετοχής των πολιτών.

Αναδεικνύεται ότι παρά την όποια νομική υποστήριξη της διαφάνειας ως αρχής της διακυβέρνησης, όταν λείπουν οι θεσμικές και τεχνικές εγγυήσεις μπορούμε να οδηγηθούμε σε παραβιάσεις της ιδιωτικότητας.

Τέλος, προτείνονται ένα σύνολο τεχνικών, οργανωτικών και πολιτικών παρεμβάσεων ώστε να δημιουργηθεί ένα πλαίσιο υπεύθυνης διαφάνειας, όπου η πληροφορία θα είναι προσβάσιμη χωρίς να τίθεται σε κίνδυνο η ιδιωτικότητα των πολιτών.

Λέξεις Κλειδιά: *RTLD- Ready to Link Data, διαφάνεια, προσωπικά δεδομένα, ιδιωτικότητα*

Abstract

This thesis examines the relationship between transparency and the protection of personal data in the context of Ready to Link Data (RTLD). It focuses on the risks arising from the publication and interconnection of public datasets, as well as on the possibilities of implementing policies that achieve a balance between accountability and privacy.

The theoretical and legal framework governing Ready to Link Data is presented, with references to the General Data Protection Regulation (GDPR), and to the principles of transparency, anonymization, and consent. This is followed by an overview of technical privacy preserving methods and best practices for data protection. A comparative case study of five EU countries is then included, analyzing national policies, regulatory gaps, and the level of citizen participation.

The study highlights that despite the legal support of transparency as a governance principle, the absence of institutional and technical safeguards may lead to violations of privacy.

Finally, the thesis proposes a set of technical, organizational, and policy interventions to build a framework of responsible transparency, in which information remains accessible without compromising the privacy of individuals.

Keywords: *RTLD- Ready to Link Data*, *transparency*, *personal data*, *privacy*

1 *Εισαγωγή*

1.1 <Η προστασία των προσωπικών δεδομένων σε μία εποχή αυξημένης ζήτησης για διαφάνεια>

Στη σημερινή εποχή, κάθε πτυχή της καθημερινότητας των ατόμων είναι στενά συνδεδεμένη με τις Νέες Τεχνολογίες [1]. Σε επίπεδο Κρατών και Κυβερνήσεων, είναι πλέον ιδιαίτερα διαδεδομένη η χρήση Τεχνολογιών Πληροφορικής και Επικοινωνίας (ΤΠΕ) όχι μόνο για την διεκπεραίωση των εσωτερικών διεργασιών των υπηρεσιών, αλλά αποτελεί πλέον και έναν από τους σημαντικότερους και λειτουργικότερους τρόπους συναλλαγής των πολιτών με το δημόσιο φορέα [11]. Επιπλέον, η χρήση Πληροφοριακών Συστημάτων και οι ΤΠΕ έχουν καταστήσει δυνατή και εύκολα προσβάσιμη τη διάθεση της πληροφορίας προς τους πολίτες, καθιστώντας δυνατή τη διαφάνεια των διεργασιών και αποφάσεων που λαμβάνουν οι Φορείς [13]. Κάθε πολίτης έχει τη δυνατότητα να αναζητήσει και να πληροφορηθεί σχετικά με τις αποφάσεις που λαμβάνονται από τους Φορείς και τις πιθανές δαπάνες που αυτές συνεπάγονται [12]. Τα δεδομένα που είναι πλέον διαθέσιμα προς όλους, γνωστά ως Ανοιχτά Δεδομένα, αποτελούν ένα τεράστιο όγκο δεδομένων που θεωρητικά θα συμβάλουν στη Διαφάνεια, έννοια στενά συνδεδεμένη με την εμπιστοσύνη που δείχνουν οι πολίτες στις Κυβερνήσεις [6]. Τα αναμενόμενα οφέλη από την πρακτική της δημοσιοποίησης των Ανοιχτών Δεδομένων είναι πολλά, μεταξύ των οποίων όπως ήδη αναφέραμε η Διαφάνεια, η εμπιστοσύνη αλλά και η αύξηση του ενδιαφέροντος των πολιτών για τα κοινά και κατά συνέπεια η συμμετοχή τους σε αυτά, ειδικά εφόσον η έννοια της Συμμετοχικής Διακυβέρνησης κερδίζει διαρκώς έδαφος [17]. Τα Ανοιχτά Δεδομένα λοιπόν αποτελούν ένα σημαντικό εργαλείο προς αυτή την κατεύθυνση, αφού οι πολίτες είναι σε θέση να τα χρησιμοποιήσουν για τη δημιουργία πληροφορίας που θα οδηγήσει στη λήψη εμπεριστατωμένων αποφάσεων, την επιλογή αντιπροσώπων βασισμένη σε απτά στοιχεία αλλά και από την πλευρά των Φορέων δίνεται η δυνατότητα μέσω εξειδικευμένων Πληροφοριακών Συστημάτων για την καλύτερη κατανόηση των αναγκών των πολιτών και τη δημιουργία πολιτικής που ανταποκρίνεται καλύτερα στις ανάγκες τους [10].

Η απόλυτη διαφάνεια λοιπόν φαίνεται να είναι ιδιαίτερα σημαντική για την έννοια της Δημοκρατίας, όπου όλοι οι πολίτες θα έχουν πρόσβαση σε όλα τα δεδομένα που αφορούν τις

διεργασίες του Κράτους, καθώς και σε αυτά που σχετίζονται με την καθημερινότητά τους κι την ποιότητα ζωής τους, όπως για παράδειγμα δεδομένα σχετικά με δρομολόγια ΜΜΜ, στοιχεία επικοινωνίας στελεχών διάφορων δημόσιων φορέων, δεδομένα μόλυνσης του περιβάλλοντος ανά περιοχή ή και εγκληματικότητας [18].

1.2 Αντικείμενο διπλωματικής

Στην παρούσα εργασία εξετάζεται η σχέση μεταξύ των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης και της προστασίας των προσωπικών δεδομένων [3]. Δίνεται βάση τόσο στο νομικό πλαίσιο που διέπει τα ανοιχτά και τα προσωπικά δεδομένα όσο και στις τεχνικές που μπορούν να χρησιμοποιηθούν προς αυτό [4]. Εστιάζουμε στον τρόπο με τον οποίο μπορεί να επιτευχθεί η επαναχρησιμοποίηση των ανοιχτών δεδομένων καθώς και η διασύνδεσή τους χωρίς να κινδυνεύει η ιδιωτικότητα των φυσικών προσώπων, σύμφωνα πάντα με όσα ορίζει ο GDPR (Γενικός Κανονισμός για την Προστασία Δεδομένων της ΕΕ) [5].

Ειδικότερα, εξετάζεται και ορίζεται η έννοια των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης (Ready to Link Data, RTLD) και αξιολογείται σύμφωνα με το νομικό πλαίσιο που υφίσταται στην Ελλάδα και την Ευρωπαϊκή Ένωση, ενώ αναζητούνται σημεία συμβατότητας [24]. Καταγράφονται τεχνικοί κίνδυνοι και προκλήσεις που εγείρονται λόγω της διασύνδεσης των δεδομένων, την ανωνυμοποίησή τους και τη δημοσίευσή τους (μεταδεδομένα, διαλειτουργικότητα). Τέλος, παρουσιάζονται πρακτικές λύσεις και μεθοδολογίες τόσο τεχνικές όσο και οργανωτικές.

Τα προβλήματα που επιχειρεί να αντιμετωπίσει η παρούσα εργασία αφορούν την διαρκώς αυξανόμενη διασύνδεση των Ανοιχτών Δεδομένων και το γεγονός ότι αυτή εγείρει κινδύνους για την προστασία της ιδιωτικότητας και της ταυτότητας των υποκειμένων στα οποία ανήκουν, ακόμα και όταν τα δεδομένα δεν περιλαμβάνουν άμεσα προσωπικά στοιχεία [26]. Όσον αφορά τη νομική πλευρά του ζητήματος, καθώς δεν υπάρχουν επί του παρόντος ξεκάθαρα όρια μεταξύ προσωπικών και μη δεδομένων στα πλαίσια των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης υπάρχει και η ανάλογη ασάφεια ως προς την επεξεργασία τους [28]. Οι διαθέσιμες λύσεις για την προστασία των προσωπικών δεδομένων (ανωνυμοποίηση, ψευδονυμοποίηση κ.α.) παρουσιάζουν υψηλή τεχνική πολυπλοκότητα με αποτέλεσμα τη δυσκολία στην εφαρμογή τους από φορείς τόσο του δημόσιου όσο και του ιδιωτικού τομέα χωρίς την ανάλογη -επαρκή- παρακολούθηση. Τέλος, επιχειρείται να εξεταστεί πως μπορεί να γεφυρωθεί η έλλειψη ενιαίων πρακτικών δημοσίευσης των Ανοιχτών Δεδομένων με τρόπο συμβατό με τον GDPR ώστε να αποφεύγονται τα συνεπακόλουθα νομικά ρίσκα που αποθαρρύνουν τη διάθεση των δεδομένων [33], [50].

1.3 Μεθοδολογία Προσέγγισης

Η παρούσα εργασία επιχειρεί να επιλύσει τα προβλήματα που αναφέρονται κατά βάση μέσω θεωρητικής επισκόπησης του θέματος [40]. Εξετάζεται σχετική βιβλιογραφία και νομοθεσία για

την προστασία των προσωπικών δεδομένων και τα Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης [4], [57].

Αναλύονται έννοιες και εργαλεία παρακείμενα του θέματος, ενώ παρουσιάζονται βέλτιστες πρακτικές δημοσίευσης και επεξεργασίας των Ανοιχτών Δεδομένων μέσω της χρήσης κριτηρίων που αξιολογούν τη συμβατότητα των RTLD με τον GDPR [55].

Προτείνεται ακόμα πίνακας απόφασης που διευκολύνει την επιλογή τεχνικών προστασίας των δεδομένων ανάλογα με το είδος τους [28], [35].

Τέλος, αναφέρεται μελέτη περίπτωσης σε υπαρκτό σύστημα ανοιχτών δεδομένων σε χώρα της Ευρωπαϊκής Ένωσης, που αποσκοπεί στην αξιολόγηση κινδύνων που μπορούν να προκύψουν και σχετικές προτάσεις βελτιώσεων [31].

Συνολικά, η εργασία στοχεύει στην κατανόηση του προβλήματος και στη διατύπωση εφαρμόσιμων λύσεων ώστε να επιτευχθεί η επιθυμητή διαφάνεια, η πρόοδος της καινοτομίας αλλά και η προστασία της ιδιωτικότητας των ατόμων στο σύγχρονο ψηφιακό περιβάλλον των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης [6], [24].

1.4 Δομή της διπλωματικής

Στο Κεφάλαιο 2 παρουσιάζεται το θεωρητικό πλαίσιο των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης, οι τομείς στους οποίους χρησιμοποιούνται και τα πλεονεκτήματά τους. Ακόμα, ορίζονται τα προσωπικά δεδομένα και οι κατηγορίες τους και η έννοια της ιδιωτικότητας στην ψηφιακή εποχή. Το Κεφάλαιο 3 αναφέρεται στο νομικό πλαίσιο της προστασίας των δεδομένων, τον Κανονισμό της ΕΕ GDPR και άλλα εθνικά και διεθνή νομικά πλαίσια, τη συμβατότητα των Ανοιχτών Δεδομένων με αυτά και τα δικαιώματα των υποκειμένων. Στο Κεφάλαιο 4 αναφέρονται οι ηθικές και τεχνικές προκλήσεις, τεχνικές προστασίας των προσωπικών δεδομένων και κίνδυνοι που ελλοχεύουν, διαλειτουργικότητα και ασφάλεια. Στο Κεφάλαιο 5 βλέπουμε βέλτιστες πρακτικές για την προστασία των δεδομένων, υφιστάμενες πολιτικές και πρωτόκολλα και την ισορροπία διαφάνειας και ιδιωτικότητας. Το Κεφάλαιο 6 αναφέρει μελέτη περίπτωσης στην ΕΕ. Το Κεφάλαιο 7 συγκεντρώνει τα συμπεράσματα της εργασίας.

2 *Θεωρητικό Πλαίσιο*

2.1 Ορισμός και Αρχές των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης (Ready to Link Data-RTLD)

Αναφορικά με τα Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης, πρόκειται για δεδομένα που θα πρέπει να πληρούν κάποιες προϋποθέσεις [1], [2]. Τα Δεδομένα θα πρέπει να είναι Ανοιχτά, δηλαδή η πρόσβαση σε αυτά να είναι ελεύθερη [56], θα πρέπει επίσης να μπορούν, υπό τις όποιες προϋποθέσεις, να επαναχρησιμοποιηθούν από τους έχοντες πρόσβαση σε αυτά ώστε να μπορούν να παράγουν χρήσιμη για τον κάθε σκοπό πληροφορία [27]. Θα πρέπει επίσης να είναι Συνδεδεμένα, ήτοι να διασυνδέονται μεταξύ τους μέσω μοναδικών αναγνωριστικών [3], πρακτική που καθιστά δυνατή τη δημιουργία ενός δικτύου που επιτρέπει το διαμοιρασμό της γνώσης, αφού γίνεται χρήση και σύνδεση δεδομένων από πολυάριθμες πηγές [51]. Η πρακτική αυτή επιτρέπει την εξόρυξη νέας πληροφορίας και παράλληλα μπορεί να συνεισφέρει στην ενίσχυση της διαφάνειας, αρχής η οποία θεωρείται θεμελιώδης για το Δημοκρατικό Πολίτευμα όπως έχει εξελιχθεί στην σύγχρονη εποχή και όπως συνεχίζει να εξελίσσεται, με τους πολίτες των κρατών-ιδιαίτερα της Δύσης – να επιθυμούν να έχουν πρόσβαση στις πληροφορίες που αφορούν τους ίδιους και τον τόπο διαβίωσής τους αλλά και τους Κυβερνώντες, καθώς και στον τρόπο διακυβέρνησης και το σχεδιασμό πολιτικής, εθνικής αλλά και διεθνούς [5]. Η καινοτομία τους λοιπόν έγκειται στο γεγονός ότι τα δεδομένα οργανώνονται και διατίθενται στο διαδίκτυο, συνδέονται μεταξύ τους μέσω της χρήσης πολλών και διαφορετικών πηγών και είναι ευκολότερα κατανοητά και κατά συνέπεια χρήσιμα [13]. Η πληροφορία ενοποιείται, είναι εύκολα προσβάσιμη και η γνώση που παράγεται οδηγεί σε πιο ολοκληρωμένες υπηρεσίες [11].

Μία εκ των βασικών αρχών που διέπουν τα Συνδεμένα Ανοιχτά Δεδομένα είναι η μοναδικότητα της πληροφορίας που λαμβάνεται, ώστε να αποφεύγεται η επανάληψη εννοιών και δεδομένων από διαφορετικές πηγές [8]. Σημαντική είναι επίσης η δυνατότητα να υπάρχει πρόσβαση μέσω διαδικτύου σε όλα αυτά τα δεδομένα, το να είναι αυτά σαφή και κατανοητά και να δύναται ο χρήστης να τα διαβάσει με ευκολία χρησιμοποιώντας εξοπλισμό και λογισμικό που έχει ήδη στη διάθεσή του [26], ώστε να μπορεί να γίνει χρήση τους για την παραγωγή γνώσης,

καθώς και φυσικά να συνδέονται με άλλα σχετικά δεδομένα και να μπορεί να δημιουργηθεί ένα δίκτυο πληροφορίας [44].

2.1.1 Ιδιαιτερότητες και προκλήσεις

Με μία πρώτη σκέψη, η έννοια των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης μπορεί να οδηγήσει στην πεποίθηση ότι είναι το κλειδί για ένα πολιτικό σύστημα που βασίζεται στη διαφάνεια και έχει ανθρωποκεντρική προσέγγιση, θέτοντας στο προσκήνιο την κοινωνία της πληροφορίας και των ανοιχτών πολιτικών πρακτικών [43]. Με μία δεύτερη, όμως, ματιά μπορεί κάποιος εύκολα να συνειδητοποιήσει πως εγείρονται θέματα που άπτονται της προστασίας των προσωπικών δεδομένων [22].

Πιθανά προβλήματα που μπορούν να προκύψουν από τη διάθεση των δεδομένων στο ευρύ κοινό, και συγκεκριμένα από τη δυνατότητα διασύνδεσης αυτών, είναι καταρχήν η πιθανότητα να αποκαλυφθούν προσωπικά δεδομένα ατόμων και πληροφορίες που δεν ήταν αρχικά εμφανείς μέσα από μία και μόνο βάση δεδομένων [7]. Ναι μεν ενισχύεται η διαφάνεια και η καινοτομία, αλλά ταυτόχρονα ενισχύεται και ο κίνδυνος ταυτοποίησης ατόμων και αποκάλυψης ευαίσθητων πληροφοριών [42].

Ένα άλλο πρόβλημα που προκύπτει, τεχνικής κατά βάση φύσεως, είναι η ασυμβατότητα των δεδομένων. Τα συνδεδεμένα δεδομένα χρησιμοποιούν διαφορετικές πηγές για την παραγωγή πληροφορίας, αλλά για να γίνει η σύνδεση αυτή απαιτούνται πρότυπα και ορολογίες συμβατά μεταξύ τους [17].

2.1.2 Συμβιβασμός Ανοιχτών Δεδομένων και Ιδιωτικότητας

Όπως έχουμε ήδη αναφέρει, η πρακτική της δημοσίευσης των δεδομένων έχει ως αποτέλεσμα την ενίσχυση της διαφάνειας και την προώθηση της καινοτομίας, αλλά ταυτόχρονα δημιουργεί κινδύνους για τις ιδιωτικές πληροφορίες των μεμονωμένων ατόμων μέσω του κινδύνου ταυτοποίησης [19]. Παρατηρείται λοιπόν η ύπαρξη επιτακτικής ανάγκης για ένα ισχυρό πλαίσιο που θα προάγει την ισορροπία μεταξύ της διάθεσης των ανοιχτών δεδομένων και της προστασίας των προσωπικών δεδομένων [33]. Ένα τέτοιο πλαίσιο θα πρέπει να λαμβάνει υπόψη τους πιθανούς κινδύνους που εγείρονται για την ιδιωτικότητα των ατόμων, παρουσιάζοντας μία εκτίμηση του εκάστοτε βαθμού κατά τον οποίο τα εν λόγω δεδομένα κινδυνεύουν να αποκαλύψουν ευαίσθητες προσωπικές πληροφορίες ατόμων [14], ενώ ταυτόχρονα να υπολογίζει και τα πιθανά οφέλη της δημοσίευσης των δεδομένων, καθώς αυτά θα μπορούσαν να προσθέσουν αξία σε πιθανά κοινωνικά, πολιτικά ή και οικονομικά διαβήματα [46]. Σε κάθε περίπτωση, αναζητείται η χρυσή τομή που θα επιτρέψει τη δημιουργία διαδικασιών και μέτρων προστασίας που με τη σειρά τους θα επιτρέψουν να αναπτυχθούν πολιτικές και τεχνολογίες που θα διασφαλίζουν την προστασία των προσωπικών δεδομένων σε όλη τη διάρκεια ζωής των βάσεων δεδομένων που χρησιμοποιούνται [31].

2.1.3 Υπεύθυνη Διαχείριση Προσωπικών Δεδομένων

Με βάση τα παραπάνω, μία πρώτη σκέψη για τη διαχείριση του προβλήματος του συμβιβασμού μεταξύ της χρήσης των ανοιχτών δεδομένων και της προστασίας των προσωπικών δεδομένων είναι η υπεύθυνη διαχείριση αυτών [40]. Η επίτευξη ισορροπίας μεταξύ των δύο μπορεί να επιτευχθεί μέσω της διεξαγωγής αναλύσεων που θα αξιολογούν τους πιθανούς κινδύνους δημοσιοποίησης προσωπικών δεδομένων και των αναμενόμενων οφελών που δύνανται να επιτευχθούν [12]. Ως προς αυτό, είναι ζωτικής σημασίας να λαμβάνεται υπόψη η προστασία της ιδιωτικότητας σε κάθε στάδιο του κύκλου ζωής των βάσεων δεδομένων, από τη συλλογή αυτών μέχρι και τη διαγραφή τους [36]. Για να επιτευχθεί αυτό, είναι σημαντική η ανάπτυξη πολιτικών και διαδικασιών που θα διαχειρίζονται την ιδιωτικότητα των δεδομένων σε επίπεδο οργανισμών [23]. Για την αύξηση της εμπιστοσύνης του κοινού στις διαδικασίες, είναι σκόπιμη και η συμμετοχή του στη διαδικασία λήψης των αποφάσεων, ενισχύοντας έτσι και τη διαφάνεια [18].

2.1.4 Εκτίμηση Κινδύνου Ιδιωτικότητας Δεδομένων

Για την επιτυχή εκτίμηση του κινδύνου να διαρρεύσουν τα προσωπικά δεδομένα των ατόμων και να γίνει ταυτοποίησή τους μπορούν να χρησιμοποιηθούν ορισμένα μοντέλα εκτίμησης του εν λόγω κινδύνου [37]. Μεταξύ των πρακτικών που μπορούν να αξιοποιηθούν, είναι να αναλύονται τα χαρακτηριστικά των εκάστοτε δεδομένων [21], να υπολογίζεται ο αναμενόμενος κίνδυνος για τα προσωπικά δεδομένα που δημοσιοποιούνται σε σχέση πάντα με τα αναμενόμενα οφέλη [6] καθώς και η εφαρμογή μέτρων που θα μετριάζουν τον κίνδυνο, όπως η ανωνυμοποίηση των δεδομένων [30].

2.2 Πλεονεκτήματα και Εφαρμογές των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης στον Δημόσιο και Ιδιωτικό Τομέα

Τα οφέλη που προσφέρουν τα Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης και η πρόοδος που μπορεί να σημειώσει όχι μόνο το πολιτικό σύστημα αλλά και η κοινωνία γενικότερα, από τη δημόσια διοίκηση μέχρι την εξέλιξη της επιχειρηματικότητας, τα πλεονεκτήματα που μπορούν να δρέψουν η ακαδημαϊκή κοινότητα μέσω της διεξαγωγής ερευνών αλλά και οι πολίτες στην καθημερινή τους ζωή, εύκολα γίνονται αντιληπτά [4], [7]. Η ελεύθερη πρόσβαση σε ένα μεγάλο όγκο δεδομένων είναι ευρέως αποδεκτό ότι προωθεί την καινοτομία, τη διαφάνεια αλλά και τη συμμετοχή των πολιτών στη λήψη αποφάσεων που τους αφορούν [27], που είναι άλλωστε και το ζητούμενο σε μια εποχή που η ηλεκτρονική και συμμετοχική διακυβέρνηση κερδίζει διαρκώς έδαφος [38]. Κρίνεται λοιπόν σκόπιμο να δούμε τα πλεονεκτήματα που προσφέρει η πρακτική αυτή αναλυτικότερα.

2.2.1 Πλεονεκτήματα των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης

Όπως έχουμε ήδη αναφέρει, η χρήση των Ανοιχτών Δεδομένων συμβάλει στη Διαφάνεια των πολιτικών πρακτικών και των κινήσεων των πολιτικών προσώπων και κατά συνέπεια στην έννοια της λογοδοσίας [19]. Όταν τα Δεδομένα είναι Ανοιχτά και διαθέσιμα προς όλους τους ενδιαφερόμενους, η Διαφάνεια ενισχύεται και έχει ως αποτέλεσμα αφενός τη μείωση της διαφθοράς [20], αφετέρου την αύξηση της εμπιστοσύνης των πολιτών στους Θεσμούς [44]. Όλο αυτό γίνεται ευκολότερα κατανοητό αν σκεφτούμε πως η πρόσβαση που έχουν πολίτες και Τύπος σε πληροφορίες που αφορούν κρατικές δαπάνες και αποφάσεις προωθούν τον έλεγχο των κινήσεων των Θεσμών και της δράσης των δημόσιων φορέων [42]. Η Δημόσια Διοίκηση και οι Θεσμοί επιπλέον μπορούν να εκμεταλλευτούν τον όγκο δεδομένων που έχουν πλέον στη διάθεσή τους ώστε να βελτιώσουν την αποτελεσματικότητά τους [12] καθώς και να επιτύχουν το στόχο της διαλειτουργικότητας, που θα επιτρέψει την ανταλλαγή πληροφορίας και δεδομένων μεταξύ των υπηρεσιών και θα διευκολύνει τη λειτουργία τους και την εξυπηρέτηση των πολιτών [26]. Τέλος, η λήψη αποφάσεων θα μπορεί πλέον να στηρίζεται σε απτά δεδομένα και κατά συνέπεια να είναι σύμφωνη με τη γνώμη του εντολέα [17].

Ταυτόχρονα ενισχύεται το ζητούμενο της αύξησης της συμμετοχής των πολιτών στις πολιτικές αποφάσεις. Οι πολίτες πλέον έχουν στη διάθεσή τους εργαλεία που βασίζονται στην τεχνολογία των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης ώστε να συμμετάσχουν στη λήψη -εμπεριστατωμένων – αποφάσεων [24], ενώ ενημερώνονται έγκαιρα και έγκυρα για ζητήματα εγχώριας και διεθνούς πολιτικής, με τη δυνατότητα να προσφέρουν ταυτόχρονα γνώμες και απόψεις [8].

Ένας τομέας που μπορεί εξίσου να ωφεληθεί και να δημιουργήσει γνώση που με τη σειρά της θα ωφελήσει το ευρύ κοινό είναι ο ακαδημαϊκός. Έχοντας στη διάθεσή του ένα τεράστιο όγκο δεδομένων τα οποία είναι επίκαιρα και έγκυρα, μπορεί να προωθήσει την παραγωγή γνώσης και να επεξεργαστεί σύνθετα φαινόμενα, ενισχύοντας τα οφέλη για το ευρύ κοινό [5], [47].

Τα παραπάνω έχουν ως σημείο αναφοράς τη Δημόσια Διοίκηση. Η χρήση όμως των Ανοιχτών Δεδομένων μπορεί και πρέπει να επεκταθεί στον ιδιωτικό τομέα. Δίνεται μέσω της ανάλυσής τους η δυνατότητα σε επιχειρήσεις να αναπτύξουν προϊόντα και υπηρεσίες χωρίς το κόστος της συλλογής των δεδομένων, γεγονός που αποτελεί σημαντικό μοχλό οικονομικής και τεχνολογικής καινοτομίας [3], [29].

2.2.2 Εφαρμογές στο Δημόσιο Τομέα

Προσδιορίζοντας στην πράξη τους τομείς που μπορεί να χρησιμοποιηθεί ην τεχνολογία των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης στον Δημόσιο Τομέα, βλέπουμε ότι ενισχύεται η διαφάνεια καθώς οι προϋπολογισμοί είναι πλέον ανοιχτοί και οι συμβάσεις δημόσιες [19]. Πλατφόρμες όπως η Διαύγεια και το gov.gr, ακόμα και Ευρωπαϊκές βάσεις δεδομένων δημοσιοποιούν δεδομένα σχετικά με τις δημόσιες δαπάνες [20], [44]. Ως έχει αναφερθεί παραπάνω, η δεδομένη πρακτική ενισχύει τη διαφάνεια των αποφάσεων και των δαπανών και συμβάλει στον έλεγχο των κινήσεων από τους πολίτες [42].

Επιπρόσθετα οφέλη της δημοσιοποίησης των δεδομένων μπορούν να παρατηρηθούν στους τομείς του περιβάλλοντος και την χάραξη πολιτικής που το αφορά. Με τη δημοσιοποίηση δεδομένων που αφορούν την ποιότητα του αέρα και του νερού, τις δασικές εκτάσεις και τις μετεωρολογικές συνθήκες, για να αναφέρουμε ορισμένα παραδείγματα, μορφοποιούνται η περιβαλλοντική πολιτική και οι ανάλογες δράσεις των φορέων [5]. Ταυτόχρονα, η ίδια τεχνολογία μπορεί να προσφέρει παραγωγή πληροφορίας και γνώσης που θα βελτιστοποιήσει τους τομείς της υγείας και της δημόσιας ασφάλειας, συγκεντρώνοντας δεδομένα που αφορούν μονάδες υγείας, ιατρικές δαπάνες, επιδημιολογικές κρίσεις όπως η πρόσφατη του κορονοϊού, βελτιώνοντας τη χάραξη στρατηγικού σχεδιασμού για την αντιμετώπιση των εκάστοτε κρίσεων και εξοικονομώντας έτσι πολύτιμο χρόνο και πόρους [26], [12].

2.2.3 Εφαρμογές στον Ιδιωτικό Τομέα

Η ανάπτυξη του Ιδιωτικού Τομέα φέρνει ευκαιρίες ως προς την οικονομική και τεχνολογική ανάπτυξη, προσφέροντας θέσεις εργασίας και εργαλεία για την περεταίρω διευκόλυνση ιδιωτών και Δημοσίου εξίσου [3]. Αναφέρονται παρακάτω ορισμένα μόνο παραδείγματα των οφελών που μπορούν να έχουν τα άτομα και οι επιχειρήσεις καθώς και ο τομέας της επιχειρηματικότητας από την ελεύθερη διάθεση και χρήση των δεδομένων που συλλέγονται από τους Φορείς [29].

Η τεχνολογία των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης προσφέρει δυνατότητες ανάπτυξης εφαρμογών και ψηφιακών υπηρεσιών που άπτονται τομέων όπως ο τουριστικός, με τη δημιουργία ψηφιακών χαρτών και άλλων εφαρμογών διάθεσης της τουριστικής πληροφορίας [45], ενώ ταυτόχρονα δίνεται και η δυνατότητα μέσω τεχνολογιών που διαχειρίζονται δεδομένα να γίνεται ανάλυση ποικίλων τομέων όπως η αγορά ακινήτων ή και η κυκλοφορία [36], για να αναφέρουμε μόνο λίγα παραδείγματα.

Η ανάλυση των Μεγάλων Δεδομένων (Big Data) σε συνδυασμό πάντα με την διάθεση των Ανοιχτών Δεδομένων σε ιδιωτικές επιχειρήσεις προς χρήση μπορεί να επιτρέψει σε αυτές την πρόβλεψη των τάσεων που θα επικρατούν στην αγορά που τις αφορά και κατά συνέπεια να κατανοήσουν καλύτερα τη συμπεριφορά των καταναλωτών και να προσαρμόσουν έτσι τις υπηρεσίες και τα προϊόντα τους στη ζήτηση αυτών, συμβάλλοντας και πάλι στην οικονομική ανάπτυξη αρχικά της εκάστοτε εταιρίας και στη συνέχεια της κοινωνίας που αναπτύσσεται και ευημερεί [18], [50].

Στον τομέα τώρα των νομικών και χρηματοοικονομικών υπηρεσιών, η πρόσβαση στα ανάλογα δεδομένα μπορεί να οδηγήσει στην παροχή συμβουλευτικών υπηρεσιών σε άτομα εύκολα και εμπεριστατωμένα, μειώνοντας έτσι την αβεβαιότητα που αντιμετωπίζουν οι αποδέκτες των υπηρεσιών αυτών [46].

2.2.4 Ισορροπία RTLD με την Ιδιωτικότητα των ατόμων

Όπως έχουμε ήδη αναφέρει, τα πλεονεκτήματα που προσφέρονται από την ελεύθερη διάθεση και χρήση των δεδομένων με τη μορφή που χαρακτηρίζεται ως Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης είναι πολυάριθμα και άπτονται εξίσου του Δημόσιου και Ιδιωτικού τομέα. Μπορούν να συμβάλουν στην ανάπτυξη του Δημοκρατικού πολιτεύματος, στη συμμετοχή των πολιτών στα

κοινά, στη χρηματοοικονομική και τεχνολογική ανάπτυξη καθώς και στην παραγωγή νέας γνώσεις από ακαδημαϊκά ιδρύματα [4], [7], [17]. Η ελεύθερη χρήση όμως ενός ανεξέλεγκτου και αφιλτράριστου όγκου δεδομένων μπορεί να θέσει σε κίνδυνο την ιδιωτικότητα των ατόμων στα οποία αυτά ανήκουν [48], [14]. Είναι λοιπόν απαραίτητο να λαμβάνεται υπόψη ο κίνδυνος παραβίασης των προσωπικών δεδομένων και ο τρόπος με τον οποίο χρησιμοποιείται η πληροφορία που αντλείται από τα Ανοιχτά Δεδομένα. Θα ήταν ως εκ τούτου σκόπιμη η χρήση τεχνολογιών που θα ενσωματωθούν στη δημιουργία των βάσεων δεδομένων που θα συμβάλλουν στο να εφαρμόζεται η ιδιωτικότητα εξ αρχής [35], καθώς και η ύπαρξη μηχανισμών αξιολόγησης ρίσκου που θα διασφαλίσουν την αξιοποίηση των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης με τρόπο υπεύθυνο και φυσικά χαμηλό ρίσκο επαναταυτοποίησης [28], [30].

2.3 Ορισμός και Βασικές Κατηγορίες Προσωπικών Δεδομένων

Για να μπορέσουμε να μιλήσουμε για την προστασία των Προσωπικών Δεδομένων θα πρέπει αρχικά να ορίσουμε τι ακριβώς είναι τα δεδομένα αυτά. Πρόκειται για ένα βασικό συστατικό στοιχείο της συζήτησης που αφορά τη διάθεση και χρήση των Ανοιχτών Δεδομένων, καθώς και βασικό στοιχείο του σύγχρονου Δικαίου που στοχεύει στην προστασία της ιδιωτικής ζωής των ατόμων στα σύγχρονα δημοκρατικά πολιτεύματα [8]. Για τον ορισμό και καθώς άπτεται της παρούσης εργασίας, συμβουλευόμαστε το Γενικό Κανονισμό για την Προστασία Δεδομένων της Ευρωπαϊκής Ένωσης (GDPR). Σύμφωνα με τον κανονισμό, ως προσωπικό δεδομένο θεωρείται κάθε πληροφορία που αφορά ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Ως ταυτοποιήσιμο πρόσωπο ορίζεται ένα πρόσωπο που μπορεί να αναγνωριστεί με τρόπο άμεσο ή έμμεσο μέσω του ονόματός του, του αριθμού ταυτότητάς του, μέσω δεδομένων της τοποθεσίας του, διαδικτυακών αναγνωριστικών ή ενός ή περισσότερων παραγόντων που θα δείξουν τη φυσική, γενετική, οικονομική, πολιτιστική ή κοινωνική ταυτότητά του [13], [16].

Σύμφωνα με τον κανονισμό της Ευρωπαϊκής Ένωσης (GDPR), υφίσταται αφενός η έννοια των απλών προσωπικών δεδομένων, ήτοι πληροφοριών όπως το ονοματεπώνυμο του ατόμου, η διεύθυνση κατοικίας του, η ημερομηνία γέννησης, η φωτογραφία του καθώς και τα στοιχεία επικοινωνίας του, όπως αριθμός τηλεφώνου και διεύθυνση ηλεκτρονικού ταχυδρομείου [9]. Τα προσωπικά αυτά δεδομένα είναι απαραίτητα για τις συνδιαλλαγές του ατόμου με δημόσιους οργανισμούς και υπηρεσίες και δεν θεωρούνται ευαίσθητα, αλλά σε κάθε περίπτωση υπόκεινται σε αυστηρούς κανόνες διαχείρισης κατά τη χρήση τους [32].

Ως ευαίσθητα ορίζονται τα δεδομένα που αφορούν ένα άτομο και τα δεδομένα υγείας αυτού, τη φυλετική και εθνική του καταγωγή, τις πολιτικές, θρησκευτικές και φιλοσοφικές του πεποιθήσεις, τυχόν συνδικαλιστική του δραστηριότητα, γενετικά και βιομετρικά του δεδομένα όπως τα δαχτυλικά αποτυπώματα και το σεξουαλικό του προσανατολισμό [10], [11]. Σύμφωνα με τον GDPR, τα δεδομένα αυτά μπορούν να τεθούν υπό επεξεργασία μόνο με τη ρητή συγκατάθεση του ατόμου και για λόγους όπως η προστασία της δημόσιας υγείας ή για νομικές υποχρεώσει ή για την προστασία ζωτικών συμφερόντων ή σε περιπτώσεις που τίθεται θέμα εθνικής ασφάλειας [33].

2.3.1 Ψευδονυμοποίηση και Ανωνυμοποίηση

Δύο από τις πρακτικές που χρησιμοποιούνται για την προστασία των Προσωπικών Δεδομένων είναι αυτές της ανωνυμοποίησης και της ψεδωνυμοποίησης [6], [31]. Στην πρώτη περίπτωση πρόκειται για την εξ ολοκλήρου αφαίρεση της ταυτοποίησης, έτσι ώστε τα δεδομένα που διατίθενται είναι πλέον μη προσωπικά. Σε αυτή την περίπτωση η παραγόμενη πληροφορία δεν καλύπτεται πλέον από τον κανονισμό GDPR [30]. Στην περίπτωση της ψευδωνυμοποίησης, υπάρχει αντικατάσταση των προσωπικών δεδομένων με κωδικό ή κάποιο άλλο μη ταυτοποιήσιμο αναγνωριστικό και έτσι μειώνεται ο κίνδυνος επαναταυτοποίησης του ατόμου ενώ τα δεδομένα παραμένουν προσωπικά και άρα καλύπτονται από τον κανονισμό GDPR [28].

Η επεξεργασία λοιπόν των προσωπικών δεδομένων κατά τη χρήση των Συνδεδεμένων Προσωπικών Δεδομένων με τη χρήση αυτών των τεχνικών τείνει να εξισορροπήσει τη χρησιμότητα των δεδομένων αυτών και την προστασία της ιδιωτικότητας των ατόμων [30], [6].

2.3.2 Προκλήσεις της Χρήσης RTLD στη Σύγχρονη Εποχή

Η ύπαρξη της τεχνολογίας των Μεγάλων δεδομένων και αυτή των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης έχει αυξήσει τον κίνδυνο ταυτοποίησης του ατόμου άμεσα ή έμμεσα, μέσω της άντλησης δεδομένων από ποικίλες πηγές [30], [14], [33]. Ακόμα και στην περίπτωση που μία βάση δεδομένων έχει προχωρήσει στη χρήση πρακτικών ανωνυμοποίησης και ψεδωνυμοποίησης, η σύζευξη πληροφοριών με αυτές από άλλες βάσεις δεδομένων μπορεί σε περιπτώσεις να οδηγήσει στην αποκάλυψη της ταυτότητας, και όχι μόνο, ενός ατόμου [31]. Για παράδειγμα, η δυνατότητα κάποιος να πληροφορηθεί τα δρομολόγια των λεωφορείων σε συνδυασμό με το πρόγραμμα εργασίας των οδηγών και τη λίστα των εργαζομένων σε αυτά, μπορεί εκτός από τη ταυτότητα ενός ατόμου να αποκαλύψει και την τοποθεσία του σε κάθε στιγμή της μέρας [10], [34]. Έτσι λοιπόν, καθίσταται αναγκαία η εκτίμηση των κινδύνων επαναταυτοποίησης πριν γίνει διαθέσιμο προς όλους το εκάστοτε σύνολο δεδομένων [28], [36], ενώ κρίνεται σκόπιμο να συλλέγονται μόνο τα απαραίτητα ως προς το σκοπό χρήσης τους δεδομένα, ήτοι η Αρχή της Ελαχιστοποίησης [13], [16]. Τέλος, λαμβάνοντας υπόψη και τον ανθρώπινο παράγοντα και για την ελαχιστοποίηση της περίπτωσης του ανθρώπινου λάθους, κρίνεται θεμιτή η διαρκής εκπαίδευση και ευαισθητοποίηση των φορέων που διαχειρίζονται τα δεδομένα, των στελεχών τους αλλά και των χρηστών των βάσεων [11], [29], [35].

Βασικές Έννοιες Προσωπικών Δεδομένων (Πίνακας 1)

Κατηγορία	**Περιγραφή**	**Παραδείγματα**
Προσωπικά Δεδομένα	Κάθε πληροφορία σχετική με ταυτοποιημένο ή ταυτοποιήσιμο πρόσωπο	Όνομα, διεύθυνση, τηλέφωνο, φωτογραφία, ηλεκτρονικό ταχυδρομείο
Απλά Προσωπικά	Πληροφορίες που δεν είναι ευαίσθητες αλλά συνδέονται με	Ημερομηνία γέννησης

Δεδομένα	την ταυτότητα του ατόμου	
Ευαίσθητα Προσωπικά Δεδομένα	Δεδομένα που άπτονται ευαίσθητων πτυχών της ταυτότητας του ατόμου	Δεδομένα υγείας, σεξουαλικός προσανατολισμός, θρησκευτικές και πολιτικές πεποιθήσεις
Ψευδονυμοποίηση	Αντικατάσταση ταυτότητας με άλλο αναγνωριστικό	Αντικατάσταση ονόματος με κωδικό
Ανωνυμοποίηση	Παντελής αφαίρεση κάθε στοιχείου ταυτοποίησης	Σύνολο δεδομένων που δεν μπορεί να εντοπιστεί η ταυτότητα
Ταυτοποιήσιμο Πρόσωπο	Άτομο που μπορεί να αναγνωριστεί άμεσα ή έμμεσα	Οδηγός λεωφορείου της γραμμής 5 που απασχολείται από το 2023
Κίνδυνος Επαναταυτοποίησης	Δυνατότητα επαναταυτοποίησης προσώπου μέσω διασύνδεσης βάσεων δεδομένων	Χρήση Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης συνδυαστικά με εμπορικά δεδομένα
Αρχή της Ελαχιστοποίησης	Συλλέγονται μόνο τα απαραίτητα για το σκοπό δεδομένα	Δεν ζητείται η οικογενειακή κατάσταση αν δεν αφορά την υπηρεσία συλλογής των δεδομένων.

2.4 Η Έννοια της Ιδιωτικότητας στην Ψηφιακή Εποχή

Όταν μιλάμε για την ιδιωτικότητα των ατόμων, πρόκειται για ένα θεμελιώδες ανθρώπινο δικαίωμα [4], [23]. Συνδέεται άμεσα με τις έννοιες της ελευθερίας, της αυτονομίας και της ανθρώπινης αξιοπρέπειας. Η έννοια της ιδιωτικότητας πρωτίστως αναφέρεται στο αναφαίρετο δικαίωμα του ατόμου να παραμένει μόνος του, ήτοι να έχει τον πλήρη έλεγχο των πληροφοριών που το αφορούν και να αποφασίζει ως προς τη διάθεσή τους [20], [40]. Στη σημερινή ψηφιακή εποχή, η έννοια έχει πλέον διαφοροποιηθεί [21].

2.4.1 Η έννοια της Ιδιωτικότητας και οι Ψηφιακές Τεχνολογίες

Στη σημερινή εποχή που κυριαρχούν οι ψηφιακές τεχνολογίες και που όλες οι λειτουργίες του Κράτους τείνουν να ψηφιοποιηθούν, παρατηρείται όπως αναμένεται μία μαζική ψηφιοποίηση των δεδομένων [45]. Τα τελευταία χρόνια σημειώνεται μεγάλη εξάπλωση των κοινωνικών δικτύων (facebook, instagram κ.α.), των έξυπνων συσκευών (IoT-Internet of Things) και τα μεγάλα δεδομένα (Big Data) [5], [17]. Όλο αυτό έχει δημιουργήσει μια κατάσταση εντός της οποίας έχουν αρχίσει να αμφισβητούνται αλλά και να επαναπροσδιορίζονται πολλές έννοιες, μεταξύ των οποίων και αυτή της ιδιωτικότητας [10]. Παρατηρείται μία διαρκής δημιουργία νέας πληροφορίας μέσω αγορών, συσκευών και περιήγησης στο διαδίκτυο, μεταξύ άλλων, και η πληροφορία αυτή διαμοιράζεται άμεσα [6]. Ο χρήστης δεν είναι σε θέση να ελέγξει τον τρόπο με τον οποίο αυτή αναλύεται, και άρα όπως αναφέραμε παραπάνω καταλύεται η παραδοσιακή έννοια της ιδιωτικότητας [14], [43].

2.4.2 Θεώρηση της Ιδιωτικότητας ως Δικαίωμα Ελέγχου της Πληροφορίας

Η σύγχρονη έννοια της ιδιωτικότητας δεν εντοπίζεται απλώς στο δικαίωμα του ατόμου στην απομόνωση. Αφορά το δικαίωμα του καθενός στο να ελέγχει τα προσωπικά του δεδομένα και τις πληροφορίες που τον αφορούν [19]. Η έννοια πλέον αναφέρεται στην συγκατάθεση που πρέπει να έχει δώσει το κάθε άτομο για την επεξεργασία των δεδομένων που τον αφορούν, τη δυνατότητα πρόσβασης και κατά περίπτωση διόρθωσης των προσωπικών του στοιχείων, όπως επίσης θα πρέπει να έχει και τη δυνατότητα να επιλέξει τη διαγραφή των πληροφοριών που αναφέρονται σε αυτόν ή τον περιορισμό της χρήσης τους [13], [24]. Τέλος, σε περίπτωση που οι προσωπικές του πληροφορίες πρόκειται να τεθούν υπό επεξεργασία, είναι δικαίωμα του ατόμου η ενημέρωση ως προς αυτό [7], [15].

Όπως βλέπουμε, η έννοια της Ιδιωτικότητας έχει λάβει κατά πολύ διαφορετικές διαστάσεις στη σύγχρονη εποχή της Ψηφιακής Τεχνολογίας, με το άτομο να μην είναι πλέον σε θέση να έχει τον πλήρη έλεγχο των προσωπικών του δεδομένων, αλλά μερικό έλεγχο στον τρόπο με τον οποίο οι πληροφορίες που συλλέγονται θα διατίθενται σε τρίτους και θα επεξεργάζονται [22].

2.4.3 Ηθική και Κοινωνική Διάσταση της Ιδιωτικότητας στην Ψηφιακή Εποχή

Αναφερόμενοι στο πρόβλημα της Ιδιωτικότητας στη σημερινή εποχή εν μέσω της αύξησης της πληροφορίας που διατίθεται στο διαδίκτυο και ενώ ένας μεγάλος όγκος αυτής αναφέρεται σε προσωπικά δεδομένα, σίγουρα η πρώτη σκέψη που λαμβάνει χώρα θα αφορά την τεχνική και νομική διάσταση της προστασίας του ατόμου και των δεδομένων του [9], [41].

Η όλη υπόθεση όμως έχει και πτυχές ηθικές, κοινωνικές και σε πολλές περιπτώσεις, πολιτικές [42], [47]. Βεβαίως και συνδέονται στενά με το νομικό πλαίσιο που διέπει τη διαχείριση της προσωπικής πληροφορίας, Ελλείψεις στον τομέα της προστασίας μπορεί να έχουν επιπτώσεις σε πολλές πτυχές της ζωής των εμπλεκόμενων ατόμων, κυρίως στην εμπιστοσύνη που δείχνουν οι πολίτες στο Κράτος και τις τεχνολογίες που αυτό χρησιμοποιεί εάν υφίσταται η αίσθηση ότι παραβιάζεται η Ιδιωτικότητα [25]. Το ίδιο το άτομο υπάρχει η πιθανότητα να προβεί σε μείωση της συμμετοχής του στα κοινά εάν νιώσει πως η ψηφιακή επιτήρηση είναι αυξημένη, σε μία προσπάθεια να προστατεύσει την Ιδιωτικότητά του [48], [12]. Τέλος, υπάρχει πάντα ο κίνδυνος χειραγώγησης των αποφάσεων των ατόμων που προβαίνουν σε χρήση των ψηφιακών τεχνολογιών μέσω της προσωποποιημένης πληροφόρησης, ακυρώνοντας έτσι την εμπεριστατωμένη λήψη αποφάσεων που είναι ζωτικής σημασίας για την ορθή διεξαγωγή των δημοκρατικών διαδικασιών [8], [44].

2.4.4 Νέα Εποχή, Νέα Μέτρα

Ενόψει της διατήρησης της προστασίας της Ιδιωτικότητας των ατόμων στη σημερινή εποχή όπου η τεχνολογία των ανοιχτών Δεδομένων έχει έρθει για να μείνει, κρίνεται απαραίτητη η λήψη μέτρων που θα βοηθήσει ως προς αυτό [26], [31].

Οι ψηφιακές τεχνολογίες που χρησιμοποιούνται για τη συλλογή και διάθεση των δεδομένων θα πρέπει να δομούνται με τρόπο τέτοιο ώστε από το σχεδιασμό τους να ενσωματώνεται η αρχή της Ιδιωτικότητας (privacy by design) [36], [18]. Οι κίνδυνοι που μπορεί

να εμφανιστούν καθώς και οι επιπτώσεις που μπορεί να έχουν στη διαρροή προσωπικών δεδομένων θα πρέπει διαρκώς να εκτιμώνται και να προλαμβάνονται, πάντα σε συνδυασμό με την εκτίμηση του ανθρώπινου παράγοντα [11]. Διαχειριστές των δεδομένων αλλά και οι πολίτες που αυτά αφορούν θα πρέπει να ενημερώνονται σχετικά με τη διαδικασία συλλογής και επεξεργασίας τους, ήτοι να καλλιεργηθεί η ψηφιακή παιδεία των χρηστών, μειώνοντας έτσι αφενός τον κίνδυνο που διέπει τη χρήση τους αλλά ταυτόχρονα αυξάνοντας την εμπιστοσύνη στις νέες τεχνολογίες και τις διαδικασίες που αυτές διέπουν [29], [49].

Βασικές Έννοιες Ιδιωτικότητας στην Ψηφιακή Εποχή (Πίνακας 2)

Θεματική Περιοχή	**Περιγραφή-Σημασία**	**Παραδείγματα-Εφαρμογές**
Παραδοσιακή Έννοια	Το δικαίωμα του ατόμου να έχει τον έλεγχο των προσωπικών του πληροφοριών	Δικαίωμα στην απομόνωση, περιορισμένη πρόσβαση τρίτων
Ψηφιακή Μεταμόρφωση	Τα δεδομένα συλλέγονται διαρκώς, μειώνοντας την Ιδιωτικότητα	Cookies, mobile tracking, AI analytics
Ιδιωτικότητα και Έλεγχος	Το άτομο αποφασίζει ποια δεδομένα δίνει, το λόγο διάθεσης, τις προϋποθέσεις	GDPR. Συγκατάθεση, πρόσβαση, διαγραφή.
Απώλεια Ανωνυμίας	Ακόμα και τα ανώνυμα δεδομένα μπορούν να χρησιμοποιηθούν για επαναταυτοποίηση μέσω διαλειτουργίας βάσεων δεδομένων	Σύνδεση RTLD, αναγνώριση προτύπων
Ηθική Διάσταση	Η παραβίαση της Ιδιωτικότητας έχει επιπτώσεις στον περιορισμό της ελευθερίας, στη συμμετοχή στα κοινά και στην εμπιστοσύνη των πολιτών	Φόβος για παρακολούθηση, μείωση συμμετοχής στα κοινά
Κίνδυνοι	Τα προσωπικά δεδομένα χρησιμοποιούνται για την επιρροή των	Χρήση σε εκλογικές καμπάνιες, διαφημίσεις

	ατόμων και των αποφάσεών τους	
Πρακτικές Προστασίας	Δόμηση Βάσεων με ενσωματωμένη προστασία στο στάδιο του σχεδιασμού, διαρκής αξιολόγηση ρίσκων	Privacy by design
Ψηφιακή Παιδεία	Πολίτες πρέπει να γνωρίζουν πώς διαχειρίζονται τα δεδομένα τους, Στελέχη των Φορέων πρέπει να εκπαιδεύονται	Εκπαίδευση, διαφάνεια.

3 *Νομικό Πλαίσιο Προστασίας Δεδομένων*

Ακρογωνιαίος λίθος για την προστασία των προσωπικών δεδομένων στη σύγχρονη ψηφιακή εποχή, αν και η εφαρμογή του περιορίζεται στη επικράτεια της Ευρωπαϊκής Ένωσης, είναι ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) (Κανονισμός (ΕΕ) 2016/679 [13], [31]. Η εφαρμογή του υφίσταται σε όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης και η ισχύς του είναι άμεση, και άρα υπερισχύει και αντικαθιστά προηγούμενες νομοθετικές ρυθμίσεις των κρατών [16].

Σκοπός του κανονισμού είναι η προστασία και ενισχύσει των δικαιωμάτων των ατόμων πάνω στα προσωπικά τους δεδομένα, ενώ καθίστανται υπεύθυνοι οι οργανισμοί που τα συλλέγουν ή/και τα επεξεργάζονται [17[. Η χρησιμότητά του έγκειται στο γεγονός ότι ενσωματώνονται σε αυτόν σύγχρονες αρχές για την ψηφιακή εποχή, χωρίς όμως τεχνολογική χροιά. Αυτό επιτρέπει την ευρεία εφαρμογή του κανονισμού συμπεριλαμβανομένων και περιπτώσεων όπου εφαρμόζονται τεχνολογίες Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης [12], [40].

3.1 Ορισμοί και Βασικά Στοιχεία

Παρακάτω παρατίθενται ορισμένοι βασικοί ορισμοί που αφορούν το αντικείμενό μας και ο ορισμός που δίνεται από τον GDPR.

- Ως προσωπικό δεδομένο ορίζεται κάθε πληροφορία πουη αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο [13].
- Ως Υπεύθυνος Επεξεργασίας ορίζεται το νομικό ή φυσικό πρόσωπο που καθορίζει τους σκοπούς και τα μέσα επεξεργασίας [31].
- Ως Εκτελών (την επεξεργασία) ορίζεται όποιος επεξεργάζεται τα δεδομένα για λογαριασμό του Υπεύθυνου [16].
- Ως Υποκείμενο των Δεδομένων ορίζεται το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα.

3.1.1 Αρχές Επεξεργασίας Προσωπικών Δεδομένων

Σύμφωνα πάντα με τον GDPR, κατά την επεξεργασία των Προσωπικών Δεδομένων θα πρέπει να τηρούνται επτά θεμελιώδεις αρχές [13], [17]. Αυτές είναι:

1. Νομιμότητα, Διαφάνεια και Δίκαιη Επεξεργασία
2. Περιορισμός του σκοπού. Τα δεδομένα που συλλέγονται θα πρέπει να χρησιμοποιούνται μόνο για το συγκεκριμένο σκοπό για τον οποίο και ζητήθηκαν
3. Ελαχιστοποίηση δεδομένων. Θα πρέπει να συλλέγονται μόνο τα απαραίτητα κατά περίπτωση δεδομένα.
4. Ακρίβεια. Τα δεδομένα που συλλέγονται θα πρέπει να είναι ακριβή και επικαιροποιημένα
5. Περιορισμός χρονικής αποθήκευσης. Τα δεδομένα διατηρούνται στις βάσεις δεδομένων για ορισμένο χρονικό διάστημα
6. Ακεραιότητα και εμπιστευτικότητα. Τα δεδομένα πρέπει να προστατεύονται ώστε να διατηρείται η ασφάλειά τους
7. Λογοδοσία. Ο υπεύθυνος της επεξεργασίας των δεδομένων θα πρέπει να συμμορφώνεται με τις ανωτέρω αρχές [40]

3.1.2 Νομικές Βάσεις για την Επεξεργασία των Δεδομένων

Όσον αφορά την επεξεργασία των προσωπικών δεδομένων ενός ατόμου, είναι επιτρεπτή μόνο εφόσον πληρούνται μία ή περισσότερες οριζόμενες νομικές προϋποθέσεις [13]. Το υποκείμενο θα πρέπει να έχει δώσει τη συγκατάθεσή του ως προς αυτό, θα πρέπει να εκπληρώνεται η συμβατική υποχρέωση συλλογής των δεδομένων, να πληρούνται οι νομικές υποχρεώσεις του υπεύθυνου, να προστατεύονται τα υφιστάμενα ζωτικά συμφέροντα, να ασκείται καθήκον δημόσιου συμφέροντος και τέλος να υφίσταται έννομο συμφέρον σε περίπτωση που δεν υπερισχύουν τα δικαιώματα του υποκειμένου, όπως για παράδειγμα το Εθνικό συμφέρον [31], [42].

3.1.3 Υποχρεώσεις για την Ασφάλεια των Δεδομένων

Σύμφωνα με το Γενικό Κανονισμό για την Προστασία Δεδομένων, επιβάλλονται μέτρα ασφάλειας αφενός τεχνικής φύσεως αλλά και οργανωτικά μέτρα [13]. Πρέπει να χρησιμοποιούνται τεχνολογίες ψευδονυμοποίησης και ανωνυμοποίησης, όπως αυτές έχουν αναφερθεί παραπάνω, και κρυπτογραφούνται τα προσωπικά δεδομένα και να εκτιμάται τι αντίκτυπο θα έχει τυχόν διαρροή δεδομένων ή επαναταυτοποίηση ατόμων σε κάθε περίπτωση [40]. Κάθε παραβίαση της Ιδιωτικότητας θα πρέπει να καταγράφεται και να ειδοποιούνται άμεσα εξίσου οι Αρχές αλλά και το άτομο ή άτομα που αφορά η εκάστοτε παραβίαση [31], [42].

Ιδιαίτερα σε περιπτώσεις που δημοσιεύονται Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης, και δύναται η συσχέτιση δεδομένων από διαφορετικές πηγές και άρα η επαναταυτοποίηση ατόμων, και κατά συνέπεια η παραβίαση της Ιδιωτικότητας, η χρήση των ανωτέρω τεχνολογιών και η ασφάλεια των Δεδομένων κρίνεται ως ζωτικής σημασίας [44].

3.1.4 Εφαρμογή του Κανονισμού σε Δημόσιους και Ιδιωτικούς Φορείς

Ο GDPR εφαρμόζεται σε κάθε δομή, είτε αυτή αφορά τους Δημόσιους Φορείς, είτε τον Ιδιωτικό τομέα, όπου υφίσταται διαχείριση ή επεξεργασία Ανοιχτών ή/και Προσωπικών Δεδομένων [13], [16]. Τέτοιες περιπτώσεις μπορεί να αφορούν δήμους, φορολογικές αρχές, εμπορικές επιχειρήσεις μεταξύ άλλων. Όλοι αυτοί οι οργανισμοί, είτε βρίσκονται εντός της Ευρωπαϊκής Ένωσης είτε επεξεργάζονται δεδομένα πολιτών της Ευρωπαϊκής Ένωσης, θα πρέπει να συμορφώνονται με τον Κανονισμό [17].

3.1.5 Privacy by Design και by Default

Επιγραμματικά αναφερόμενοι στις δύο έννοιες, Privacy by Design υφίσταται όταν η προστασία των δεδομένων βρίσκεται ενσωματωμένη εξ αρχής στα πληροφοριακά συστήματα από τον σχεδιασμό τους [42], ενώ στην περίπτωση του Privacy by Default ο τρόπος με τον οποίο ρυθμίζονται τα συστήματα περιορίζει την έκθεση των προσωπικών δεδομένων [44].

3.2 Εθνική Νομοθεσία και Διεθνείς Συνθήκες

Η προστασία των προσωπικών δεδομένων στη σύγχρονη ψηφιακή εποχή δεν αφορά αποκλειστικά την Ευρωπαϊκή Ένωση. Επεκτείνεται στη εθνική και διεθνή πολιτική σκηνή. Στην περίπτωση των κρατών-μελών της Ένωσης έχουμε ήδη πει πως ο κανονισμός εφαρμόζεται υποχρεωτικά σε όλα [13]. Συμπληρωματικά, πολλά κράτη εφαρμόζουν και επιπλέον διατάξεις σε εθνικό επίπεδο, ενώ υφίστανται και διεθνείς συνθήκες για την προστασία των ατόμων-υποκειμένων των δεδομένων και των δικαιωμάτων τους [14].

3.2.1 Εθνικό Πλαίσιο Προστασίας Προσωπικών Δεδομένων-Η Περίπτωση της Ελλάδας

Στην Ελλάδα εφαρμόζεται ο νόμος 4624/2019, ο οποίος ισχύει στα πλαίσια της εφαρμογής του GDPR και εξειδικεύει ορισμένες εκ των προβλέψεων του κανονισμού [13]. Συγκεκριμένα, ορίζει ως εθνική εποπτική αρχή την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), ενώ ρυθμίζονται και θέματα όπως η επεξεργασία των δεδομένων στα πλαίσια του δημόσιου τομέα, προσδιορίζονται οι ευαίσθητες κατηγορίες δεδομένων καθώς και οι διοικητικές κυρώσεις σε περίπτωση παραβίασης του GDPR. Επιπρόσθετα, θέτει περιορισμούς στα δικαιώματα των υποκειμένων όπως αυτά ορίζονται σε περιπτώσεις που η επεξεργασία των δεδομένων έγκειται της εθνικής ή δημόσιας ασφάλειας ή τίθεται θέμα πρόληψης ή δίωξης ποινικών αδικημάτων, όπως για παράδειγμα η άρση του τηλεφωνικού απορρήτου [38] σε περίπτωση κακουργηματικής πράξης.

3.2.2 Διεθνείς Συμβάσεις και Νομοθετικές Πηγές

Ιστορικά η πρώτη διεθνής συνθήκη με νομικά δεσμευτικό χαρακτήρα με στόχο την προστασία των προσωπικών δεδομένων που εφαρμόζεται σε ευρωπαϊκά και μη κράτη, ήταν η σύμβαση 108/1981 του Συμβουλίου της Ευρώπης. Στην επικαιροποιημένη της μορφή 108+/2018 ενισχύονται οι υποχρεώσεις των κρατών κα προβλέπεται ρητά η προστασία του υποκειμένου από αυτοματοποιημένη επεξεργασία και επαναταυτοποίηση [14].

Στην πορεία, ο Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ πλέον αναγνωρίζει ως θεμελιώδες δικαίωμα των ατόμων την προστασία των προσωπικών τους δεδομένων, δικαίωμα διακριτό από την ιδιωτική ζωή [15].

Στη συνέχεια έρχεται η Σύμβαση του ΟΗΕ για τα δικαιώματα του ανθρώπου, όπου με το άρθρο 12 απαγορεύονται ρητά αυθαίρετες παρεμβάσεις στην ιδιωτική ζωή και απαιτείται επιπλέον νομική προστασία από αυτές [32].

Με τις κατευθυντήριες οδηγίες του ΟΟΣΑ των ετών 1982 και 2013 θεσπίζονται διεθνώς αποδεκτές αρχές προστασίας προσωπικών δεδομένων, ήτοι ο περιορισμός του σκοπού, δηλαδή η συλλογή των εκάστοτε προσωπικών δεδομένων πρέπει να έχει ορισμένο σκοπό, τα δεδομένα θα πρέπει να είναι ποιοτικά, να υφίσταται ασφάλεια και λογοδοσία των υπεύθυνων που τα διαχειρίζονται, καθώς να δίνεται και η ρητή συγκατάθεση των υποκειμένων και να υπάρχει διαφάνεια ως προς τη χρήση τους [35].

Όσον αφορά τα κανονιστικά πλαίσια που ισχύουν εκτός ΕΕ, επιγραμματικά αναφέρεται η περίπτωση των ΗΠΑ όπου εφαρμόζονται τομεακές ρυθμίσεις (COPPA για τα παιδιά), ενώ σε χώρες της Ασίας έχουν υιοθετηθεί νόμοι συμβατοί με τον GDPR με σκοπό τη διευκόλυνση διασυνοριακών ροών δεδομένων [39], σύμφωνα με την απαίτηση του τελευταίου για τη συλλογή και επεξεργασία των δεδομένων των πολιτών της ΕΕ.

3.2.3 Σχέση Εθνικών και Διεθνών Ρυθμίσεων με τα RTLD

Οι ρυθμίσεις που υφίστανται σε εθνικό και διεθνές επίπεδο είναι άμεσα συνδεδεμένες με τη δημοσιοποίηση και σύνδεση των προσωπικών δεδομένων μέσω της τεχνολογίας των Ready to Link Data (RTLD) [40]. Το αν τα δεδομένα θα δημοσιευτούν εξαρτάται από το αν αυτά θα αναγνωρίζονται ως προσωπικά ή ανωνυμοποιημένα. Επιπροσθέτως, η ανάγκη ύπαρξης νομικής βάσης και η εκ των προτέρων αξιολόγηση του πιθανού ρίσκου για τα δεδομένα καθορίζονται από το ισχύον νομικό πλαίσιο [33]. Τέλος, προκειμένου να υπάρξουν διασυνοριακές συνεργασίες με μη ευρωπαϊκές χώρες απαιτείται η ύπαρξη επαρκών εγγυήσεων ως προς τη μεταφορά και χρήση των δεδομένων [45].

Σύγκριση Εθνικού και Διεθνούς Νομικού Πλαισίου Προστασίας Δεδομένων (Πίνακας 3)

Κατηγορία	Εθνικό Πλαίσιο	Διεθνές-Υπερεθνικό Πλαίσιο
Βασική Νομοθεσία	Ν.4624/2019 (συνδυαστικά με GDPR)	Γενικός Κανονισμός GDPR, σύμβαση 108+, Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ, Οδηγίες ΟΟΣΑ
Εποπτική Αρχή	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)	Εθνικές Αρχές εκάστοτε Κράτους-Μέλους ΕΕ, Εποπτικοί μηχανισμοί ΣτΕ
Αρχές Επεξεργασίας	Ταυτίζονται με του GDPR, Νομιμότητα-Διαφάνεια-Ελαχιστοποίηση-Ασφάλεια	Καθολικά αποδεκτές αρχές μέσω GDPR, Σύμβαση 108+, ΟΟΣΑ-ασφάλεια, ποιότητα, περιορισμός σκοπού

Ρύθμιση RTLD και δημόσιων δεδομένων	Δεν υπάρχει ειδική πρόβλεψη, εφαρμόζονται οι αρχές GDPR	GDPR άρθρα 6, 25. Διεθνείς οδηγίες με όρους για επεξεργασία ανοιχτών δεδομένων
Δικαιώματα Υποκειμένου	Πλήρης αναγνώριση και πρόσβαση, διόρθωση, διαγραφή, περιορισμός και εναντίωση στη διάθεση και την επεξεργασία	Ισχύουν βάση GDPR, Χάρτη Δικαιωμάτων ΕΕ, Σύμβασης 108+
Ειδικές εξαιρέσεις	Εθνική ασφάλεια, ποινικές έρευνες, δημόσια διοίκηση	Αναγνωρίζονται από διεθνείς συνθήκες υπό αυστηρούς όμως όρους και περιορισμούς
Διασυνοριακή μεταφορά	Επιτρέπεται με τις κατάλληλες εγγυήσεις όπως ορίζονται από τον GDPR	GDPR, Σύμβαση 108+
Εφαρμογή στα πλαίσια RTLD	Απαιτείται ανωνυμοποίηση, τεκμηρίωση νομικής βάσης	Απαραίτητη η συμβατότητα με GDPR, υποχρεωτική η τεχνική και νομική αξιολόγηση των κινδύνων που εμφανίζονται από την επανασύνδεση των Ανοιχτών Δεδομένων

3.3 Συμβατότητα των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης με το Νομικό Πλαίσιο

Όπως έχουμε πλέον εμπεδώσει, η χρήση των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης και η αξιοποίησή τους μπορεί να επιφέρει σημαντικά οφέλη όσον αφορά τη διαφάνεια, την καινοτομία και την επιστημονική έρευνα, ενώ ταυτόχρονα εγείρονται σοβαρά νομικά ζητήματα, στην περίπτωση που αυτά τα δεδομένα αφορούν τα προσωπικά δεδομένα των υποκειμένων που αυτά ανήκουν [10]. Αυτό οδηγεί στην ανάγκη συμμόρφωσης με τις αρχές προστασίας της ιδιωτικότητας, της ασφάλειας και της λογοδοσίας όταν πρέπει να μιλήσουμε για συμβατότητα μεταξύ RTLD και GDPR καθώς και άλλα σχετικά νομικά πλαίσια [22].

3.3.1 Νομικές Προκλήσεις

Αρχικά έχουμε την πιθανότητα επαναταυτοποίησης του ατόμου μέσω δεδομένων. Ενώ αυτά που βρίσκονται σε μία συγκεκριμένη Data Base μπορεί να έχουν ανωνυμοποιηθεί, υπάρχει πάντα ο κίνδυνος να διασυνδεθούν με δεδομένα από διαφορετικές βάσεις και άρα να προκύψει επαναταυτοποίηση φυσικών προσώπων μέσω της διασύνδεσης των ανοιχτών δεδομένων [8]. Για παράδειγμα, στατιστικά στοιχεία που αφορούν ασθενείς μπορεί να εμφανίζονται ανώνυμα, αλλά

αν συνδυαστούν με γεωγραφικά δεδομένα καθώς και τυχόν χρονικά δεδομένα θα μπορούσαν να οδηγήσουν στην ταυτοποίηση υποκειμένων.

Μία ακόμα πρόκληση που αντιμετωπίζεται στο νομικό πεδίο, είναι αυτή της έλλειψης καθορισμένου σκοπού όσον αφορά τη συλλογή και επεξεργασία προσωπικών δεδομένων. Σύμφωνα με τον Κανονισμό της ΕΕ, η επεξεργασία των προσωπικών δεδομένων θα πρέπει να γίνεται για σκοπό συγκεκριμένο, νόμιμο και σαφώς καθορισμένο. Παράλληλα όμως η ίδια η φύση των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης, τα οποία δημοσιεύονται εξ ορισμού για την ελεύθερη διάθεση και χρήση δεδομένων από το ευρύ κοινό, έρχεται σε αντίθεση με την αρχή του περιορισμού του σκοπού [9].

Έχουμε ακόμα αναφέρει πως το υποκείμενο στο οποίο ανήκουν τα εκάστοτε δεδομένα έχει το δικαίωμα ελέγχου πάνω στον τρόπο με τον οποίο αυτά δημοσιεύονται και επεξεργάζονται, όπως και στη διαγραφή τους. Και πάλι όμως η φύση των ανοιχτών δεδομένων καθιστά δύσκολη οποιαδήποτε άσκηση αυτών των δικαιωμάτων από το υποκείμενο [16], καθώς δυσχεραίνεται η αναγνώριση του υπεύθυνου επεξεργασίας.

Τέλος, σε περίπτωση που τα δεδομένα θα μεταφερθούν εκτός της ΕΕ, δεν υπάρχουν επαρκείς εγγυήσεις ως προς την επεξεργασία τους, καθώς δεν ισχύει ο GDPR [18].

3.3.2 Όροι Συμβατότητας με τον Κανονισμό της ΕΕ GDPR

Ως προς τη νομιμότητα της δημοσίευσης και διασύνδεσης των Δεδομένων, θα πρέπει να πληρούνται συγκεκριμένες προϋποθέσεις. Αρχικά, θα πρέπει να υφίσταται νομιμότητα ως προς την επεξεργασία, δηλαδή έγκυρη νομική βάση, όπως η συγκατάθεση του υποκειμένου [29], προκειμένου να διατίθενται τα δεδομένα του προς επεξεργασία. Τα δεδομένα αυτά θα πρέπει να υπόκεινται σε ανωνυμοποίηση και ψευδονυμοποίηση ώστε να μην μπορούν να οδηγήσουν στην ταυτοποίηση φυσικών προσώπων. Ως προς τα λειτουργικά συστήματα που θα χρησιμοποιούνται για τη διάθεση και επεξεργασία των προσωπικών δεδομένων, αυτά θα πρέπει να έχουν ενσωματώσει συστήματα προστασίας κατά το σχεδιασμό τους (Privacy by Design, Privacy by Default) [11]. Για να είναι η όποια επεξεργασία σύμφωνη με τον Κανονισμό, θα πρέπει υποχρεωτικά να υφίσταται εκτίμηση του πιθανού αντίκτυπου στο υποκείμενο όταν θεωρείται πως υπάρχει υψηλός κίνδυνος για τα δικαιώματα αυτού λόγω της επεξεργασίας [30]. Τέλος, θα πρέπει να υφίσταται έλεγχος στην πρόσβαση στα δεδομένα ανάλογα με τον καθορισμένο σκοπό.

3.3.3 Καλές Πρακτικές Δημοσίευσης Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης με Προστασία Δεδομένων

Ως προς τη γεφύρωση της δημοσίευσης των δεδομένων με την προστασία τους, ενδείκνυνται ορισμένες πρακτικές που μπορούν να συμβάλλουν στη μείωση του κινδύνου διαρροής προσωπικών δεδομένων και επαναταυτοποίησης του υποκειμένου. Αρχικά μπορούμε να κάνουμε χρήση πρακτικών ανωνυμοποίησης των δεδομένων [28], πρακτική που έχουμε ήδη αναφέρει ως ούσα χρήσιμη για την ασφαλέστερη δημοσιοποίηση αυτών. Επιπλέον, τα μεταδεδομένα τεκμηριώνονται με τρόπους που μπορούν να εξηγήσουν τα όρια και τους κινδύνους της χρήσης. Μία άλλη πρακτική απαιτεί να καθορίζονται οι όροι χρήσης των δεδομένων, και άρα να περιορίζεται η επαναχρησιμοποίηση των δεδομένων για σκοπούς άλλους από τον αρχικό για τον οποίο και έχει δοθεί η συγκατάθεση του υποκειμένου, και μάλιστα μη συμβατούς με τους όρους

προστασίας των προσωπικών δεδομένων. Τέλος, μπορούν να εφαρμόζονται συστήματα παρακολούθησης της επαναχρησιμοποίησης των δεδομένων, όπως επί παραδείγματι η χρήση API με περιορισμούς [17].

3.3.4 Νομολογιακές και Ακαδημαϊκές Αντιπαραθέσεις

Με μία πρώτη ανασκόπηση σχετικής βιβλιογραφίας που αφορά τα ανοιχτά δεδομένα και την ιδιωτικότητα, βλέπουμε πως υπάρχει η κοινώς αποδεκτή αντίληψη ότι το δικαίωμα του υποκειμένου στην ιδιωτικότητα δεν θα πρέπει να υποβιβάζεται ή και να αναιρείται για χάρη της διαφάνειας [26]. Η χρήση των Ανοιχτών Δεδομένων όπως έχει ειπωθεί και παραπάνω μπορεί να έχει πολυάριθμα οφέλη για Θεσμούς αλλά και πολίτες, ενισχύοντας τη διαφάνεια και την εμπιστοσύνη. Η κατάχρηση όμως των Ανοιχτών Δεδομένων και οι ανάλυσή τους από τρίτα μέρη όπως για παράδειγμα διαφημιστικές εταιρίες ή και πολιτικά κόμματα μπορεί να ενέχει σημαντικούς κινδύνους όπως η δημιουργία προφίλ των ατόμων και πιθανή διάκριση μεταξύ των πολιτών [20]. Άρα, υπάρχει η απαίτηση για ένα ισορροπημένο ρυθμιστικό πλαίσιο που θα είναι σε θέση αφενός να προστατεύσει την ιδιωτικότητα των υποκειμένων ενώ ταυτόχρονα να επιτρέπει την προώθηση της καινοτομίας μέσω της χρήσης και επεξεργασίας των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης.

3.4 Δικαιώματα των Υποκειμένων που Αφορούν τα Δεδομένα

Προκειμένου κάποιος, είτε πρόκειται για μεμονωμένο άτομο είτε για δημόσιο ή ιδιωτικό φορέα, να προβεί σε χρήση και επεξεργασία Ανοιχτών Δεδομένων τα οποία περιλαμβάνουν ή και σχετίζονται με προσωπικά δεδομένα, θα πρέπει να συμμορφώνεται πλήρως με τα δικαιώματα των υποκειμένων των εν λόγω δεδομένων, όπως αυτά ορίζονται στον Γενικό Κανονισμό για την Προστασία Δεδομένων της ΕΕ, γνωστό και ως GDPR [4]. Το ζητούμενο είναι να βρεθεί η χρυσή τομή ανάμεσα στην ελεύθερη διάθεση των δεδομένων και την προστασία της ιδιωτικότητας των ατόμων [27]. Τα δικαιώματα των υποκειμένων λοιπόν δεν μπορεί παρά να αποτελούν σημαντικό πυλώνα της όλης συζήτησης [20].

3.4.1 Βασικά Δικαιώματα των Υποκειμένων σύμφωνα με τον GDPR

Σύμφωνα με τον Κανονισμό της ΕΕ, το Υποκείμενο των Δεδομένων έχει ορισμένα από αυτόν δικαιώματα.

Δικαίωμα ενημέρωσης. Θα πρέπει να ενημερώνεται σχετικά με τη συλλογή και χρήση ή/και επεξεργασία των δεδομένων του. Στην περίπτωση των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης όμως δεν είναι πάντοτε σαφής ο υπεύθυνος επεξεργασίας τους, και άρα υπάρχει αυξημένη απαίτηση για τεκμηρίωση σκοπού και διαφάνεια [10].

Δικαίωμα πρόσβασης. Κάθε υποκείμενο μπορεί να λάβει αντίγραφο των δεδομένων που το αφορούν καθώς και πληροφορίες σχετικά με τη χρήση τους. Πρακτικά όμως κάτι τέτοιο είναι δύσκολο καθώς όταν τα δεδομένα έχουν δημοσιευτεί υπό τη μορφή των RTLD [16].

Δικαίωμα διόρθωσης. Το υποκείμενο των δεδομένων δικαιούται να ζητήσει τη διόρθωση στοιχείων τα οποία κρίνει ως ανακριβή προσωπικά δεδομένα. Το συγκεκριμένο εγχείρημα μπορεί

να καταστεί τεχνικώς ιδιαίτερα περίπλοκο όταν μιλάμε για Ready to Link Data, καθώς τα υπό αίτηση διόρθωσης δεδομένα μπορεί να βρίσκονται σε πολλές βάσεις δεδομένων ταυτόχρονα [18].

Δικαίωμα διαγραφής, ή αλλιώς Δικαίωμα στη Λήθη. Το υποκείμενο έχει το δικαίωμα να ζητήσει ακόμα και τη διαγραφή των δεδομένων που το αφορούν. Αυτό πρακτικά είναι ανεφάρμοστο αν έχουν δημοσιευτεί τα δεδομένα αυτά υπό την μορφή των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης, και κατά συνέπεια έχουν ήδη διαμοιραστεί [8].

Δικαίωμα περιορισμού της επεξεργασίας. Κάθε άτομο έχει το δικαίωμα, υπό προϋποθέσεις, να ζητήσει να πάψει η χρήση των δεδομένων του, αν και πάλι πρακτικά και τεχνικά δύσκολα εφαρμόζεται ειδικά σε περιπτώσεις ανοιχτών βάσεων δεδομένων [9].

Δικαίωμα εναντίωσης. Κάθε υποκείμενο διατηρεί το δικαίωμα να αντιτίθεται στη χρήση των δεδομένων του για συγκεκριμένους σκοπούς. Η διαχείριση όμως τέτοιων αντιρρήσεων στα πλαίσια των ανοιχτών βάσεων δεδομένων δεν είναι εύκολη υπόθεση [29].

Δικαίωμα φορητότητας. Κάθε άτομο είναι σε θέση να λάβει τα δεδομένα του από έναν υπεύθυνο επεξεργασίας και να τα μεταφέρει σε άλλον. Η σημασία του δικαιώματος αυτού στην περίπτωση Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης είναι όμως περιορισμένη, καθώς τα δεδομένα είναι ήδη προσβάσιμα αν και χωρίς εγγυημένη μορφοποίηση [30].

3.4.2 Προκλήσεις Εφαρμογής Δικαιωμάτων των Υποκειμένων στα πλαίσια Περιβάλλοντος RTLD

Το περιβάλλον των RTLD δυστυχώς από τη φύση του δυσχεραίνει την προστασία των προσωπικών δεδομένων. Υφιστάμενες προκλήσεις εντοπίζονται σε αρκετά σημεία, και συγκεκριμένα επειδή τα δεδομένα δημοσιεύονται και είναι ανοιχτά, δεν υπάρχει καθορισμένος υπεύθυνος επεξεργασίας, καθιστώντας στην ουσία πρακτικά αδύνατη την άσκηση των δικαιωμάτων του υποκειμένου [6]. Τεχνικά αδύνατη είναι και η διαγραφή ή διόρθωση ανοιχτών δεδομένων, καθώς αυτά από τη φύση τους υπόκεινται σε αντιγραφές και επαναχρησιμοποιήσεις. Οποιαδήποτε διόρθωση θα γίνεται σε περιορισμένο αριθμό βάσεων, και ποτέ σε όλες. Επιπλέον, η χρήση, επαναχρησιμοποίηση και επεξεργασία των Ανοιχτών Δεδομένων μπορεί να γίνει από το οποιοδήποτε τρίτο μέρος, χωρίς καν να ειδοποιηθεί το αρχικό υποκείμενο. Τέλος, ο σημαντικότερος κίνδυνος από τη διασύνδεση των βάσεων δεδομένων είναι η πιθανότητα να επαναταυτοποιηθεί το υποκείμενο χωρίς να γνωρίζει σχετικά, αφού διαφορετικά σύνολα Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης μπορεί να οδηγήσουν στη δημιουργία ενός προφίλ του υποκειμένου [7].

3.4.3 Πιθανά Βήματα για την Ενίσχυση της Προστασίας Δικαιωμάτων

Για να επιτευχθεί η πολυπόθητη προστασία των προσωπικών δεδομένων των υποκειμένων, ειδικά σε περιβάλλοντα Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης, υφίστανται επί του παρόντος ορισμένες προτάσεις. Αρχικά, κάθε σύνολο RTLD θα πρέπει να έχει και καθορισμένο υπεύθυνο επεξεργασίας [28], και άρα νομικά υπεύθυνο για την προστασία των δεδομένων της βάσης. Αυτό μπορεί να επιτευχθεί μέσω μεταδεδομένων ή URI identification, για παράδειγμα. Μία ακόμα πρόταση είναι η ενσωμάτωση μηχανισμών μέσω των οποίων θα γίνεται η άσκηση των δικαιωμάτων των υποκειμένων, με τη χρήση φόρμας online [13], όπου τα άτομα θα μπορούν να

αιτηθούν τη διαγραφή ή τροποποίηση των δεδομένων τους, ή να αρνηθούν ή να δεχτούν την επεξεργασία αυτών.

Όσον αφορά την τεχνική της ανωνυμοποίησης, ενώ είναι κοινώς αποδεκτή η χρησιμότητά της, θα ήταν σκόπιμος ο έλεγχος της αποτελεσματικότητάς της κατά περίπτωση με ειδικά ελεγκτικά τεστ [15] που θα μπορούν να αναλύσουν τον κίνδυνο ταυτοποίησης των υποκειμένων των δεδομένων που διαθέτει μία βάση ανοιχτών δεδομένων.

Ακόμα, θα μπορούσαν να δημιουργηθούν πλατφόρμες που θα επιτρέπουν την τροποποίηση ή αφαίρεση προσωπικών δεδομένων σε ειδικές περιπτώσεις, όπως για παράδειγμα όταν ένα άτομο διαπιστώνει ότι τα προσωπικά του δεδομένα έχουν δημοσιευτεί σε μία ανοιχτή βάση δεδομένων, και επιθυμεί την τροποποίηση ή διαγραφή τους. Μετά από νόμιμο αίτημα και αφού διαπιστωθεί η ταυτότητα του αιτούντος, η οποιαδήποτε αλλαγή ή διαγραφή γίνεται μετά από επεξεργασία του αιτήματος από τον υπεύθυνο διαχειριστή. Με αυτό τον τρόπο και πάντα σε συμφωνία με τον Κανονισμό της ΕΕ GDPR, ενισχύεται από τη μία πλευρά η εμπιστοσύνη των ατόμων, καταγράφονται οι αλλαγές και ταυτόχρονα ενισχύεται και η λογοδοσία, ενώ η ελεγχόμενη επεξεργασία των δεδομένων προστατεύει τα υποκείμενα χωρίς όμως να καταργεί την ανοιχτή φύση των δεδομένων.

Όλα τα παραπάνω θα ήταν σκόπιμο να συνοδεύονται και από διαρκείς αναθεωρήσεις του νομικού πλαισίου που υφίσταται σε επίπεδο ΕΕ [22], με σκοπό την καλύτερη προσαρμογή στις ανάγκες της εποχής των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης.

4 *Ηθικές, Κοινωνικές και Τεχνικές Προκλήσεις στην Επαναχρησιμοποίηση Δεδομένων*

Έχοντας πλέον περάσει σε μία εποχή που τα δεδομένα αποτελούν έναν ιδιαίτερα σημαντικό πόρο για την ανάπτυξη, τη διακυβέρνηση αλλά και την επιστημονική πρόοδο, παρατηρείται μία έντονη πίεση για τη διάθεση των πληροφοριών χωρίς περιορισμούς, δηλαδή ανοιχτά. Αυτό συμβαίνει κατά κύριο λόγο στο πεδίο των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης (Ready to Link Data, RTLD). Αν και όντως η δημοσιοποίηση των δεδομένων προάγει τη διαφάνεια, την αξιοπιστία των δημόσιων πολιτικών καθώς και την καινοτομία, την ίδια στιγμή τίθενται σημαντικά ερωτήματα που αφορούν τα όρια της ιδιωτικότητας των ατόμων, την χωρίς συναίνεση χρήση των δεδομένων και άλλους τεχνολογικούς κινδύνους που εμφανίζονται από τη χρήση και επεξεργασία τους.

Στο παρόν κεφάλαιο αναλύονται ηθικές, κοινωνικές και τεχνικές διαστάσεις του ζητήματος οι οποίες προκύπτουν από την επεξεργασία και επαναχρησιμοποίηση των προσωπικών δεδομένων των υποκειμένων στο πεδίο εφαρμογής των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης. Συγκεκριμένα, αναλύονται τεχνικές προστασίας της ιδιωτικότητας των ατόμων, όπως οι βασικές τεχνικές της ανωνυμοποίησης και ψευδονυμοποίησης, οι κίνδυνοι επαναπροσδιορισμού της ταυτότητας των ατόμων μέσω συνδυασμού δεδομένων από διαφορετικές πηγές, προκλήσεις που προκύπτουν στη διαλειτουργικότητα και ασφάλεια των ανοιχτών βάσεων δεδομένων και αναφέρονται ορισμένα παραδείγματα όπου η επαναχρησιμοποίηση και επεξεργασία των δεδομένων οδήγησε σε παραβιάσεις της ιδιωτικότητας.

Επιδιώκεται η ανάδειξη για την αναγκαιότητα μίας πολυεπίπεδης προσέγγισης για την προστασία των προσωπικών δεδομένων όπου θα πρέπει να συνδυαστούν τεχνικές λύσεις,

συμμόρφωση με το νομικό πλαίσιο αλλά και ηθική ευθύνη των μερών που εμπλέκονται. Σημειώνεται επίσης η σημασία τεχνολογιών προληπτικής στρατηγικής όπως της "Privacy by Design", που φαίνεται να είναι στρατηγικής σημασίας για το σχεδιασμό δημόσιων πολιτικών και τεχνολογικών συστημάτων.

4.1 Ανωνυμοποίηση και Ψευδονυμοποίηση Δεδομένων

Η προστασία της ιδιωτικότητας, ειδικά στην περίπτωση των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης, αποτελεί πολύ σημαντικό θέμα όταν μιλάμε για ανοιχτά προσωπικά δεδομένα, ή άλλα δεδομένα που μπορούν να συσχετιστούν με αυτά. Η χρήση των τεχνικών της ανωνυμοποίησης και ψευδονυμοποίησης αποτελεί βασικό εργαλείο ώστε να γίνει διαχείριση της εν λόγω πρόκλησης, και έτσι να μετριαστεί ο κίνδυνος ταυτοποίησης των υποκειμένων στα οποία ανήκουν τα δεδομένα που αναρτώνται [7].

4.1.1 Θεωρητικό και Νομικό Πλαίσιο

Αρχικά βλέπουμε πως ορίζονται οι έννοιες της ανωνυμοποίησης και ψευδονυμοποίησης.

Ως ανωνυμοποίηση ορίζεται η επεξεργασία των δεδομένων με τέτοιο τρόπο ώστε να μην είναι πλέον δυνατή η ταυτοποίηση ενός φυσικού προσώπου. Όταν αυτή είναι επιτυχής, τα δεδομένα δεν υπόκεινται πλέον στο Γενικό Κανονισμό Προστασίας Δεδομένων της ΕΕ (GDPR) [21].

Ως ψευδονυμοποίηση ορίζεται η μετατροπή των προσωπικών δεδομένων σε μη αναγνωρίσιμα και χωρίς πρόσθετες πληροφορίες, όπως για παράδειγμα με τη χρήση κωδικών, όμως παραμένουν προσωπικά δεδομένα και άρα συνεχίζουν να διέπονται από τον Κανονισμό (GDPR).

Σε κάθε περίπτωση, η επιλογή της τεχνικής που θα χρησιμοποιηθεί για την προστασία των δεδομένων εξαρτάται από παράγοντες όπως ο σκοπός επεξεργασίας των δεδομένων, η ίδια η φύση των δεδομένων, ο κίνδυνος επαναταυτοποίησης του υποκειμένου καθώς και η περίπτωση που απαιτείται επανασύνδεση με ταυτοποίηση, όπως στην περίπτωση ιατρικών μητρώων [19].

4.1.2 Περιορισμοί και Κίνδυνοι

Αν και οι συγκεκριμένες τεχνικές είναι όντως πολύ χρήσιμες για την προστασία των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης, δεν παύουν να έχουν ορισμένους περιορισμούς και να υπόκεινται σε κινδύνους [7].

Συγκεκριμένα, υφίσταται ο κίνδυνος του επαναπροσδιορισμού-επαναταυτοποίησης του ατόμου. Αν και τα δεδομένα είναι ανώνυμα, η διασύνδεση δεδομένων από διαφορετικές πηγές RTLD ,ε εξωτερικές βάσεις δεδομένων μπορεί να επιτρέψει την αναγνώριση προσώπων [13]. Τέτοια ήταν η περίπτωση ταυτοποίησης χρηστών στην υπόθεση Netflix του 2006, όπου ερευνητές κατάφεραν να συνδέσουν ανώνυμα δεδομένα, που όπως είδαμε δεν προστατεύονται πλέον από νομικό πλαίσιο καθώς δεν είναι προσωπικά μετά τη διαδικασία της ανωνυμοποίησης, με IMDb και συνεπώς να ταυτοποιήσουν χρήστες [4].

Το εργαλείο της ανωνυμοποίησης από μόνο του αποτελεί έννοια σχετική και όχι απόλυτη. Η επιτυχία ή αποτυχία της τεχνικής εξαρτάται από παράγοντες όπως το τεχνολογικό επίπεδο που

χρησιμοποιείται, τις γνώσεις που είναι διαθέσιμες εξωτερικά του συστήματος και τα υπόλοιπα χαρακτηριστικά της βάσης δεδομένων [19].

Αξίζει ακόμα να αναφερθούμε στο γεγονός ότι ενώ το ζητούμενο είναι ένα υψηλό επίπεδο προστασίας, αυτό κατά κανόνα συνεπάγεται την απώλεια της ακρίβειας των δεδομένων ή και της χρησιμότητάς τους [7]. Για την καλύτερη κατανόηση της αντίφασης, αναφέρουμε σχετικό παράδειγμα σύγκρουσης χρηστικότητας δεδομένων και ιδιωτικότητας.

Έστω ότι την περίοδο του Covid-19 ένας δημόσιος οργανισμός δημοσιεύει υπό τη μορφή των Open Linked Data δεδομένα σχετικά με τα κρούσματα της ασθένειας. Στόχος της δημοσίευσης είναι η έρευνα και η πρόληψη. Αρχικά το σύνολο των δεδομένων αφορά περιοχή, ηλικία ασθενούς, ημερομηνία διάγνωσης, φύλο και τύπο συμπτωμάτων. Η χρηστικότητα του συνόλου είναι εδώ υψηλή, αφού μπορεί να γίνει έρευνα σχετική με τις εστίες μετάδοσης, τη σχέση των ηλικιακών ομάδων με την εξάπλωση του ιού, τη συχνότητα των κρουσμάτων ανά περιοχή και πολλά άλλα. Μετά από τη διαδικασία της ανωνυμοποίησης, η περιοχή θα αντικατασταθεί από το νομό, η ηλικία των ατόμων ομαδοποιείται, τυχόν σπάνια συμπτώματα θα αφαιρεθούν εντελών από το σύνολο των δεδομένων ώστε να αποφευχθεί η ταυτοποίηση των υποκειμένων, η ημερομηνία διάγνωσης θα ομαδοποιηθεί επίσης ανά εβδομάδα. Πλέον οι ερευνητές δεν είναι σε θέση να εξάγουν συμπεράσματα όσον αφορά τάσεις εξάπλωσης του ιού ανά περιοχή, δεν μπορεί να γίνει συσχετισμός ηλικίας και σοβαρότητας των συμπτωμάτων, και γενικά εξειδικευμένες έρευνες, όπως για παράδειγμα περιπτώσεις που αφορούν ευάλωτες ομάδες του πληθυσμού καθίστανται ανέφικτες.

Βλέπουμε λοιπόν το μείζον δίλημμα μεταξύ προστασίας της ιδιωτικότητας και χρηστικότητας των δεδομένων. Αυξημένη προστασία των προσωπικών δεδομένων σημαίνει χαμηλή ακρίβεια στην παραγόμενη πληροφορία και χαμηλότερη ερευνητική αξία, ενώ από την άλλη χρήσιμα δεδομένα για την παραγωγή πληροφορίας ενέχουν μεγάλο κίνδυνο για την προστασία της ιδιωτικής ζωής των ατόμων [19].

Ουσιαστικά, το ζητούμενο είναι η εξισορρόπηση μεταξύ του κινδύνου αποκάλυψης προσωπικών δεδομένων και της ανάγκης για ανοιχτά και χρήσιμα δεδομένα [4].

Αξίζει τέλος να σημειωθεί ότι η εφαρμογή των υφιστάμενων τεχνικών πληροφοριακών συστημάτων για την προστασία των δεδομένων μέσω των εργαλείων της ανωνυμοποίησης και ψευδονυμοποίησης στα πλαίσια των βάσεων Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης απαιτεί προσεκτικό σχεδιασμό [7], καθώς πρέπει να γίνεται σεβαστή η δομή και το περιεχόμενο των πεδίων που θα ανωνυμοποιηθούν, το επίπεδο προστασίας θα πρέπει να τεκμηριώνεται και σαφώς θα πρέπει να υπάρχουν πολιτικές ελέγχου της πρόσβασης στα δεδομένα [21].

Συμπερασματικά, οι δύο αυτές τεχνικές μπορούν να αποδειχτούν πολύ χρήσιμες αλλά σε καμία περίπτωση δεν εγγυώνται την απόλυτη προστασία [7]. Θα πρέπει να συμβάλει και ο ανθρώπινος παράγοντας, με τον υπεύθυνο επεξεργασίας της κάθε βάσης δεδομένων να είναι σε θέση να αξιολογεί διαρκώς την αποτελεσματικότητά τους, να επιλέγει τις κατάλληλες μεθόδους ανάλογα με τον τύπο των δεδομένων, το σκοπό που αυτά χρησιμοποιούνται και τον κίνδυνο που μπορεί να εμφανιστεί, και πάντα σε συμφωνία με τον GDPR να ενσωματώνει αυτές τις τεχνικές στο ευρύτερο πλαίσιο της Privacy by Design και των εκτιμήσεων αντικτύπου σε περίπτωση επαναταυτοποίησης ατόμων [17].

Πίνακας Απόφασης: Ανωνυμοποίηση vs Ψευδονυμοποίηση (Πίνακας 4)

Κριτήριο	**Ανωνυμοποίηση**	**Ψευδονυμοποίηση**
Σκοπός Επεξεργασίας	Μη αναστρέψιμη δημοσίευση για ανοιχτή χρήση (RTLD)	Εσωτερική χρήση με δυνατότητα ταυτοποίησης (ιατρικά αρχεία, έρευνες πελατών)
Ανάγκη επανασύνδεσης με το Υποκείμενο	Όχι	Ναι
Ενσωμάτωση σε Ready to Link Data	Ναι, όταν απαιτείται αποδέσμευση από την ταυτότητα	Περιορισμένα και με αυστηρό έλεγχο πρόσβασης
Εφαρμογή GDPR	Δεν εφαρμόζεται εφόσον τα δεδομένα είναι ανώνυμα	Ισχύει πλήρως καθώς τα δεδομένα παραμένουν προσωπικά
Κίνδυνος Επαναταυτοποίησης	Εξαρτάται από την ποιότητα της ανωνυμοποίησης και τη διασύνδεση με άλλα δεδομένα	Υψηλός αν διαρρεύσει ο πίνακας αντιστοίχισης
Χρήση σε Συστήματα Υγείας, Δημόσιες Βάσεις Δεδομένων	Για δημοσίευση στατιστικών ή ανοιχτών δεδομένων	Για διαχείριση φακέλων με πρόσβαση μόνο σε εξουσιοδοτημένα άτομα
Επίπεδο Χρηστικότητας Δεδομένων	Μειωμένο λόγω γενίκευσης ή παραμόρφωσης	Υψηλό καθώς διατηρείται η πληρότητα των δεδομένων
Δυνατότητα Συμμόρφωσης με Αρχή Ελαχιστοποίησης	Ναι- Κατάλληλο για σύνολα δεδομένων όπου δεν απαιτείται ταυτοποίηση	Περιορισμένο- Απαιτεί μέτρα προστασίας για αποφυγή κατάχρησης
Καταλληλότητα για Έρευνα με Υψηλή Ευαισθησία	Κατάλληλη όταν επιθυμείται η πλήρης προστασία της ταυτότητας	Κατάλληλη για έρευνες όπου απαιτείται μελλοντική επικοινωνία με το υποκείμενο
Τεχνικά Μέσα	Generalization, Suppression, Noise Addition	Tokenization, Hashing, Key Coding

Σε γενικές γραμμές, επιλέγεται η χρήση της ανωνυμοποίησης σε περιπτώσεις που τα σύνολα δεδομένων πρόκειται να δημοσιευτούν ως Ανοιχτά Δεδομένα χωρίς έλεγχο πρόσβασης σε αυτά, ενώ ταυτόχρονα δεν θα χρειαστεί επανασύνδεση με το υποκείμενο των δεδομένων στο μέλλον. Σε κάθε περίπτωση, το νομικό αλλά και το ηθικό πλαίσιο που διέπει την προστασία της ιδιωτικότητας απαιτεί την μη αναστρέψιμη προστασία της ταυτότητας των υποκειμένων.

Ψευδονυμοποίηση από την άλλη χρησιμοποιείται σε περιπτώσεις όπου τα δεδομένα θα πρέπει να μπορούν να ανακτηθούν ή και να ενημερωθούν από το ίδιο το υποκείμενο, ενώ η πρόσβαση σε αυτά είναι περιορισμένη και υπό προϋποθέσεις. Για παράδειγμα, μπορούν να χρησιμοποιηθούν για προσωποποιημένες υπηρεσίες, όπως σε περιπτώσεις επανεξέτασης ασθενών.

4.2 Κίνδυνοι Επαναπροσδιορισμού της Ταυτότητας (Re-identification)

Η επαναταυτοποίηση, ή αλλιώς επαναπροσδιορισμός ταυτότητας, ορίζεται ως η διαδικασία με την οποία ένα άτομο μπορεί να αναγνωριστεί με τη χρήση ενός συνόλου ανωνυμοποιημένων ή ψευδονυμοποιημένων δεδομένων, κατά βάση μέσω της διασταύρωσής τους με άλλα σύνολα δεδομένων. Όταν μιλάμε για Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης (Open Kinked Data, RTLD), όπου τα δεδομένα είναι ανοιχτά και προσβάσιμα σε τρίτους και, όπως αναφέρεται και στην ονομασία τους, συνδεδεμένα, ο κίνδυνος επαναπροσδιορισμού της ταυτότητας του υποκειμένου είναι μεγαλύτερος λόγω της αυξημένης συσχέτισης διαφορετικών πηγών [14].

4.2.1 Θεωρητικό Υπόβαθρο

Όταν μιλάμε για επαναταυτοποίηση υποκειμένου, ταυτόχρονα πρέπει να δούμε και τις έννοιες της πληροφοριακής ταυτότητας (Information Identity), και της έμμεσης ταυτοποίησης. Η πρώτη αναφέρεται στο σύνολο των πληροφοριών που μπορούν να προσδιορίσουν ένα άτομο άμεσα ή έμμεσα, μέσω της σχέσης τους με τα χαρακτηριστικά, τις συνήθειες ή και τις δραστηριότητές του [32]. Ειδικότερα, πρόκειται για το προφίλ ενός ατόμου όπως διαμορφώνεται από δεδομένα που το περιγράφουν όπως άμεσα αναγνωριστικά στοιχεία, για παράδειγμα όνομα και αριθμός ταυτότητας, έμμεσα αναγνωριστικά στοιχεία όπως το φύλο, η ηλικία και το επάγγελμα μεταξύ άλλων, δεδομένα που αφορούν τη συμπεριφορά του ατόμου, όπως αγοραστικές συνήθειες, επίσκεψη ιστοσελίδων, και διασυνδέσεις με φίλους, δίκτυα ή άλλες σχέσεις. Ακόμα κι όταν αφαιρούνται τα άμεσα αναγνωριστικά στοιχεία, όπως το όνομα και η διεύθυνση κατοικίας, τα έμμεσα αναγνωριστικά όπως η ηλικία και το φύλο μπορούν να χρησιμοποιηθούν για να γίνει ο εντοπισμός ενός ατόμου όταν αυτά συνδυάζονται με εξωτερικά δεδομένα. Αξίζει εδώ να σημειωθεί ότι σύμφωνα με τον GDPR προσωπικά θεωρούνται τα δεδομένα όταν υπάρχει εύλογος τρόπος ταυτοποίησης όταν αυτά συνδυαστούν με πρόσθετες πληροφορίες. Οποιαδήποτε λοιπόν πληροφορία μπορεί να συμβάλλει στην αναγνώριση ενός υποκειμένου θεωρείται προσωπικό δεδομένο. Όταν αυτά τα δεδομένα συνδέονται, μπορεί να επαναταυτοποιηθεί η πληροφοριακή ταυτότητά του και να οδηγήσει σε επικίνδυνες καταστάσεις, όπως ο σχηματισμός προφίλ, παράβαση της ιδιωτικότητας ή και διακρίσεις σε βάρος ορισμένου ατόμου [23].

Ως ταυτότητα λοιπόν δεν νοείται μόνο το όνομα ενός ατόμου, αλλά και όλα τα χαρακτηριστικά και οι πληροφορίες ο συνδυασμός των οποίων καθιστούν ένα άτομο μοναδικό και επαναταυτοποιήσιμο. Κάθε ψηφιακό αποτύπωμα μπορεί να συμβάλλει στη συγκρότηση της ταυτότητας ενός ατόμου ως οντότητα δεδομένων, και μπορεί να υποστεί ανάλυση, ταξινόμηση ή ακόμα και στόχευση.

Αναφορικά με τα παραπάνω, μπορούμε να δούμε παράδειγμα επαναταυτοποίησης. Έστω ότι έχουμε μία ανοιχτή βάση δεδομένων όπου δεν αναφέρονται ονόματα. Έχουμε όμως ένα άτομο 30 ετών, το οποίο κατοικεί σε ένα χωριό 250 ατόμων. Αν γνωρίζουμε ότι το υποκείμενο είναι γυναίκα με επίπεδο εκπαίδευσης μεταπτυχιακού και έχει διαγνωστεί με σπάνιο νόσημα, μπορούμε

να οδηγηθούμε σε μία μοναδική ταυτοποίηση. Η πληροφοριακή ταυτότητα παραμένει εκτεθειμένη παρά την ανωνυμία [24].

4.2.2 Μηχανισμοί Επαναπροσδιορισμού

Υφίστανται αρκετοί μηχανισμοί μέσω των οποίων μπορεί να γίνει επαναταυτοποίηση ενός υποκειμένου.

Στην περίπτωση του Linkage attack, γίνεται διασταύρωση ανώνυμων δεδομένων με άλλα σύνολα δεδομένων. Παράδειγμα, ο συνδυασμός δεδομένων υγείας με δεδομένα από κοινωνικά δίκτυα [23].

Όταν υφίσταται background knowledge attack, ο επιτιθέμενος μπορεί να έχει ήδη κάποιες πληροφορίες για το υποκείμενο-θύμα και να τις χρησιμοποιήσει για τον εντοπισμό του [14]. Αν για παράδειγμα γνωρίζει ότι το υποκείμενο της επίθεσης είναι ορισμένης ηλικίας και ζει σε ήδη γνωστή περιοχή ενώ ταυτόχρονα πάσχει από σπάνια ασθένεια.

Μέσω Inference attack, μπορεί να επιτευχθεί η ταυτοποίηση μέσω ακραίων τιμών ή και στατιστικών συσχετισμών [24]. Αν σε συγκεκριμένη περιοχή ζει μόνο ένα άτομο άνω μίας συγκεκριμένης ηλικίας, είναι εύκολα αναγνωρίσιμο.

Graph-based attack. Σε αυτή την περίπτωση υφίσταται εκμετάλλευση των RTLD σε σύνδεση με το RDF με αποτέλεσμα τον εντοπισμό της ταυτότητας ενός ατόμου [13].

4.2.3 Παράγοντες Αύξησης του Κινδύνου Επαναταυτοποίησης

Υφίστανται συγκεκριμένοι παράγοντες που αυξάνουν τον κίνδυνο επαναταυτοποίησης των υποκειμένων. Όσο πιο λεπτομερή είναι τα δεδομένα, με περισσότερες διαστάσεις, τόσο ευκολότερη γίνεται η ταύτιση με συγκεκριμένο άτομο. Επιπλέον, άτομα με εξεζητημένα χαρακτηριστικά είναι ευκολότερο να ταυτοποιηθούν, ακόμα κι αν τα δεδομένα παραμένουν ανώνυμα. Όταν έχουμε διασύνδεση πολλών συνόλων δεδομένων, και πάλι αυτά μπορεί να είναι ανώνυμα ή ψευδονυμοποιημένα αλλά να οδηγήσουν σε ταυτοποίηση [36]. Ειδικά σε περιπτώσεις όπου μπορεί να γίνει χρήση εξωτερικών πηγών, όπως βάσεις δεδομένων αγορών ή κοινωνικά δίκτυα τα οποία παρέχουν πληθώρα κρίσιμων πληροφοριών.

Στηνπράξη μπορούμε να υποθέσουμε ότι έχουμε δημόσια πλατφόρμα δεδομένων που δημοσιεύει ανωνυμοποιημένα στατιστικά στοιχεία ασθενών. Αν από αυτή μπορούμε να δούμε ότι σε συγκεκριμένο δήμο συγκεκριμένης περιφέρειας υπάρχει άνδρας 48 ετών που έχει διαγνωστεί με τύπο καρκίνου σπάνιας μορφής, συνδυαστικά με την ημερομηνία διάγνωσης, και δούμε ανάρτηση σε κοινωνικά δίκτυα ή τον τοπικό Τύπο από ογκολογικό νοσοκομείο άνδρα αυτής της ηλικίας και που διαμένει στη συγκεκριμένη περιοχή, εύκολα μπορούμε να συμπεράνουμε την ταυτότητα του υποκειμένου ακόμα κι αν δεν αναφέρεται πουθενά το όνομά του [23].

4.2.4 Νομικές και Τεχνικές Επιπτώσεις και Συμπεράσματα

Σε περίπτωση που η ανωνυμοποίηση των προσωπικών δεδομένων των υποκειμένων ,μπορεί να επαναπροσδιοριστεί, θεωρείται ανεπαρκής [19]. Αυτό σημαίνει πως ενώ τα ανώνυμα δεδομένα δεν υπόκεινται στις διατάξεις του GDPR, τα επαναπροσδιοριμένα ανωνυμοπιημένα δεδομένα δεν απαλλάσσονται από αυτές [21]. Ο όποιος υπεύθυνος επεξεργασίας φέρει την ευθύνη να αποδείξει

ότι τα δεδομένα που δημοσιεύονται ως ανώνυμα και ανοιχτά δεν δύνανται να οδηγήσουν σε επαναταυτοποίηση υποκειμένων με τρόπο άμεσο ή έμμεσο. Ταυτόχρονα, θεωρείται επιβεβλημένη η χρήση τεχνικών διαχείρισης κινδύνου, όπως για παράδειγμα δοκιμές επαναπροσδιορισμού, αλλιώς re-identification testing, όπως και διαδικασία εκτίμησης αντικτύπου όταν ο κίνδυνος που αναμένεται να υπάρξει είναι υψηλός [36].

Είναι ευνόητο ότι οι κίνδυνοι επαναταυτοποίησης αποτελούν σοβαρή και απτή απειλή όσον αφορά τη χρήση και δημοσίευση των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης, ειδικά όταν τα δεδομένα αυτά σχετίζονται με ευαίσθητες και σπάνιες περιπτώσεις. Είναι πλέον κατανοητό ότι η απλή απουσία ονομάτων από τα σύνολα δεδομένων δεν είναι αρκετή για την αποφυγή των κινδύνων. Απαιτείται ακόμα να μην καθίσταται δυνατή η έμμεση ταυτοποίηση. Θα πρέπει να συνδυάζονται τεχνικά αλλά και νομικά μέσα, να αξιολογείται διαρκώς ο κίνδυνος επαναπροσδιορισμού και φυσικά τα πληροφοριακά συστήματα που χρησιμοποιούνται να είναι δομημένα με ενσωματωμένη την αρχή του Privacy by Design στο στάδιο του σχεδιασμού τους [5].

4.3 Προκλήσεις στη Διαλειτουργικότητα και Ασφάλεια

Όπως είναι ήδη γνωστό, τα Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης βασίζονται στη διασύνδεση και στην ανοιχτή πρόσβαση σε πολλές διαφορετικές πηγές πληροφορίας [3] [56]. Αυτή η διασύνδεση, όμως, είναι που δημιουργεί σοβαρές προκλήσεις αφενός για τη διαλειτουργικότητα, αφετέρου για την ασφάλεια των δεδομένων. Ειδικά στις περιπτώσεις που οι πληροφορίες που είναι διαθέσιμες ως ανοιχτά δεδομένα συνδέονται ή περιλαμβάνουν και προσωπικά δεδομένα, ο κίνδυνος για τα υποκείμενα αυτών είναι αυξημένος.

4.3.1 Προκλήσεις Διαλειτουργικότητας

Πριν ασχοληθούμε με τις προκλήσεις που πρέπει να αντιμετωπιστούν λόγω της διασύνδεσης των Ανοιχτών Δεδομένων στη διαλειτουργικότητα, ας δούμε πρώτα πώς αυτή ορίζεται.

Η Διαλειτουργικότητα αναφέρεται στην ικανότητα που έχουν διαφορετικά πληροφοριακά συστήματα, εφαρμογές και μορφές δεδομένων να επικοινωνούν μεταξύ τους, να ανταλλάσσουν πληροφορίες καθώς και να τις χρησιμοποιούν με τρόπο που είναι συνεπής και κατανοητός [3].

Όσον αφορά τα προβλήματα που μπορεί να δημιουργηθούν, βασικό θέμα αποτελεί η μη ομοιογένεια των προτύπων που χρησιμοποιούνται. Κοινώς, διαφορετικοί φορείς που χρησιμοποιούν, δημοσιεύουν και επεξεργάζονται δεδομένα κάνουν χρήση διαφορετικών σχημάτων, γλώσσας ή φόρμας. Με αυτό όμως δυσκολεύεται η ενοποίηση των συστημάτων. Άλλο θέμα που εγείρεται είναι η ασυμβατότητα της ορολογίας που χρησιμοποιείται στο εύρος των πληροφοριακών συστημάτων. Μπορούν να προκληθούν σύγχυση και λάθη όταν η ορολογία που δίνεται για την ίδια έννοια από διαφορετικά πληροφοριακά συστήματα, όπως για παράδειγμα birthdate αντί για dateofbirth. Επίσης, όταν δεν υπάρχουν κοινοί ταυτοποιητές για το ίδιο υποκείμενο ανάμεσα στα συστήματα, δεν υπάρχει δυνατότητα να υπάρξει αντιστοιχία. Τέλος, ανάμεσα στα συστήματα υπάρχει και ασυνέπεια στην πολιτική πρόσβασης που εφαρμόζουν. Κάποια συστήματα απαιτούν πιστοποίηση προκειμένου να επιτρέψουν την πρόσβαση στα δεδομένα τους, ενώ άλλα είναι ανοιχτά. Το γεγονός αυτό περιπλέκει την ενοποίηση των συστημάτων [56].

Τα παραπάνω έχουν ορισμένες αναμενόμενες συνέπειες. Η ανάλυση των δεδομένων που επιτυγχάνεται μπορεί να είναι ελλιπής ή παραμορφωμένη. Ταυτόχρονα, λόγω ακριβώς της παραμόρφωσης των στοιχείων, αυξάνεται ο κίνδυνος λανθασμένης συσχέτισης που θα μπορούσε με τη σειρά του να οδηγήσει στη χωρίς πρόθεση ταυτοποίηση ατόμων, παραβιάζοντας έτσι την ιδιωτικότητα [13]. Όλα αυτά οδηγούν στην μείωση της αξιοπιστίας των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης ως υποδομή παροχής πληροφορίας.

4.3.2 Προκλήσεις Ασφάλειας

Προκειμένου να έχουμε τη διάθεση και τη χρήση των Ready to Link Data, βασικό ρόλο παίζει η ύπαρξη ασφάλειας για τα δεδομένα και τα υποκείμενά τους. Τα Ανοιχτά Δεδομένα εξ ορισμού είναι συνδεδεμένα με ορισμένους κινδύνους, κυρίως όσον αφορά την ασφάλεια των δεδομένων και δη των προσωπικών [4]. Τα πρώτα είναι εκ φύσεως ανοιχτά, τα δε δεν είναι κατάλληλα για δημόσια έκθεση. Πρώτος βασικός κίνδυνος λοιπόν είναι η μη εξουσιοδοτημένη πρόσβαση σε δεδομένα. Κατά δεύτερον, κακόβουλοι χρήστες επιτιθέμενοι μέσω API μπορούν να εξάγουν ευαίσθητες πληροφορίες για άτομα ή ακόμα να πραγματοποιήσουν επιθέσεις επαναπροσδιορισμού ταυτότητας [5]. Ένας ακόμα κίνδυνος μπορεί να προέρχεται όχι από τα ίδια τα δεδομένα που είναι διαθέσιμα, αλλά από τα μεταδεδομένα τους. Εφόσον δεν έχει προηγηθεί επαρκής έλεγχος αυτών, μπορεί να αποκαλύψουν περισσότερα από τα δεδομένα οδηγώντας έτσι σε παραβίαση της ιδιωτικότητας με έμμεσο τρόπο [10]. Κακόβουλα υποκείμενα μπορεί ακόμα να εκμεταλλευτούν σχέσεις RDF δημιουργώντας χάρτες που θα επιτρέψουν τη δημιουρία προφίλ υποκειμένου ή την ταυτοποίηση [53]. Η χρήση, ή μάλλον, κατάχρηση, των πληροφοριών που προκύπτουν από την επεξεργασία των δεδομένων δεν χρησιμοποιείται αποκλειστικά για κυβερνο-επιθέσεις, κάτι που εν τέλει μοιάζει πολύ μακρινό στους περισσότερους από εμάς. Μπορεί όμως να χρησιμοποιηθεί και για να εξάγονται πληροφορίες ακόμα και για εμπορική χρήση [6].

4.3.3 Τεχνικά Μέτρα Αντιμετώπισης

Προκειμένου να αντιμετωπιστεί ο κίνδυνος της ασφάλειας στο χώρο των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης, υπάρχει η δυνατότητα λήψης ορισμένων μέτρων που δεν θα εκμηδενίσουν τον κίνδυνο αλλά σίγουρα θα τον περιορίσουν.

Η ταυτοποίηση του ατόμου που αιτείται πρόσβαση σε ευαίσθητα σύνολα δεδομένων είναι ένα από αυτά. Ένα επιπλέον μέτρο που είναι χρήσιμο για την αντιμετώπιση των κινδύνων που εμφανίζονται κατά τη χρήση των ανοιχτών βάσεων δεδομένων είναι τα rate-limiting APIs. Εδώ περιορίζεται ο αριθμός αιτημάτων ανά χρήστη της κάθε βάσης ώστε να αποφευχθεί η αυτόματη εξαγωγή δεδομένων από ιστοσελίδες ή βάσεις δεδομένων [21]. Ένα άλλο μέτρο είναι να εφαρμόζονται διαφορετικά επίπεδα ανωνυμοποίησης ανάλογα με το περιβάλλον στο οποίο δημοσιεύονται τα δεδομένα. Όσο ευκολότερα είναι αυτά προσβάσιμα, τόσο θα πρέπει να βελτιώνεται και το επίπεδο της ανωνυμοποίησης [34]. Όσον αφορά τώρα τις πολιτικές πρόσβασης στις βάσεις δεδομένων, θα πρέπει να καθορίζονται ρητά οι όροι και τα όρια της επαναχρησιμοποίησης και επεξεργασίας των δεδομένων [18].

Τα ως άνω αναφέρονται στην προστασία των ευαίσθητων και προσωπικών δεδομένων κατά τη διασύνδεση των συστημάτων και των βάσεων που τα φέρουν. Ως προς την καλύτερη διασύνδεση των βάσεων, όμως, ώστε να αποφευχθεί και η λανθασμένη συσχέτιση με άτομα

διαφορετικά του υποκειμένου των προσωπικών δεδομένων, ως αναφέρθηκε παραπάνω, θα ήταν σκόπιμη η προτυποποίηση λεξιλογίου και ορολογίας που θα χρησιμοποιείται ευρέως από τα πληροφορικά συστήματα και θα ενισχύσει τη συμβατότητα με τη χρήση κοινών λεξιλογίων [10], [12], [29].

Συμπερασματικά, η χρήση των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης θα πρέπει να συνοδεύεται από ασφάλεια, ώστε να αποτελούν εργαλείο διαφάνειας και προόδου και όχι εργαλείο παραβίασης της ιδιωτικότητας των ατόμων [6], [16], [33].

RTLD, Διαλειτουργικότητα και Κίνδυνοι για την Ιδιωτικότητα και την Ασφάλεια (Πίνακας 5)

RTLD	Παρέχουν ανοιχτά και συνδεδεμένα δεδομένα με σκοπό την επαναχρησιμοποίηση και επεξεργασία
Διαλειτουργικότητα	Διευκολύνει τη σύνδεση δεδομένων μεταξύ ποικίλων πηγών
Συνδεσιμότητα	Συμβάλει στη δημιουργία πλούσιων γραφικών γνώσης
Συνδυασμός Δεδομένων	Διευκολύνει τη συσχέτιση και τη συλλογιστική αλλά και την επαναταυτοποίηση
Κίνδυνοι	Πιθανότητα παραβίασης ιδιωτικότητας σε περίπτωση ελλιπών μέτρων
Ανάγκη Προστασίας	Χρήση τεχνικών όπως η ανωνυμοποίηση, η ψευδονυμοποίηση και άλλες.

4.4 Δυναμικές Παραβίασης Προσωπικών Δεδομένων μέσω Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης

Σε αυτή την ενότητα σημειώνονται μηχανιστικές και δομικές αιτίες που δύνανται να οδηγήσουν σε παραβίαση προσωπικών δεδομένων σε πλαίσια εφαρμογής τεχνολογίας Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης [7], [20].

4.4.1 Η Φύση των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης ως Παράγοντας Κινδύνου

Τα Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης υφίστανται ως μέσο προαγωγής της διαφάνειας, της διασυνδεσιμότητας και της επαναχρησιμοποίησης και επεξεργασίας των δεδομένων [51]. Τα ανωτέρω χαρακτηριστικά είναι ευεργετικά για την καινοτομία και τη Δημοκρατία [13], αλλά ταυτόχρονα διαθέτουν τα δεδομένα προσβάσιμα σε κοινό πέρα από το προβλεπόμενο, ταυτόχρονα επιτρέπουν στα δεδομένα να συσχετίζονται με άλλα σύνολα και όλο αυτό έχει ως αποτέλεσμα τη δυσκολία της προστασίας των προσωπικών πληροφοριών των υποκειμένων ακόμα και στην περίπτωση που έχει γίνει χρήση τεχνικών ανωνυμοποίησης [21].

4.4.2 Μηχανισμοί Παραβίασης μέσω Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης

Οι παραβιάσεις που μπορούν να συμβούν με τη χρήση των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης αφορούν εξίσου κακόβουλη πρόθεση αλλά και τεχνικά ζητήματα [10], [5].

Στην περίπτωση του επαναπροσδιορισμού της ταυτότητας του υποκειμένου, έχουμε αβλαβή δεδομένα, ακόμα και ανώνυμα, που όταν συνδυάζονται με εξωτερικές πηγές μπορούν να οδηγήσουν σε ταυτοποίηση φυσικού προσώπου [2], [26].

Σε άλλη περίπτωση, οι σχέσεις RDF και τα URI έχουν τη δυνατότητα να επιτρέψουν την ανακατασκευή κοινωνικών ή/και θεσμικών δικτύων και άρα την αποκάλυψη προσωπικών δεδομένων μέσω γραφικών σχέσεων [53].

Τρίτη περίπτωση όπου έχουμε κακόβουλη χρήση της τεχνολογίας των RTLD είναι αυτή της κακόβουλης επεξεργασίας τους από τρίτους. Εδώ παρατηρείται η δημιουργία προφίλ για τα υποκείμενα και η ανάλυσή τους από ιδιωτικούς φορείς, όπως για τη στόχευση των διαφημίσεων ή τον επηρεασμό των πολιτικών επιλογών [8], [41].

Σε καταστάσεις που η παραβίαση έχει ως αφετηρία τεχνικά προβλήματα, μπορούμε να έχουμε σφάλματα καταρχήν στην ανωνυμοποίηση των δεδομένων [25], γεγονός που μπορεί να οδηγήσει στην ψευδαίσθηση της προστασίας, ενώ ελλείψεις στην προστασία και των μεταδεδομένων και τυχόν διαρροή αυτών μπορεί και πάλι να οδηγήσει σε επαναταυτοποίηση ατόμων [27]. Μία ακόμα περίπτωση είναι να υφίστανται σφάλματα διαλειτουργικότητας. Εδώ, κινδυνεύουμε να έχουμε ως αποτέλεσμα ευαίσθητα ή παραπλανητικά δεδομένα και πληροφορίες ως αποτέλεσμα της κακής μετατροπής ή συγχώνευσης των Ανοιχτών Δεδομένων [14], [3].

4.4.3 Τύπος RTLD και Επίπεδα Κινδύνου

Κάθε είδος Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης δεν φέρει το ίδιο επίπεδο κινδύνου κατά τη χρήση και επεξεργασία του [19]. Αναφορικά, όταν τα δεδομένα αφορούν δημογραφικά σύνολα το επίπεδο κινδύνου είναι μεσαίο, όπως στατιστικά στοιχεία ανά περιοχή. Όταν έχουμε υγειονομικά δεδομένα ο κίνδυνος είναι υψηλός όπως συμβαίνει όταν κάποιος χρησιμοποιεί ή επεξεργάζεται στοιχεία νοσηρότητας [48], [9]. Στην περίπτωση εκπαιδευτικών και ακαδημαϊκών δεδομένων, όπως βιογραφικά και έργα και πάλι τα επίπεδα κινδύνου χαρακτηρίζονται ως μεσαία, ενώ όταν έχουμε συναλλαγές πολιτών με το κράτος το επίπεδο κινδύνου είναι υψηλό καθώς υφίσταται επεξεργασία οικονομικών δεδομένων και δημόσιων συμβάσεων [17], [23]. Πολύ υψηλός είναι ο κίνδυνος επαναταυτοποίησης όταν έχουμε να κάνουμε με ωφελούμενους κοινωνικών προγραμμάτων και δεδομένα από κοινωνικές υπηρεσίες [19].

4.4.4 Νομοθετικές και Τεχνικές Λύσεις

Για την επίτευξη προστασίας των προσωπικών και ευαίσθητων δεδομένων από παραβιάσεις απαιτείται αντιμετώπιση σε πολλά επίπεδα. Με αφετηρία τα μέτρα που επιβάλει ο GDPR [57] εφαρμόζονται οι αρχές του Privacy by Design, που όπως έχει ήδη αναφερθεί αφορά την ένταξη της προστασίας στην αρχιτεκτονική δομή των πληροφοριακών συστημάτων και την ελαχιστοποίηση των δεδομένων [54], [33]. Εφαρμόζονται επίσης κατάλληλα τεχνικά μέτρα (k-anonymity, I-diversity, differential privacy) [28]. Υφίστανται και κανονισμοί πρόσβασης στις βάσεις δεδομένων με περιορισμούς στην επεναχρησιμοποίηση των δεδομένων και υποχρεωτικές άδειες πρόσβασης ώστε σε βάσεις με δεδομένα με υψηλό ρίσκο να μην έχει πρόσβαση ο οποιοσδήποτε και τέλος οφείλει να υφίσταται διαρκής παρακολούθηση του κινδύνου που δύναται να εμφανιστεί σε κάθε νέα διασύνδεση ή χρήση των δεδομένων [50], [55].

Με βάση τα ανωτέρω, η παραβίαση των προσωπικών δεδομένων στα πλαίσια της χρήσης των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης είναι ένα χαρακτηριστικό και κίνδυνος που ενυπάρχει σε αυτά λόγω της φύσης τους. Η συνύπαρξή τους με την ιδιωτικότητα είναι εφικτή όταν ισορροπείται η ζυγαριά μεταξύ διαφάνειας και προστασίας, η οποία ενσωματώνεται εξ αρχής και ταυτόχρονα καλλιεργείται μία θεώρηση ευθύνης νομικής και τεχνικής [6], [24].

Κίνδυνοι και Προστασία στα Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης (Πίνακας 6)

Τύπος Κινδύνου	**Περιγραφή**	**Πιθανές Συνέπειες**	**Αντίμετρα/Μηχανισμοί Προστασίας**
Επαναπροσδιορισμός	Συσχέτιση Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης με εξωτερικά δεδομένα προκαλεί επαναταυτοποίηση	Παραβίαση ιδιωτικότητας, νομικές κυρώσεις	Anonymization, k-anonymity, differential privacy
Γραφική Ανάλυση RDF σχέσεων	Εντοπισμός ταυτοτήτων μέσω σχέσεων	Έμμεση ταυτοπίηση, δημιουργία προφίλ	Εξάλλειψη-περιορισμός δισυνδέδεων με προσωπικό χαρακτήρα
Διαρροή από Μεταδεδομένα	Πληροφορίες που αποκαλύπτουν ταυτότητα υποκειμένων	Έκθεση ονομάτων, ρόλων ή χρονολογίου σχετικών με συγκεκριμένα πρόσωπα	Φιλτράρισμα μεταδεδομένων, ελαχιστοποίηση πληροφοριών
Ελλιπής Ανωνυμοποίηση	Λανθασμένη επιλογή τεχνικών, ανεπαρκή εργαλεία	Ψευδής αίσθηση ασφάλειας, δυνατότητα επανασυσχέτισης	DPIA
Ανεξέλεγκτη Επαναχρησιμοποίηση	Τρίτοι επαναχρησιμοποιούν τα δεδομένα για σκοπούς δημιουργίας προφίλ ή εμπορικής εκμετάλλευσης	Παραβίαση δικαιωμάτων ατόμων, στοχοποίηση	Περιοριστικές άδειες χρήσης, περιορισμοί πρόσβασης
Ανεπαρκής Έλεγχος Πρόσβασης	Ελεύθερη πρόσβαση σε ευαίσθητα και προσωπικά δεδομένα	Μαζική εξαγωγή δεδομένων	API keys

5 *Βέλτιστες Πρακτικές και Προτάσεις*

Το κεφάλαιο 5 αναφέρεται στις ήδη υπάρχουσες πρακτικές και προσεγγίσεις που υφίστανται για την προστασία των προσωπικών δεδομένων καθώς αυτά επεξεργάζονται και δημοσιεύονται ως Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης. Το γεγονός ότι υφίσταται διαρκώς αυξανόμενη ζήτηση για διαφάνεια και λογοδοσία από φορείς του δημόσιου αλλά και ιδιωτικού τομέα καθιστά την ανάγκη πρακτικών και αποτελεσματικών μέτρων για την προστασία των δεδομένων και των υποκειμένων τους. Στην παρούσα ενότητα αναλύονται τεχνικές και οργανωτικές στρατηγικές που έχουν τη δυνατότητα να συμβάλουν στην επίτευξη ισορροπίας μεταξύ της διαφάνειας και της προστασίας της ιδιωτικότητας.

5.1 Βέλτιστες Πρακτικές Προστασίας των Προσωπικών Δεδομένων

Ως προς το στόχο της προστασίας των προσωπικών δεδομένων, δεν δύναται η επίτευξή του απλώς μέσω νομοθετικών ρυθμίσεων. Θα πρέπει να ενσωματωθεί επίσης ένα πλαίσιο πρακτικών που θα λειτουργεί ως πρόληψη και θα αποτρέπει τους κινδύνους. Έχουμε λοιπόν τεχνικές πρακτικές και οργανωτικές πρακτικές και πώς ακριβώς λειτουργούν και μειώνουν τον κίνδυνο, καθώς και παραδείγματα ανά περίπτωση για την καλύτερη κατανόησή τους.

Ως προς την κατηγορία των τεχνικών πρακτικών, αρχικά συναντάμε την ενσωμάτωση της προστασίας στην αρχιτεκτονική των πληροφοριακών συστημάτων καθ' όλη τη διάρκεια ζωής της πληροφορίας. Από το στάδιο του σχεδιασμού, πρέπει να ενσωματώνονται ορισμένα φίλτρα, περιορισμοί και μηχανισμοί ανωνυμοποίησης στις βάσεις δεδομένων και τις εφαρμογές που φέρουν τις πληροφορίες. Η τεχνική αυτή είναι γνωστή ως Privacy by Design [5]. Έστω ότι σε μία πλατφόρμα Ανοιχτών δεδομένων που αφορούν τη δημόσια υγεία, προβλέπεται βάσει σχεδιασμού ότι τα ονόματα και οι αριθμοί μητρώου των ασθενών δεν αποθηκεύονται. Τα δεδομένα εμφανίζονται μόνο με κωδικοποιημένο αριθμό ταυτότητας.

Σε περιπτώσεις που θέλουμε μείωση της πιθανότητας να ταυτοποιηθούν τα υποκείμενα των δεδομένων χρησιμοποιούνται οι τεχνικές της ανωνυμοποίησης και ψευδονυμοποίησης [2],

[5], [28]. Εδώ, πριν τη δημοσίευση ενός συνόλου δεδομένων με, ας πούμε, στατιστικά απασχόλησης, θα αφαιρεθούν όλα τα προσωπικά στοιχεία των εργαζομένων και αυτές οι εγγραφές θα ορίζονται με έναν τυχαίο αριθμό ως ψευδώνυμο ώστε να μην δύναται κάποιος να αναγνωρίσει φυσικά πρόσωπα βάσει των πληροφοριών που καθίστανται διαθέσιμες.

Ένας ακόμα τρόπος να προστατευτούν τα προσωπικά δεδομένα και τα υποκείμενά τους είναι ο περιορισμός της πρόσβασης σε αυτά μέσω API. Για την αποφυγή της μαζικής εξαγωγής ευαίσθητων δεδομένων, καθορίζονται ο ρόλος και τα δικαιώματα κάθε χρήστη ή συστήματος [3], [6]. Αν για παράδειγμα μία δημόσια υπηρεσία παρέχει μεν πρόσβαση σε Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης αλλά περιορίζει τη χρήση με βάση διαφορετικά επίπεδα πρόσβασης, οι ερευνητές μπορούν να έχουν πλήρη πρόσβαση στα ανωνυμοποιημένα δεδομένα ενώ οι ιδιώτες μόνο σε σύνολα γενικής στατιστικής πληροφορίας, προστατεύοντας έτσι τα δεδομένα από κακόβουλη χρήση.

Τέλος, υφίσταται και η τεχνική της συνεχούς ανάλυσης του ρίσκου, όπου αξιολογούνται διαρκώς οι κίνδυνοι που μπορεί να εμφανιστούν με κάθε νέα διασύνδεση δεδομένων. Στόχος είναι η αποφυγή διαρροών ή/και παραβιάσεων [10], [25], [28]. Ως παράδειγμα παρατίθεται περίπτωση που μία δημόσια αρχή προχωρά σε αξιολόγηση ρίσκου ως προς το ενδεχόμενο επαναταυτοποίησης των χρηστών, κάθε φορά που πρόκειται να εκδοθεί νέα ανοιχτή βάση δεδομένων, ειδικά όταν αυτή θα διασυνδέεται μα βάσεις τρίτων μερών.

Ως προς την κατηγορία τώρα των οργανωτικών πρακτικών που χρησιμοποιούνται για την προστασία των δεδομένων, αρχικά έχουμε τον ορισμό ενός υπεύθυνου προστασίας δεδομένων, δηλαδή τον καθορισμό ενός προσώπου ή τμήματος με την αρμοδιότητα να επιτηρεί τη συμμόρφωση με τα νομικά και τεχνικά πλαίσια που απαιτούνται [57], [58]. Ένας δήμος που αναρτά νέα δημοσίευση με δεδομένα, πρέπει να έχει ορίσει υπεύθυνο που θα εξασφαλίσει ότι η νέα αυτή δημοσίευση είναι σύμφωνη με το εθνικό νομοθετικό πλαίσιο και τον GDPR.

Σε οργανωτικό επίπεδο, υφίστανται επίσης διάφορες εσωτερικές πολιτικές και πρωτόκολλα που αποσκοπούν στη διασαφήνιση των διαδικασιών της επεξεργασίας, αποθήκευσης και κοινοποίησης των δεδομένων [1], [4], [33]. Ένας ερευνητικός οργανισμός, για παράδειγμα, μπορεί να καθορίζει εσωτερικά πολιτική που θα απαγορεύει να διατηρούνται προσωπικά δεδομένα σε servers χωρίς αυτά να είναι κρυπτογραφημένα, ενώ ταυτόχρονα να απαιτεί να αποθηκεύονται τα δεδομένα μόνο σε παρόχους cloud οι οποίοι είναι διαπιστευμένοι, διατηρώντας έτσι ένα καλύτερο επίπεδο ασφάλειας.

Επειδή πάντα, σε κάθε διαδικασία, εμπλέκεται και ο ανθρώπινος παράγοντας, και όλες οι πρακτικές είτε πρόκειται για τεχνικές είτε για οργανωτικές εξαρτώνται από ανθρώπους για τη διεξαγωγή και θέσπισή τους, μία ακόμα ιδιαίτερα σημαντική πρακτική σε οργανωτικό επίπεδο αφορά την εκπαίδευση των στελεχών που διαχειρίζονται τα δεδομένα. Με τη διαρκή και συστηματική αυτή εκπαίδευση μειώνεται η πιθανότητα του ανθρώπινου λάθους κατά τη διαχείριση των δεδομένων [39], [42]. Ως παράδειγμα αναφέρουμε την υποχρεωτική παρακολούθηση σεμιναρίου κάθε χρόνο από στελέχη ενός υπουργείου σχετικά με τεχνικές πρακτικές προστασιας δεδομένων, όπως η ανωνυμοποίηση, η ψευδονυμοποίηση και η πρόληψη των παραβιάσεων.

Τέλος, όσον αφορά την οργάνωση, καλό είναι να υπάρχει πρόβλεψη και για την ψηφιακή παιδεία των πολιτών, δηλαδή την ενημέρωση και εκπαίδευση των πολιτών σχετικά με τα

δικαιώματά τους, το σκοπό επεξεργασίας των δεδομένων τους αλλά και τα μέσα προστασίας που χρησιμοποιούνται ως προς αυτό [6], [21], [23]. Έστω λοιπόν ότι έχουμε ένα δημόσιο portal που θα δημοσιεύσει έναν οδηγό χρήσης δεδομένων όπου και θα αναφέρεται ο ορισμός των προσωπικών δεδομένων, θα εξηγείται ο τρόπος με τον οποίο μπορεί ο χρήστης να διαχειρίζεται τα δικαιώματά του και πώς θα μπορεί να αιτηθεί διαγραφή ή διόρθωση των δεδομένων του.

5.2 Πολιτικές και Πρωτόκολλα Διαχείρισης Προσωπικών Δεδομένων σε Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης

Οι τεχνικές που υφίστανται επί του παρόντος για την προστασία των προσωπικών δεδομένων είναι μεν αναγκαίες, αλλά δεν επαρκούν ως προς το σκοπό αυτό. Θα πρέπει να συνδυάζονται με την εφαρμογή συγκεκριμένων πολιτικών και πρωτόκολλων διαχείρισης δεδομένων ώστε να επιτευχθεί το ζητούμενο της προστασίας των δεδομένων και της ιδιωτικότητας στα πλαίσια των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης [2], [17], [28]. Οι πολιτικές αυτές θα πρέπει να καθορίζουν το ποιος θα έχει δικαίωμα πρόσβασης στην εκάστοτε βάση δεδομένων καθώς και σε ποια από αυτά τα δεδομένα θα έχει πρόσβαση, όπως επίσης θα πρέπει να ορίζεται και ο σκοπός της επεξεργασίας των δεδομένων και η νομική βάση αυτού [57]. Θα πρέπει επίσης να υπάρχει πρόβλεψη για το εύρος του χρονικού διαστήματος κατά το οποίο τα δεδομένα θα διατηρούνται στις βάσεις αλλά και το πότε αυτά θα διαγράφονται [25]. Και εφόσον τα δεδομένα αφορούν συγκεκριμένα υποκείμενα, θα πρέπει να ορίζονται και οι διαδικασίες που θα ισχύουν για την ενημέρωση των υποκειμένων, καθώς και για τυχόν αιτήσεις διαγραφής και διόρθωσης πληροφοριών τους [55].

Με το να τηρούνται τέτοιες πολιτικές επιτυγχάνεται αφενός η συμμόρφωση με το νομικό πλαίσιο, αφετέρου η αύξηση της εμπιστοσύνης των πολιτών στην επεξεργασία των δεδομένων τους [11], [23]. Όταν οι παραπάνω πολιτικές εφαρμόζονται συνδυαστικά με τις τεχνικές λύσεις που αναφέρθηκαν στην προηγούμενη ενότητα, έχουμε πλέον λειτουργικό και συστηματικό χαρακτήρα στην προστασία της ιδιωτικότητας [5], [25].

5.2.1 Παραδείγματα Κρίσιμων Πολιτικών

Παρατίθενται ορισμένα παραδείγματα πολιτικών που υφίστανται και που μπορούν να προωθήσουν την ασφάλεια της ιδιωτικότητας μέσω της προστασίας των προσωπικών και ευαίσθητων δεδομένων.

Υιοθετείται η πολιτική της ελαχιστοποίησης των δεδομένων. Τα δεδομένα που συλλέγονται και δημοσιοποιούνται θα πρέπει να είναι τα απολύτως απαραίτητα για το σκοπό για τον οποίο συλλέγονται εξ αρχής [57].

Μία επιπλέον πολιτική που ακολουθείται είναι αυτή της διαφάνειας. Οι χρήστες του εκάστοτε πληροφοριακού συστήματος ή εφαρμογής θα πρέπει να ενημερώνονται με σαφήνεια και με απλή και κατανοητή γλώσσα σχετικά με τον τρόπο που γίνεται η επεξεργασία των δεδομένων τους [1], [2].

Τέλος, υπάρχει και το παράδειγμα της πολιτικής ανταπόκρισης σε αιτήματα των υποκειμένων. Είναι σκόπιμη η ύπαρξη μηχανισμού όπου θα μπορούν να υποβάλλονται αιτήματα

των υποκειμένων των δεδομένων σχετικά με την πρόσβαση σε αυτά, τυχόν αντιρρήσεις που θα εγείρονται, διόρθωσή τους ή και διαγραφή τους σύμφωνα πάντα με τον GDPR [25], [55], [57].

5.2.2 Πρωτόκολλα Εφαρμογής

Αναφορικά με τα πρωτόκολλα που εργαλειοποιούνται για την ενίσχυση της προστασίας των προσωπικών δεδομένων, διακρίνουμε ότι υπάρχουν πρωτόκολλα που αναφέρονται στην καταγραφή των διεργασιών επεξεργασίας, στην εκτίμηση του αντικτύπου στην προστασία των δεδομένων, καθώς και σε πρωτόκολλα κοινοποίησης σε τρίτους.

Όσον αφορά την πρώτη κατηγορία, αυτή της καταγραφής των διεργασιών επεξεργασίας, και πάντα σε συμφωνία με τον GDPR, κάθε οργανισμός που διαχειρίζεται δεδομένα θα πρέπει να καταγράφει το είδος των δεδομένων που συλλέγει, το λόγο που τα συλλέγει, δηλαδή τον σκοπό της επεξεργασίας, θα πρέπει επίσης να ορίζει ποιος θα έχει πρόσβαση σε αυτά, το πού αυτά θα αποθηκεύονται καθώς και για πόσο χρονικό διάστημα [57], [58]. Η σημασία αυτών τον πρωτόκολλων έγκειται στο γεγονός ότι σε περιβάλλοντα Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης όπου υφίστανται πολλές πηγές και πολλές διασυνδέσεις των πηγών αυτών, η διαφάνεια καθίσταται δύσκολη [10], [17]. Τα πρωτόκολλα αυτά λειτουργούν ως ένας χάρτης διαχείρισης του συνόλου των δεδομένων, γεγονός που επιτρέπει την παρακολούθηση των διαδικασιών, των διασυνδέσεων και συνεπώς της λογοδοσίας [6], [25].

Στην περίπτωση των πρωτόκολλων εκτίμησης αντίκτυπου στην προστασία δεδομένων, μιλάμε για την προληπτική μελέτη που θα εξάγει συμπεράσματα ως προς την εκτίμηση των κινδύνων για τα δικαιώματα των υποκειμένων των δεδομένων [10], [25], [33]. Λαμβάνουν χώρα πριν από κάθε δημοσίευση ενός νέου συνόλου δεδομένων, σε περίπτωση διασύνδεσης με διαφορετικές βάσεις δεδομένων ή όταν πρόκειται να γίνει εισαγωγή μίας νέας τεχνολογίας. Η σημασία τους εντοπίζεται στο ότι πρόκειται για προληπτική μέθοδο, δηλαδή μετριάζεται η πιθανότητα πραγματοποίησης του κινδύνου και κατά συνέπεια μείωση των παραβιάσεων, ειδικά σε περιβάλλοντα RTLD που αποτελεί πραγματικότητα ο απρόβλεπτος επαναπροσδιορισμός ταυτότητας [2], [19] [28].

Τέλος, περιγράφουμε τα πρωτόκολλα κοινοποίησης σε τρίτους, όπου αναφέρονται στα προαπαιτούμενα της παραχώρησης προσωπικών δεδομένων σε άλλους φορείς, δημόσιους ή ιδιωτικούς [54], [57]. Προκειμένου να υπάρξει κοινοποίηση θα πρέπει να έχουν προηγηθεί συμβάσεις επεξεργασίας δεδομένων, να έχει ελεγχθεί η συμβατότητα με το νομικό πλαίσιο του αποδέκτη και θα έχουν προκαθοριστεί οι όροι και οι περιορισμοί της επεξεργασίας των δεδομένων [25], [57]. Η σημασία των πρωτοκόλλων αυτών έγκειται στο ότι όταν δεν υπάρχει έλεγχος, τα δεδομένα δύνανται να χρησιμοποιηθούν για σκοπούς διαφορετικούς των αρχικών ή ακόμα και να προωθηθούν σε χώρες όπου δεν υφίσταται επαρκές επίπεδο προστασίας [16], [35], [36].

5.2.3 Θεωρητικά Παραδείγματα Πρωτόκολλων Εφαρμογής

Παρατίθενται θεωρητικά παραδείγματα για την καλύτερη κατανόηση του τρόπου με τον οποίο τα ανωτέρω πρωτόκολλα συμβάλλουν στην προστασία της ιδιωτικότητας.

Για την καταγραφή των διεργασιών επεξεργασίας, μπορούμε να δούμε την περίπτωση όπου ένας δήμος διατηρεί πλατφόρμα Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης όπου

περιλαμβάνονται στατιστικά στοιχεία σχετικά με τις αιτήσεις κοινωνικής πρόνοιας. Συντάσσεται και διατηρείται από την υπηρεσία πληροφορικής αρχείο όπου καταγράφεται το τμήμα που συλλέγει τα δεδομένα, ότι αυτά αφορούν μεταξύ άλλων ημερομηνία αίτησης, ηλικιακή ομάδα και ταχυδρομικό κώδικα, καταγράφεται επίσης ο σκοπός συλλογής και επεξεργασίας, ας οριστεί ως στατιστική ανάλυση για το σχεδιασμό πολιτικών στήριξης. Αναφέρεται επίσης ότι τα δεδομένα της βάσης αποθηκεύονται σε server εντός ης ΕΕ και ότι τα δεδομένα θα διατηρηθούν για πέντε έτη. Το αρχείο αυτό μπορεί να αποδείξει τη συμμόρφωση με τον Κανονισμό GDPR σε περίπτωση που διεξαχθεί έλεγχος.

Τα πρωτόκολλα εκτίμησης αντικτύπου μπορούν να οδηγήσουν σε αλλαγές στον τρόπο που σχεδιάζεται το σύνολο των δεδομένων (dataset), με στόχο την ασφαλή δημοσίευση χωρίς να υπονομεύεται η ιδιωτικότητα. Έστω ότι ένα πανεπιστήμιο προτίθεται να δημοσιεύσει διασυνδεδεμένη βάση δεδομένων όπου θα αναφέρονται στοιχεία των φοιτητών με σκοπό την ανάλυση των επιδόσεων. Τα δεδομένα θα περιλαμβάνουν στοιχεία όπως φύλο, βαθμολογίες και τόπο διαμονής. Πριν προβεί σε δημοσίευση προχωρά σε ανάλυση κινδύνου ώστε να αξιολογηθεί ο κίνδυνος επαναταυτοποίησης, ιδιαίτερα χρήσιμη πρακτική όταν υποθέτουμε ότι τα δεδομένα ανήκουν σε υποκείμενα που ανήκουν σε μικρή πληθυσμιακή ομάδα όπως φοιτητές από νησιά, και εντοπίζει την ανάγκη να αθροίσει τις εγγραφές κατά περιφέρεια και όχι κατά δήμο ώστε να μειωθεί η πιθανότητα επαναταυτοποίησης.

Αναφορικά με τα πρωτόκολλα κοινοποίησης σε τρίτους, μπορούμε να δώσουμε ένα παράδειγμα αν υποθέσουμε την παραχώρηση ανωνυμοποιημένων δεδομένων σχολικής φοίτησης σε ιδιωτική εταιρία με σκοπό την έρευνα από το Υπουργείο Παιδείας. Αρχικά θα συνταχθεί συμφωνητικό επεξεργασίας όπου θα ορίζεται ότι τα δεδομένα θα χρησιμοποιηθούν αποκλειστικά και μόνο για ακαδημαϊκή ανάλυση, ότι θα απαγορεύεται η συσχέτιση των δεδομένων με εξωτερικές πηγές και τέλος ότι η εταιρία θα υποχρεούται να καταστρέψει τα δεδομένα μετά το πέρας της έρευνας. Με τον τρόπο αυτό το πρωτόκολλο προστατεύει από την κατάχρηση των δεδομένων για άλλους σκοπούς μη θεμιτούς και ελέγχει το τι επιτρέπεται ή απαιτείται να γίνει με τα δεδομένα μετά την παραχώρησή τους.

Πρωτόκολλα Εφαρμογής και Θεωρητικά Παραδείγματα (Πίνακας 7)

Πρωτόκολλο Εφαρμογής	**Περιγραφή**	**Θεωρητικό Παράδειγμα**
Καταγραφή Διεργασιών Επεξεργασίας	Αναλυτική τεκμηρίωση των δεδομένων, σκοπών. αποθηκευτικών μέσων, προσβάσεων και χρόνου διατήρησης	Δήμος καταγράφει τα σύνολα RTLD που αφορούν αιτήσεις πρόνοιας με σκοπό τη διαφάνεια και λογοδοσία σύμφωνα με τον GDPR
Εκτίμηση Αντικτύπου	Αξιολόγηση κινδύνου ιδιωτικότητας πριν από επεξεργασία ή διασύνδεση	Πανεπιστήμιο διενεργεί έλεγχο κινδύνου πριν τη δημοσίευση φοιτητικών δεδομένων και τροποποιεί το dataset ώστε αυτός να μειωθεί.
Πρωτόκολλα Κοινοποίησης σε Τρίτους	Νομικά και οργανωτικά μέτρα για τον έλεγχο παραχώρησης δεδομένων σε εξωτερικούς	Υπουργείο Παιδείας υπογράφει σύμβαση με ερευνητική εταιρία

	φορείς	περιορίζοντας τη χρήση των RTLD και επιβάλλοντας διαγραφή μετά την ολοκλήρωση του έργου

5.3 Εκπαίδευση και Ευαισθητοποίηση Οργανισμών και Πολιτών

Το ζήτημα της προστασίας των προσωπικών δεδομένων δεν αφορά μόνο τεχνικές λύσεις και νομικό πλαίσιο. Πρόκειται για ένα ζήτημα που άπτεται της κουλτούρας, της αντίληψης και της καθημερινής πρακτικής των πολιτών [37]. Είναι λοιπόν συνεπακόλουθο ότι η εκπαίδευση και ευαισθητοποίηση πολιτών αλλά και οργανισμών παίζει κρίσιμο ρόλο στη χρήση και επεξεργασία των δεδομένων με τρόπο που θα ωθήσει σε πρόοδο και δημοκρατικές πρακτικές [6], [23].

Το να καλλιεργηθεί ψηφιακή παιδεία και να εκπαιδευτούν ανάλογα οι φορείς μπορεί να οδηγήσει στη δημιουργία ενός ενεργού και ενημερωμένου οικοσυστήματος διαχείρισης των δεδομένων όπου θα εφαρμόζεται και θα λειτουργεί η ισορροπία μεταξύ της διαφάνειας και της ιδιωτικότητας [2], [11], [22].

5.3.1 Εκπαίδευση Οργανισμών

Όταν ορισμένοι φορείς διαχειρίζονται ή δημοσιεύουν Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης, οφείλουν να διασφαλίζουν ότι το προσωπικό τους θα γνωρίζει αρχικά τις υποχρεώσεις που υφίστανται για την ασφαλή και νόμιμη δημοσίευση και επεξεργασία των δεδομένων βάσει GDPR [57], καθώς και ότι τα στελέχη του έχουν εκπαιδευτεί στις τεχνικές της ανωνυμοποίησης και ψεδονυμοποίησης [25], [28], [5]. Θα πρέπει να είναι σε θέση να αναγνωρίζουν πότε θα πρέπει να διεξάγεται εκτίμηση του αντικτύπου που επιφέρει τυχόν διαρροή των πληροφοριών και παραβίαση της ιδιωτικότητας [10], [33], και να εφαρμόζονται διαρκώς πολιτικές ασφάλειας και περιορισμού πρόσβασης στα δεδομένα σύμφωνα με τις οργανωτικές πρακτικές [4], [25].

Ως παράδειγμα, ένα νοσοκομείο θα πρέπει να πραγματοποιεί ετήσια σεμινάρια υποχρεωτικού χαρακτήρα στους υπαλλήλους του ώστε αυτοί να είναι καταρτισμένοι στη διαχείριση ευαίσθητων ιατρικών δεδομένων και καταρτισμένοι σχετικά με τα νομικά δικαιώματα των ασθενών [21], [42].

5.3.2 Ευαισθητοποίηση Πολιτών

Πέρα από τους φορείς, και οι πολίτες, καθώς αποτελούν τα υποκείμενα των δεδομένων, θα πρέπει να είναι σχετικά ενήμεροι και ευαισθητοποιημένοι [38]. Θα πρέπει να γνωρίζουν τα δικαιώματά τους ως προς την πρόσβαση, τη διόρθωση και τη διαγραφή των δεδομένων [57], [55], να κατανοούν έννοιες όπως ο επαναπροσδιορισμός της ταυτότητας ή η επαναταυτοποίηση [2], [28] και τους λόγους για τους οποίους η δημοσιοποίηση των δεδομένων τους, η οποία πολλές φορές πραγματοποιείται και από τους ίδιους ακριβώς λόγω της έλλειψης σχετικής παιδείας, μπορεί να καταστεί επικίνδυνη [39], [26], αλλά και να ενημερώνονται σχετικά με τους κινδύνους της υπερβολικής διαφάνειας, αν μας επιτρέπεται ο όρος, και τον τρόπο με τον οποίο μπορεί να οδηγήσει από το ιδανικό της ενημέρωσης στο άκρο του περιορισμού και της περιθωριοποίησης

[47], [17]. Θα πρέπει επίσης να ενημερωθούν σχετικά με τη χρήση εργαλείων αυτοπροστασίας όπως ο έλεγχος των cookies [43], [49].

Έστω ότι ένας δημόσιος φορέας δημιουργεί μία διαδικτυακή πλατφόρμα ενημέρωσης, που θα επιτρέπει στους πολίτες να ενημερωθούν σχετικά με τους τρόπους προστασίας των προσωπικών τους δεδομένων κατά τη χρήση διαδικτυακών υπηρεσιών. Ταυτόχρονα με τον αρχικό σκοπό της ευαισθητοποίησης των πολιτών και την προστασία της ιδιωτικότητας, θα ήταν ίσως ένας τρόπος να αυξηθεί και η εμπιστοσύνη στους φορείς όταν δεν υφίσταται η υπόνοια ότι υπάρχει υπέρ το δέον έλεγχος και παρεμβατισμός [23], [24];

5.4 Προτάσεις για την Επίτευξη Ισορροπίας μεταξύ Διαφάνειας και Ιδιωτικότητας

Εν όψει της διαρκώς αυξανόμενης απαίτησης για διαφάνεια στη δημόσια διοίκηση παρατηρείται η τάση για ανάγκη πρόσβασης σε ανοιχτά δεδομένα που την αφορούν. Αυτά από τη φύση τους απειλούν την έννοια της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων στην καθαρή τους μορφή [2], [7], [16], [21]. Υπάρχει προφανώς σύγκρουση ανάμεσα στα δύο φαινόμενα. Η πρόκληση που καλούμαστε να αντιμετωπίσουμε είναι η επίτευξη ισορροπίας μεταξύ της προστασίας της ιδιωτικότητας των ατόμων και της ανάγκης για διαφάνεια καθώς και την ελεύθερη χρήση των δεδομένων που αποδεδειγμένα μπορεί να συμβάλει στην ανάπτυξη πολλών μορφών, όπως η οικονομία και η τεχνολογική πρόοδος, και ουσιαστικά ανάμεσα στις θεμελιώδεις αξίες της λογοδοσίας και του δικαιώματος στην ιδιωτική ζωή [6], [17], [22], [23].

Για την επιτυχή έκβαση του ζητούμενου προτείνεται ένας συνδυασμός πολιτικών που αφορούν την πολιτική και τη διακυβέρνηση, τεχνολογικές πρακτικές αλλά και τη συμμετοχή των πολιτών στα κοινά και τη συνεπακόλουθη διαβούλευση [1], [25], [33]. Ο συνδυασμός πολιτικών, τεχνολογικών λύσεων και συμμετοχικών διαδικασιών συνεπάγεται την επίτευξη διαφάνειας σε αρμονία με την ιδιωτικότητα χωρίς να αποκλείει η μια έννοια την άλλη.

5.4.1 Προτάσεις Πολιτικής και Διακυβέρνησης

Καθώς υφίστανται διακρίσεις μεταξύ των δεδομένων ως προς την ευαισθησία τους, προτείνεται η κατηγοριοποίησή τους κατά επίπεδο κινδύνου. Τα Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης λοιπόν μπορούν να διαχωριστούν στο σύνολό τους βάσει αυτού.

Υπάρχουν δεδομένα χαμηλού κινδύνου, μεταξύ των οποίων βρίσκονται τα στατιστικά και συγκεντρωτικά στοιχεία. Στην ουσία πρόκειται για δεδομένα που δεν επιτρέπουν την ταυτοποίηση ατόμων, ακόμα και σε περιπτώσεις διασταύρωσης με άλλες πηγές. Ως παράδειγμα, εάν το Υπουργείο Παιδείας δημοσιεύσει δεδομένα που αφορούν στατιστικά στοιχεία εγγραφών σε σχολεία κατά περιφέρεια και φύλο χωρίς όμως πληροφορίες σχετικές με άτομα ή μικρές γεωγραφικές περιοχές, δεν μπορούν αυτά τα δεδομένα να συνδυαστούν με άλλα με τρόπο τέτοιο που να οδηγήσει σε ταυτοποιήσεις φυσικών προσώπων.

Ως δεδομένα μέτριου κινδύνου ορίζονται αυτά που είναι για παράδειγμα ψευδονυμοποιημένα. Ακόμα χαρακτηρίζονται ως προσωπικά και υπόκεινται στις διατάξεις του GDPR. Δεν περιλαμβάνουν ονόματα, αλλά ενδέχεται να οδηγήσουν σε επαναταυτοποίηση φυσικών προσώπων υπό ορισμένες συνθήκες, ειδικά αν διασταυρωθούν με εξωτερικές πηγές

δεδομένων. Εφόσον ένας δήμος επιλέγει να δημοσιεύσει ψευδονυμοποιημένα δεδομένα που αφορούν αιτήσεις κοινωνικής στήριξης, και μάλιστα στη βάση εμφανίζονται φύλο, ηλικιακή ομάδα, ταχυδρομικός κώδικας και χρονικό διάστημα που λαμβάνεται η κοινωνική παροχή, σε περίπτωση που αφορούν μικρή περιοχή θα μπορούσε να γίνει επαναταυτοποίηση μέσω διαστάυρωσης με άλλα δημόσια δεδομένα.

Υψηλός είναι ο κίνδυνος για την ιδιωτικότητα όταν μπορεί να επέλθει προσδιορισμός γεωγραφίας ή προσωπικών χαρακτηριστικών. Εδώ τα δεδομένα μπορούν εύκολα να οδηγήσουν σε ταυτοποίηση φυσικού προσώπου ακόμα κι αν δεν δίνεται όνομα. Συχνά αυτός ο τύπος δεδομένων περιλαμβάνει ευαίσθητες κατηγορίες δεδομένων και ατόμων με ακριβή χωρικά και χρονικά σημεία. Έστω ότι δημοσιεύεται από φορέα σύνολο Ανοιχτών δεδομένων με συντεταγμένες κατοικιών όπου διαμένουν άτομα που ωφελούνται από κοινωνικά προγράμματα. Αν περιγράφεται ταυτόχρονα και το είδος της παρεχόμενης βοήθειας (ψυχολογική υποστήριξη, επίδομα αναπηρίας) καθώς και η ημερομηνία των παρεχόμενων υπηρεσιών, μπορεί να μην έχουμε όνομα αλλά έχουμε όλα τα απαραίτητα δεδομένα για να προχωρήσουμε σε ταυτοποίηση ατόμων ειδικά σε περιορισμένες γεωγραφικά και πληθυσμιακά κοινότητες.

Πέρα από την κατηγοριοποίηση των δεδομένων με βάση το επίπεδο κινδύνου, προτείνεται και η υποχρεωτική εκτίμηση του αντικτύπου της παραβίασης της ιδιωτικότητας [5], [10], [33], [50]. Τα σύνολα Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης που περιέχουν ή ενδέχεται να περιέχουν προσωπικά δεδομένα πρέπει υποχρεωτικά να απαιτούν την εκ των προτέρων εκτίμηση. Η σημασία της συγκεκριμένης πολιτικής μπορεί να γίνει κατανοητή μέσω παραδείγματος όπου ένα ερευνητικό ινστιτούτο προτίθεται να δημοσιεύσει σύνολο δεδομένων που είναι αποτέλεσμα έρευνας για την ψυχική υγεία των φοιτητών που φοιτούν σε ελληνικά πανεπιστήμια. Εφόσον τα δεδομένα περιλαμβάνουν στοιχεία σχετικά με το τμήμα φοίτησης, το φύλο και την ηλικιακή ομάδα, τη συχνότητα των συμπτωμάτων και το αν ζητήθηκε βοήθεια εντός ή εκτός ιδρύματος, ακόμα κι αν η ταυτότητα των συμμετεχόντων έχει ψευδονυμοποιηθεί, το ινστιτούτο εκπονεί εκτίμηση κινδύνου για το αν κάποιοι συνδυασμοί(π.χ. τμήμα και φύλο και ηλικία) μπορούν να οδηγήσουν σε ταυτοποίηση υποκειμένου, ειδικά σε μικρά τμήματα. Εφόσον τα δεδομένα δύνανται να αποκαλύψουν ευαίσθητες πληροφορίες. Αναζητούνται περεταίρω τεχνικά μέτρα μπορούν να μειώσουν τον κίνδυνο (π.χ. γεωγραφική γενίκευση, περιφέρεια αντί για δήμος). Ελλείψει εκτίμησης κινδύνου μπορεί να παραβιαστεί η ιδιωτικότητα των φοιτητών, ενώ με την τεχνική αυτή μπορούμε να έχουμε την απόφαση να ομαδοποιηθούν τα τμήματα σε σχολές και να αφαιρεθούν τα έτη εισαγωγής, δυσχεραίνοντας έτσι κατά μεγάλο βαθμό την επαναταυτοποίηση.

Τέλος, θεωρείται σκόπιμη η δημιουργία ανεξάρτητων επιτροπών ελέγχου Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης [1], [6], [17], [19]. Θα μπορούν να υφίστανται φορείς που να συνδυάζουν νομική, τεχνική και ηθική κατάρτιση που θα αξιολογούν κατά πόσο η κάθε δημοσίευση δύναται να παραβιάσει τις αρχές της ιδιωτικότητας. Αν λοιπόν υποθέσουμε ότι το Υπουργείο Υγείας σκοπεύει τη δημοσίευση RTLD σχετικά με επισκέψεις πολιτών σε δομές πρωτοβάθμιας φροντίδας υγείας, συμπεριλαμβανομένων δεδομένων που αφορούν ημερομηνίες επίσκεψης, κατηγορία νοσημάτων μαζί με ηλικία και φύλο ασθενών και ταχυδρομικό κώδικα όπου βρίσκεται η εκάστοτε μονάδα, το Υπουργείο δημιουργεί ανεξάρτητη επιτροπή που περιλαμβάνει νομικό εμπειρογνώμονα σε θέματα προστασίας προσωπικών δεδομένων, ειδικό σε τεχνικά θέματα RTLD και εκπρόσωπο από επιτροπή βιοηθικής. Η ομάδα αυτή επωμίζεται την εξέταση των δεδομένων ως προς το περιεχόμενο και την συμπερίληψη ευαίσθητων πληροφοριών

οι οποίες σε συνδυασμό με τον ταχυδρομικό κώδικα και τη σπανιότητα του νοσήματος επιτρέπουν την άμεση ταυτοποίηση. Στη συνέχεια προχωρά σε αξιολόγηση των ηθικών επιπτώσεων από τη δημοσιοποίηση των δεδομένων, όπως το στιγματισμό που μπορούν να προκαλέσουν επισκέψεις σε ψυχιατρική κλινική, και προτείνει τεχνικές λύσεις όπως πρόσθετη ανωνυμοποίηση (αφαίρεση ημερομηνιών, συγχώνευση γεωγραφικών περιοχών). Στο τέλος εκδίδονται δεδομένα με αυξημένα μέτρα προστασίας της ιδιωτικότητας προστατεύοντας έτσι και τα υποκείμενα των δεδομένων και ταυτόχρονα το Υπουργείο συμμορφώνεται με το νομικό πλαίσιο αλλά και με τις αρχές της ηθικής και της υπευθυνότητας.

5.4.2 Προτάσεις Τεχνολογικού Χαρακτήρα

Οι προτάσεις παραπάνω που αφορούν το νομικό και οργανωτικό πλαίσιο της προστασίας των προσωπικών δεδομένων όταν αυτά εμφανίζονται σε σύνολα ανοιχτών δεδομένων θα πρέπει να συνδυάζονται με τις ανάλογες κινήσεις τεχνολογικού χαρακτήρα [5], [10], [25], [33]. Εδώ αναφέρονται τρεις προτάσεις με τα σχετικά παραδείγματα.

Προτείνεται αρχικά η δημιουργία ιδιωτικώς φιλικών φορμάτ δεδομένων. Σχεδιάζονται σύνολα δεδομένων που έχουν ενσωματωμένους κανόνες πρόσβασης, ανωνυμοποίησης ή και ελέγχου διασύνδεσης [2], [27], [43], [51]. Πρακτικά, έστω ότι ένας δημόσιος οργανισμός πολιτισμού αποφασίζει να δημοσιεύσει Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης με πληροφορίες σχετικές με την επισκεψιμότητα μουσείων. Τα δεδομένα δεν θα περιλαμβάνουν ονόματα, αλλά θα μπορούσε να προκύψει ταυτοποίηση ατόμων μέσω της διασταύρωσης των δεδομένων που αφορούν ημερομηνία, τοποθεσία και εισιτήριο. Αντί λοιπόν να δημοσιευτούν τα δεδομένα σε αυτή την αρχικά μορφή, υφίσταται μία πρώτη επεξεργασία όπου στρογγυλοποιείται ο προσδιορισμός του χρόνου επίσκεψης (μήνας, όχι ακριβής ημερομηνία), ενώ ταυτόχρονα ενσωματώνονται κανόνες πρόσβασης σε αυτά (μόνο σε χρήστες με ακαδημαϊκό email επιτρέπεται η πλήρης πρόσβαση). Αυτά σε συνδυασμό με κατηγοριοποίηση του κινδύνου με βάση το αν περιλαμβάνονται προσωπικά ή συμπεριφορικά μοτίβα καθιστούν την τεχνολογία αυτή τεχνικά σωστή και κανονιστικά υπεύθυνη [25], [54].

Έπειτα συναντάμε την περίπτωση της ελεγχόμενης διαλειτουργικότητας. Εδώ, οι βάσεις δεδομένων διασυνδέονται μόνο με εγκεκριμένες πηγές και υπηρεσίες που πληρούν έστω τα ελάχιστα πρότυπα προστασίας [3], [14], [15], [56]. Αν θέλαμε να δημοσιεύσουμε δεδομένα που παρέχει ένα περιφερειακό νοσοκομείο και συγκεκριμένα τα δεδομένα του για την πληρότητα των κλινών και τους μέσους χρόνους αναμονής, ένα σύνολο που ουσιαστικά μπορεί να συνδεθεί με τα δεδομένα του ΕΟΔΥ, και προκειμένου να είναι υφίσταται έλεγχος της διαλειτουργικότητας θα επιτρέπεται η σύνδεση μόνο με κατοχυρωμένες πηγές οι οποίες και θα πληρούν τα υφιστάμενα τεχνικά και νομικά πρότυπα, όπως επίσης θα παρέχονται μεταδεδομένα σε μορφή όπου θα δηλώνεται ότι δεν συνίσταται η συσχέτιση με γεωγραφικά σύνολα δεδομένων σε επίπεδο κάτω του νομού, αυξάνοντας έτσι τα πληθυσμιακά μεγέθη και μειώνοντας τον κίνδυνο ταυτοποίησης, ενώ θα χρησιμοποιούνται και πρότυπα πιστοποίησης [27], [30], [33]. Με τον τρόπο αυτό μειώνεται ο κίνδυνος επαναταυτοποίησης των νοσηλευόμενων από ανεξέλεγκτες διασυνδέσεις.

Τελευταία εκ των προτάσεων τεχνολογικού χαρακτήρα είναι η χρήση της τεχνητής νοημοσύνης για τη δημιουργία αυτοματοποιημένων μηχανισμών πρόβλεψης κινδύνου [28], [39], [43], [48]. Εδώ, εργαλεία τεχνητής νοημοσύνης θα μπορούν να εκτιμούν αν ένα νέο σύνολο

δεδομένων μπορεί να οδηγήσει σε επαναταυτοποίηση υποκειμένων. Τα σύνολα δεδομένων θα μπορούν να αναλύονται πριν δημοσιευτούν, θα ανιχνεύονται ευκολότερα δυνητικά επικίνδυνοι συνδυασμοί όπως μοναδικές ηλικιακές τιμές και σπάνια επαγγέλματα, ενώ ταυτόχρονα θα προβλέπεται και το ποσοστό της πιθανής επαναταυτοποίησης με βάση γνωστές δημόσιες πηγές όπως τα κοινωνικά δίκτυα. Ένα τέτοι εργαλείο θα μπορούσε επίσης να προτείνει κατάλληλες τροποποιήσεις στα σύνολα των δεδομένων πριν από τη δημοσίευσή τους στο κοινό, παρέχοντας έτσι προληπτική άμυνα που θα βασίζεται στα μεγάλα δεδομένα και την αναγνώριση μοτίβων [41], [43], [47].

5.4.3 Συμμετοχή Πολιτών και Διαβούλευση

Πέραν της τεχνικής και νομικής διάστασης της προστασίας των προσωπικών δεδομένων, δεν θα πρέπει να ξεχνάμε ότι το δικαίωμα στην ιδιωτικότητα είναι και δημοκρατικό ζήτημα. Για την ακρίβεια, η δημοκρατία είναι και το σημείο αφετηρίας των δικαιωμάτων των υποκειμένων. Κατά συνέπεια, η ενεργή συμμετοχή των πολιτών στις αποφάσεις που αφορούν την προστασία της ιδιωτικότητας θα νομιμοποιήσει τη διαχείριση των δεδομένων τους και θα μειώσει τον κίνδυνο κατάχρησής τους [7], [20], [24], [36]. Η σημασία της συμμετοχής των πολιτών έγκειται στο γεγονός ότι οι ίδιοι γνωρίζουν πολύ καλύτερα το τί ακριβώς θεωρούν προσωπικό, ευαίσθητο ή πιθανώς επιβλαβές να δημοσιευτεί, ενώ από την πλευρά τους οι φορείς αποκτούν την κοινωνική συναίνεση για τυχόν αμφιλεγόμενα σύνολα δεδομένων, ενισχύοντας ταυτόχρονα την εμπιστοσύνη στις ψηφιακές πολιτικές της πολιτείας και των θεσμών [7], [24], [31]. Αν λοιπόν η συγκατάθεση δεν είναι γενική και αόριστη, καθιστώντας το υποκείμενο των δεδομένων μπερδεμένο σε σχέση με τον τρόπο συλλογής, επεξεργασίας και δημοσίευσης των δεδομένων του, αλλά προωθηθεί ένα μοντέλο συγκατάθεσης βάσει σκοπού, όπου ο πολίτης θα ενημερώνεται σχετικά με τον συγκεκριμένο σκοπό επεξεργασίας ή δημοσίευσης των δεδομένων του, το ποιος θα έχει πρόσβαση σε αυτά και για πόσο χρονικό διάστημα, και φυσικά το είδος των δεδομένων που υπόκεινται σε δημοσιοποίηση και το επίπεδο ανωνυμοποίησης αυτών, η συγκατάθεση είναι πλέον στοχευμένη, περιορισμένη και ανακλητή ανά πάσα στιγμή το θελήσει το υποκείμενο, έχουμε πλέον την ουσιαστική συμμετοχή του στο σχεδιασμό της πολιτικής διαφάνειας [5], [20], [36], [53]. Στη συνέχεια παρατίθενται παραδείγματα εφαρμογής της συμμετοχής των πολιτών σε επίπεδο τοπικής αυτοδιοίκησης, εθνικό αλλά και στα πλαίσια πανεπιστημιακής έρευνας.

Στο περιβάλλον της τοπικής αυτοδιοίκησης, προκειμένου ένας δήμος να έχει αφενός τη συναίνεση της κοινότητας, αφετέρου να επιτύχει τη ζητούμενη διαφάνεια μέσω της συμμετοχικής διαδικασίας, μπορεί αν για παράδειγμα σκοπεύει να δημοσιεύσει ως Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης στατιστικά στοιχεία για τις κοινωνικές υπηρεσίες που λαμβάνουν οι δημότες ανά περιοχή και ηλικιακή ομάδα., να προβεί σε ορισμένες ενέργειες σχετικά. Αρχικά, οργανώνει διαβούλευση με δημότες αλλά και λοιπούς φορείς όπως συλλόγους αναπήρων και ΜΚΟ για να ενημερώσει σχετικά με τη δημοσιοποίηση. Μπορεί τοιουτοτρόπως να λάβει ενημέρωση και σχόλια σχετικά με το ποια δεδομένα θεωρούνται ευαίσθητα από τα ίδια τα υποκείμενά τους, και συνεπώς να προχωρήσει σε τροποποίηση του συνόλου των δεδομένων της βάσης πριν από τη δημοσιοποίησή της, αφαιρώντας εντελώς ορισμένα δεδομένα ή γενικεύοντας συγκεκριμένα πεδία [7], [20], [36].

Σε εθνικό επίπεδο, εφόσον το κράτος επιθυμεί τη δημιουργία εθνικής πλατφόρμας ανοιχτών δεδομένων ώστε να δώσει πρόσβαση σε αυτά προκειμένου να διευκολύνονται οι

διαδρομές των χρηστών στις κρατικές ιστοσελίδες. Όταν υφίσταται διαφανής συγκατάθεση, δηλαδή όταν ο χρήστης ενημερώνεται σχετικά με τη διάθεση συγκεκριμένων και ανώνυμων δεδομένων πλοήγησης τα οποία δύνανται να διατεθούν για στατιστική ανάλυση, και ότι η εν λόγω συγκατάθεση αφορά το συγκεκριμένο και μόνο σκοπό και επίσης μπορεί να ανακληθεί ανά πάσα στιγμή, αφενός ο χρήστης διατηρεί τον έλεγχο των δεδομένων του, αφετέρου το κράτος δεν προχωρά σε κρυφή ή αόριστη συλλογή των δεδομένων. Και πάλι προωθείται η διαφάνεια και η εμπιστοσύνη [6], [20], [53].

Τέλος, όταν τα δεδομένα συγκεντρώνονται προς επεξεργασία για ακαδημαϊκούς σκοπούς, όπως στην περίπτωση που έχουμε ήδη χρησιμοποιήσει προηγουμένως ως παράδειγμα, όπου ένα πανεπιστήμιο συλλέγει δεδομένα σχετικά με τη χρήση ψυχολογικής υποστήριξης που τυχόν λαμβάνουν φοιτητές, και επιθυμεί να δημοσιεύσει τα δεδομένα ως Συνδεδεμένα και Ανοιχτά, οι φοιτητές παρέχουν τα δεδομένα τους μόνο ως στατιστικά στοιχεία και συγκατατίθενται μόνο ως προς αυτό με καθορισμένο σκοπό την ακαδημαϊκή έρευνα. Στη φόρμα συγκατάθεσης θα πρέπει να αναφέρεται ότι τα συγκεκριμένα δεδομένα δημοσιεύονται μόνο εάν δεν δύναται η επαναταυτοποίηση των υποκειμένων και θα αφαιρεθούν τα πεδία που αφορούν μικρές πληθυσμιακές ομάδες. Με τον τρόπο αυτό, η χρήση των δεδομένων καθίσταται δεοντολογικά κατοχυρωμένη και ταυτόχρονα διασφαλίζεται η προστασία των φοιτητών [24], [53].

Συμπερασματικά, η διαχείριση των προσωπικών δεδομένων σε περιβάλλοντα RTLD έχει ανάγκη την πολυδιάστατη και ισορροπημένη προσέγγιση όπου η τεχνολογία, η πολιτική και η κοινωνική συγκατάθεση και συνείδηση συνδυάζονται. Οι προτάσεις και οι πρακτικές που έχουν αναφερθεί εδώ στοχεύουν στη θωράκιση της ιδιωτικότητας των υποκειμένων των δεδομένων, τη συμμόρφωση με τα νομικά πλαίσια που τη διέπουν σε εθνικό και ευρωπαϊκό επίπεδο και τη διατήρηση των αξιών της διαφάνειας και της ανοικτής πρόσβασης. Με τη χρήση και αξιοποίηση ενός εύρους πρακτικών που εκτείνεται από την προστασία και τα πρωτόκολλα έως τη θεσμική ενίσχυση με ανεξάρτητους φορείς και τη συμμετοχή των πολιτών, διαμορφώνεται ένα πλαίσιο υπεύθυνης δημοσίευσης που συνδυάζει την καινοτομία, τη νομιμότητα και τη δημοκρατική συμμετοχή. Η ζητούμενη ισορροπία δεν επιτυγχάνεται αυτόματα. Δημιουργείται με συστηματικό σχεδιασμό, αξιολόγηση και διαρκή προσαρμογή στα συνεχώς διαφοροποιούμενα δεδομένα της εποχής. άλλωστε, ο δρόμος για τα ανοιχτά αλλά και δίκαια δεδομένα περνά οπωσδήποτε μέσα από την ενσυνείδητη προστασία του ατόμου [24], [36].

6 *Μελέτες Περιπτώσεων Ευρωπαϊκών Χωρών*

Τα όσα αναλύθηκαν στα προηγούμενα κεφάλαια καταδεικνύουν τις προκλήσεις, τα νομικά όρια και τις τεχνικές δυνατότητες που υφίστανται κατά τη διαχείριση των προσωπικών δεδομένων στο πλαίσιο των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης [7]. Για την επίτευξη όμως πλήρους κατανόησης των ζητημάτων που εγείρονται κατά την εφαρμογή της προαναφερθείσας θεωρίας των αρχών προστασίας της ιδιωτικότητας, κρίνεται σκόπιμη η ανάλυση πραγματικών περιπτώσεων από χώρες της Ευρωπαϊκής Ένωσης, όπου και εφαρμόζεται ο Κανονισμός GDPR.

Στο παρόν κεφάλαιο λοιπόν αναφέρονται τέσσερις μελέτες περίπτωσης από χώρες της ΕΕ όπου έχουν αναπτυχθεί προχωρημένες πολιτικές ανοιχτών δεδομένων, και συγκεκριμένα το Ηνωμένο Βασίλειο, την Εσθονία, τη Φινλανδία και την Ολλανδία. Η επιλογή των χωρών αυτών έγινε βάσει της ποικιλομορφίας των προσεγγίσεων που εφαρμόζουν και της διαφοράς στη στάθμιση μεταξύ ιδιωτικότητας και διαφάνειας, καθώς και τη διαθεσιμότητα δημόσιων και αξιολογήσιμων στοιχείων σχετικά με τις πρακτικές τους.

Αναλύονται τρία βασικά πεδία. Αυτά αφορούν το είδος και τη χρήση των δημοσιευμένων δεδομένων, τα μέτρα προστασίας των προσωπικών δεδομένων που εφαρμόζονται κατά περίπτωση και πώς έχει επηρεαστεί το επίπεδο εμπιστοσύνης των πολιτών και η αποδοχή των πρακτικών από αυτούς.

Η μελέτη των περιπτώσεων αποσκοπεί στην ανάδειξη καλών πρακτικών, ενώ σημειώνει κενά και αδυναμίες που εξακολουθούν να υπάρχουν και χρήζουν διόρθωσης. Στόχος είναι η εξαγωγή συμπερασμάτων και προτάσεων πολιτικής και υλοποίησης ενός μοντέλου δημοσίευσης των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης που θα σέβεται την ιδιωτικότητα χωρίς να υποβαθμίζει τη διαφάνεια [22].

6.1 Η Περίπτωση του Ηνωμένου Βασιλείου και η Πλατφόρμα police.uk

Ξεκινώντας με την περίπτωση του Ηνωμένου Βασιλείου, έχουμε τη βρετανική κυβέρνηση η οποία μέσω της πρωτοβουλίας data.gov.uk επέλεξε την εισαγωγή εκτεταμένων δράσεων διαφάνειας και επέτρεψε την ελεύθερη πρόσβαση σε μεγάλο όγκο ανοιχτών δεδομένων [3], [7], [22]. Εδώ θα αναφερθούμε στην πλατφόρμα police.uk, όπου και παρέχονται αναλυτικά δεδομένα εγκληματικότητας διαθέσιμα ανά περιοχή, τύπο εγκλήματος και χρονική περίοδο τέλεσης [7]. Τα δεδομένα συνοδεύονται από χάρτες, στατιστικά και API ενώ παράλληλα χρησιμοποιούνται και τεχνικές προστασίας προσωπικών δεδομένων όπως η γεωγραφική ασάφεια, όπου για παράδειγμα μία αναφορά εγκλήματος συγκεντρώνει τουλάχιστον οχτώ διαφορετικές διευθύνσεις, με αποτέλεσμα να μην μπορεί να εντοπιστεί με ακρίβεια το σημείο του συμβάντος [12]. Με τη συγκεκριμένη πρωτοβουλία επιδιώκεται να ενισχυθεί η κοινωνική εμπιστοσύνη στους θεσμούς, η ανάπτυξη της συμμετοχής των πολιτών στα κοινά καθώς και η δημιουργία εφαρμογών τρίτων φορέων που αξιοποιούν τα δημοσιευμένα δεδομένα για την πληροφόρηση των πολιτών [4], [7].

6.1.1 Αξιολόγηση Πολιτικής Προστασίας Δεδομένων

Οι αρχές στις οποίες στηρίζεται η πολιτική ανοιχτών δεδομένων του Ηνωμένου Βασιλείου, είναι η Transparency by design, όπου ενσωματώνεται η διαφάνεια στις βασικές λειτουργίες της κυβέρνησης [2], η Privacy by design, που όπως έχει ήδη πολλές φορές αναφερθεί αφορά το σχεδιασμό των πληροφοριακών συστημάτων με ενσωματωμένη την προστασία των προσωπικών δεδομένων, χρησιμοποιώντας τεχνικές όπως η ανωνυμοποίηση των δεδομένων και περιορισμούς γεωγραφικής ακρίβειας, όπως και έλεγχος πρόσβασης [12], [15]. Τέλος, έχουμε το Open Government Licence βάσει του οποίου κατοχυρώνεται νομικά η ελεύθερη και μη περιορισμένη χρήση των δεδομένων [7].

Αν και στην περίπτωση του Ηνωμένου Βασιλείου τα δεδομένα είναι ανωνυμοποιημένα, έχει σημειωθεί ότι η ίδια η ύπαρξη των διασυνδεδεμένων δεδομένων υπό τη μορφή BORTLD (Big, Open, Linked Data) μπορεί να οδηγήσει σε περιπτώσεις όπου η διασταύρωση διαφορετικών πηγών μπορεί να οδηγήσει σε επαναταυτοποίηση υποκειμένων ή και κατάχρηση σε επίπεδο παρακολούθησης [9], [15], αυξάνοντας τον κίνδυνο που πρέπει να αντιμετωπιστεί με κατάλληλα τεχνικά και οργανωτικά μέσα.

Για την καλύτερη προστασία των προσωπικών δεδομένων και της ιδιωτικότητας, και κατά συνέπεια την επίτευξη ισορροπίας ανάμεσα στη διαφάνεια και τις έννοιες αυτές, συνίσταται η ύπαρξη ανεξάρτητων μηχανισμών ελέγχου όπως αυτοί έχουν παρουσιαστεί στην προηγούμενη ενότητα 5.4 [16], ο διαχωρισμός των ρόλων καθώς και θεσμικές δικλείδες ασφαλείας. Συγκεκριμένα, θα ήταν χρήσιμη η αναβάθμιση των τεχνικών ανωνυμοποίησης του ήδη χρησιμοποιούνται με πιο δυναμικά μοντέλα ανάλογα με τον πληθυσμό της εκάστοτε περιοχής που αναφέρονται τα δεδομένα, όπως και η συμπερίληψη των πολιτών σε διαβουλεύσεις που αφορούν τη δημοσιοποίηση, χρήση και επεξεργασία των δεδομένων τους [4], [9].

6.1.2 Συμπεράσματα της Περίπτωσης του Ηνωμένου Βασιλείου

Μέσω της μελέτης της πλατφόρμας police.uk αλλά και της γενικότερης εικόνας που αφορά την πολιτική διαφάνεια στην περίπτωση του Ηνωμένου Βασιλείου, μπορούμε να προβούμε σε

ορισμένα συμπεράσματα. Αρχικά θα πρέπει να αναφέρουμε πως η διάθεση των δεδομένων ως Συνδεδεμένα και Ανοιχτά ενισχύει τη διαφάνεια των φορέων και ως αποτέλεσμα έχουμε την ενίσχυση της εμπιστοσύνης των πολιτών προς αυτούς [3], [4]. Επιπροσθέτως, όσο πιο πλήρη και προσβάσιμα είναι τα δεδομένα, τόσο υψηλότερα εμφανίζονται και τα επίπεδα εμπιστοσύνης των πολιτών στους θεσμούς [4]. Βέβαια δεν μπορούμε να μιλάμε για πλήρη διαφάνεια τη στιγμή που ένα από τα ζητούμενα είναι και η προστασία των προσωπικών δεδομένων και η διατήρηση της αρχής της ιδιωτικότητας [2], [15], όπως αυτή έχει εξελιχθεί τη σημερινή εποχή της πληροφορίας και της διασύνδεσης. Παρατηρούμε την ύπαρξη ανάγκης για ισορροπία ανάμεσα στα δύο άκρα [9], και άρα τα συστήματα που διαχειρίζονται την πληροφορία θα πρέπει να περιλαμβάνουν μηχανισμούς ανωνυμοποίησης, ελέγχου διασυνδέσεων και προσβασιμότητας [12], [15]. Τέλος θα πρέπει να δοθεί έμφαση και στην κοινωνική διάσταση του ζητήματος, καθώς η συμμετοχή των πολιτών στις αποφάσεις μπορεί να έχει οφέλη και για τις δύο πλευρές [4], [9], με τους μεν πολίτες να γίνονται μέρος του συστήματος λήψης αποφάσεων ενώ οι θεσμοί αποκτούν την πολυπόθητη νομιμοποίηση. Η αντίληψη περί νομιμότητας και η αίσθηση της λογοδοσίας είναι ζωτικής σημασίας [4] για την ύπαρξη και επιβίωση αυτών των προγραμμάτων.

Η περίπτωση του Ηνωμένου Βασιλείου μας δείχνει ότι για την επιτυχή υλοποίηση προγραμμάτων Συνδεδεμένων και Ανοιχτών Δεδομένων και διαφάνειας απαιτείται εξίσου τεχνική υποδομή, δημοκρατική οργάνωση, εμπιστοσύνη και θεσμική ενσωμάτωση των πολιτικών προστασίας των προσωπικών δεδομένων [3], [7].

6.2 Η Περίπτωση της Εσθονίας και η Αρχιτεκτονική Διακυβέρνησης Δεδομένων

Η Εσθονία αποτελεί μία από τις πρώτες χώρες που προχώρησαν σε ψηφιοποίηση του δημόσιου τομέα [6], [10]. Έχει αναπτυχθεί ενιαίο πλαίσιο διασύνδεσης και διάθεσης ανοιχτών δεδομένων, που πραγματοποιείται μέσω της πλατφόρμας opendata.riik.ee [10].

6.2.1 X-Road

Το X-Road αποτελεί το θεμέλιο λίθο της ψηφιακής αρχιτεκτονικής της Εσθονίας [10]. Πρόκειται για ένα αποκεντρωμένο πρωτόκολλο ανταλλαγής δεδομένων μεταξύ των δημόσιων φορέων, μεταξύ των λειτουργιών του οποίου είναι η διασφάλιση της ασφάλειας, της διαλειτουργικότητας και της διαφάνειας [6], [10].

Οι τομείς που καλύπτονται μέσω των διαθέσιμων Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης αφορούν πληθυσμιακά και δημογραφικά δεδομένα, στατιστικά απασχόλησης, γεωχωρικά δεδομένα και διοικητικά μητρώα [10].

Η προσέγγιση που υιοθετεί η Εσθονία έχει ως βασικό χαρακτηριστικό αυτό της αποκέντρωσης. Αυτό σημαίνει ότι τα δεδομένα που αποθηκεύονται δεν βρίσκονται στο σύνολό τους σε μία και μόνο ενιαία κρατική βάση, αλλά παραμένουν σε επιμέρους βάσεις των αρμόδιων φορέων και διαμοιράζονται μόνο έπειτα από αιτιολογημένη αίτηση πρόσβασης. Οι πολίτες κατέχουν ηλεκτρονική ταυτότητα ώστε να έχουν πρόσβαση σε όλα τα στοιχεία που αφορούν τους ίδιους καθώς επίσης έχουν τον έλεγχο αυτών, δηλαδή είναι σε θέση να γνωρίζουν ποιος φορέας ζήτησε δεδομένα τους, ποια ήταν αυτά τα δεδομένα και πότε ζητήθηκαν.

6.2.2 Αξιολόγηση της Πολιτικής για την Προστασία των Δεδομένων στην Εσθονία

Η πολιτική για την προστασία των δεδομένων στην περίπτωση της Εσθονίας θα μπορούσε κανείς να πει ότι αφορά ένα καλό παράδειγμα προς μίμηση [6], [10]. Σίγουρα όπως και όλα τα συστήματα και οι πολιτικές έχει τα αδύναμα σημεία τους στα οποία θα αναφερθούμε παρακάτω.

Αρχικά βλέπουμε τις τεχνολογίες που χρησιμοποιούνται, με βασικές τις Privacy by architecture [15], [2], με το σχεδιασμό του X-Road να είναι τέτοιος ώστε κανένας φορέας να μην έχει πλήρη εικόνα για έναν πολίτη χωρίς τη συναίνεσή του, Transparency by default, με τα δημόσια δεδομένα να είναι ανοιχτά εκτός περιπτώσεων που συντρέχουν λόγοι προστασίας προσωπικών ή εθνικών συμφερόντων, και τέλος με τις πρακτικές eConsent και eAudit [10]. Εδώ, ο κάθε πολίτης έχει τον πλήρη έλεγχο των ροών των δεδομένων του και υφίσταται πλήρης ιχνηλασιμότητα της κάθε πρόσβασης σε αυτά.

Όλα τα παραπάνω εφαρμόζονται παράλληλα με επιπλέον πρότυπα προστασίας, διαδικασίες DPIA (αξιολόγηση κινδύνου) σε νέες εφαρμογές RTLD [15], ενώ ταυτόχρονα υφίσταται η ανεξάρτητη εποπτεία από την Data Protection Inspectorate της Εσθονίας [10].

Η περίπτωση της Εσθονίας αποτελεί παράδειγμα χώρας που δεν εργαλειοποιεί τα Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης απλά ως μέσο αύξησης της εμπιστοσύνης των πολιτών [4], αλλά έχει προσεγγίσει το ζήτημα από όλες του τις πλευρές ώστε να βρει τη ζητούμενη ισορροπία μεταξύ διαφάνειας και ιδιωτικότητας [9].

Όπως είπαμε ήδη, όμως, κανένα σύστημα δεν λειτουργεί χωρίς μελανά σημεία. Όσον αφορά την Εσθονία, βασικό σημείο που θα πρέπει να ερευνηθεί και να αντιμετωπιστεί είναι η απαίτηση για υψηλό επίπεδο ψηφιακού αλφαβητισμού, γεγονός το οποίο ενδέχεται να αποκλείσει ορισμένες ομάδες του πληθυσμού από την πρόσβαση στα δεδομένα που δημοσιεύονται όπως ευάλωτες κοινωνικές ομάδες και ορισμένα ηλικιακά στρώματα. Υφίσταται λοιπόν απαίτηση να ενισχυθεί η ευαισθητοποίηση των λιγότερο εξοικειωμένων ατόμων με το ψηφιακό περιβάλλον και τις ψηφιακές τεχνολογίες [6]. Το συγκεκριμένο ζήτημα βέβαια αποτελεί κοινωνικό κυρίως θέμα. Σε επίπεδο τεχνολογικό, θα ήταν θεμιτή η διερεύνηση τυχόν αλγοριθμικών κινδύνων στη διασύνδεση των υπηρεσιών ώστε να αποφευχθούν πιθανές παραβιάσεις [15].

6.2.3 Συμπεράσματα της Περίπτωσης

Συμπερασματικά, η περίπτωση της Εσθονίας αποτελεί ένα καλό παράδειγμα, καθώς παρουσιάζει μια ολοκληρωμένη και συνεκτική στρατηγική ως προς τη διαχείριση των Ανοιχτών Δεδομένων με ταυτόχρονο σεβασμό στην ιδιωτικότητα [6], [10]. Η χώρα αυτή έχει καταφέρει την τεχνική και θεσμική ενοποίηση και συνδυάζει την ασφάλεια με τη λειτουργικότητα. Κάθε πολίτης είναι σε θέση να αποκτήσει ενεργό ρόλο όσον αφορά τον έλεγχο των δεδομένων του, και την ίδια στιγμή η αρχή της διαφάνειας εφαρμόζεται στην πράξη [2].

Στον αντίποδα, παραμένει το θέμα της έλλειψης ισότιμης πρόσβασης στις παρεχόμενες υπηρεσίες για όλους τους πολίτες, περιθωριοποιώντας ομάδες του πληθυσμού, ενώ θα πρέπει να υπάρξει και πρόβλεψη σχετικά με πιθανούς μελλοντικούς κινδύνους για την παραβίαση της ιδιωτικότητας από εξελιγμένες μορφές τεχνητής νοημοσύνης [15].

Εν κατακλείδι, το αποτύπωμα της Εσθονίας είναι μάλλον θετικό, αφού έχει επιτευχθεί σε μεγάλο βαθμό η τεχνολογική πρόοδος και η θεσμική καινοτομία, οι οποίες συμβαδίζουν με την

προστασία των θεμελιωδών δικαιωμάτων και άρα έχουμε ισορροπία ανάμεσα στα δύο ζητούμενα [4], [9].

6.3 Η Περίπτωση της Φινλανδίας-Διαφάνεια με Κοινωνική Εμπιστοσύνη

Η πολιτική των Ανοιχτών Δεδομένων πραγματοποιείται στη χώρα της Φινλανδίας μέσω της πλατφόρμας avoindata.fi. Εκεί συγκεντρώνονται δεδομένα από πολυάριθμους κυβερνητικούς φορείς, δήμους αλλά και ανεξάρτητους οργανισμούς. Τα δεδομένα που είναι διαθέσιμα μέσω της εθνικής αυτής πύλης αφορούν στοιχεία για την εκπαίδευση, τον πολιτισμό, την υγεία και πρόνοια, το περιβάλλον και τις μεταφορές. Μέσω αυτής προάγεται η χρήση των δεδομένων από επιχειρήσεις, ερευνητές και πολίτες, και υποστηρίζει μηχανισμούς αναζήτησης, API και metadata, προωθώντας με αυτό τον τρόπο την καινοτομία, την ακαδημαϊκή έρευνα και τη διαφάνεια [28].

Θεσμικά, η λειτουργία της πλατφόρμας βασίζεται στη Συνταγματική Αρχή της Δημοσιότητας, βάσει της οποίας οι πολίτες δικαιούνται την πρόσβαση στα δημόσια έγγραφα και τις δημόσιες πληροφορίες [12].

6.3.1 Αξιολόγηση Πολιτικής Προστασίας Δεδομένων

Ως χώρα της Ευρωπαϊκής Ένωσης, η Φινλανδία υπόκειται στις διατάξεις του GDPR και έχει εναρμονίσει πλήρως το εθνικό της δίκαιο με τον κανονισμό [5]. Με τη σειρά της, η πολιτική ανοιχτών δεδομένων καθορίζεται από σαφείς διαχωρισμούς μεταξύ προσωπικών δεδομένων και μη προσωπικών δεδομένων σε θεωρητικό επίπεδο, ενώ τεχνολογικά χρησιμοποιούνται προτυποποιημένες διαδικασίες ανωνυμοποίησης πριν την εκάστοτε δημοσίευση Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης [16]. Να σημειωθεί και πάλι ότι σύμφωνα με τον κανονισμό GDPR τα ανωνυμοποιημένα δεδομένα δεν θεωρούνται προσωπικά [5]. Σε θεσμικό, τέλος, επίπεδο, υφίσταται η Ανεξάρτητη Αρχή Προστασίας Δεδομένων (Tietosuojavaltuutetun toimisto) η οποία και λειτουργεί ως ανεξάρτητος εποπτικός μηχανισμός για να βεβαιωθεί η συμμόρφωση της δημοσίευσης των δεδομένων με την προστασία τους σύμφωνα με το ισχύον νομικό πλαίσιο [17].

Έχουμε λοιπόν ένα σταθερό θεσμικό πλαίσιο, όπως επίσης και την εμπιστοσύνη των πολιτών σε αυτό. Υφίσταται όμως ανάγκη για εναρμονισμένες πρακτικές ανωνυμοποίησης μεταξύ των εμπλεκόμενων φορέων για την καλύτερη προστασία των προσωπικών δεδομένων και την αποφυγή περιπτώσεων επαναταυτοποίησης μέσω συνδυασμού δεδομένων από διαφορετικές πηγές [15].

Το γεγονός ότι υπάρχουν τα προαναφερθέντα εθνικά πρότυπα σε συνδυασμό με τη χρήση των Ανοιχτών Δεδομένων από τον ιδιωτικό τομέα, προάγει ταυτόχρονα και τη διαλειτουργικότητα. Η πολιτική που ακολουθείται όμως στο σύνολό της προάγει έναν μάλλον τεχνοκρατικό χαρακτήρα, αφού η κοινωνική συμμετοχή διατηρείται στο ελάχιστο, όπως και η διαβούλευση με τους πολίτες τόσο ως προς τη χρήση των προσωπικών τους δεδομένων ως RTLD αλλά και ΄την ηθική διάσταση του θέματος.

6.3.2 Συμπεράσματα Περίπτωσης

Εν κατακλείδι η περίπτωση της Φινλανδίας αντιπροσωπεύει ένα μοντέλο διαχείρισης των Ανοιχτών Δεδομένων όπου η σταθερότητα των θεσμών και το υφιστάμενο πολιτισμικό κεφάλαιο εμπιστοσύνης επιτρέπουν την εκτεταμένη χρήση των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης, και η τεχνική και νομική συμμόρφωση με τον κανονισμό του GDPR είναι πλήρως εναρμονισμένες [5], [28].

Αυτό το οποίο υπολείπεται όμως αφορά την ηθική πλευρά του ζητήματος, με τη συμμετοχή των πολιτών στη διαβούλευση για τα δεδομένα τους σε συνδυασμό με τη γενικότερη έλλειψη θεσμών συμμετοχικότητας να δύναται να προκαλέσει κενά στην προστασία των προσωπικών δεδομένων όταν αυτά αφορούν ευαίσθητους τομείς, όπως για παράδειγμα αυτός της υγείας και της παιδείας [14].

6.4 Η Περίπτωση της Ολλανδίας-Ιδιωτικότητα μέσω Διαμοιρασμένης Ευθύνης

Η Ολλανδία αποτελεί μία από τις χώρες που σημειώνουν ισχυρή παράδοση στο ζήτημα της ανοιχτής διακυβέρνησης, εφαρμόζοντας όμως μια πιο συντηρητική διαχείριση της ιδιωτικότητας σε σχέση με άλλα κράτη, όπως το Ηνωμένο Βασίλειο [28], που εφαρμόζουν πιο επιθετικές πολιτικές Ανοιχτών Δεδομένων. Η Ολλανδία διαθέτει την ψηφιακή πύλη data.overheid.nl, μέσω της οποίας οι κυβερνητικοί οργανισμοί προωθούν τα σύνολα των Ανοιχτών Δεδομένων. Στην περίπτωσή της όμως, η διαλειτουργικότητα που υφίσταται μεταξύ των διάφορων φορολογικών, επιχειρηματικών, κοινωνικών και άλλων μητρώων είναι αυστηρά ελεγχόμενη [18], και όχι αυτόματη ή ελεύθερη. Διέπεται από αρχές όπως αυτή της ελάχιστης αναγκαίας πρόσβασης, όπου κάθε δημόσιος φορέας που επιθυμεί την πρόσβαση σε δεδομένα μπορεί να την έχει μόνο στα απολύτως απαραίτητα τμήματα ενός άλλου μητρώου, και όχι στο σύνολο αυτών, ενώ ισχύει και εδώ η αρχή του σκοπού, δηλαδή η πρόσβαση θα επιτραπεί για ορισμένο και μόνο σκοπό. Έπεται η αρχή της κατανεμημένης ευθύνης, όπου δεν υπάρχει ενιαία και κεντρική βάση που να περιέχει πλήρη προφίλ πολιτών. Κάθε μητρώο διατηρεί τις δικές του πληροφορίες και η πρόσβαση σε αυτές παρέχεται μόνο υπό όρους. Για την ακρίβεια, η Ολλανδία διαθέτει κατανεμημένες βάσεις δεδομένων και για να μπορέσει ένας φορέας να συνθέσει ένα πλήρες προφίλ πολίτη θα πρέπει να υφίσταται διασταυρωμένη εξουσιοδότηση. Τέλος, έχουμε και τις αρχές της ιχνηλασιμότητας και της διαφάνειας. Κάθε περίπτωση ανταλλαγής δεδομένων ανάμεσα σε διαφορετικά μητρώα θα καταγραφεί και στις περισσότερες των περιπτώσεων θα είναι γνωστή και στον ίδιο τον πολίτη τον οποίο θα αφορούν τα διαμοιραζόμενα δεδομένα μέσω του προσωπικού του λογαριασμού [12], [5].

Όσον αφορά τώρα τα προσωπικά δεδομένα, αυτά δεν δημοσιεύονται ούτε καν σε ψευδονυμοποιημένη μορφή χωρίς πρότερη εκτενή νομική αξιολόγηση ως προς την προστασία αυτών.

6.4.1 Αξιολόγηση Πολιτικής Προστασίας Δεδομένων

Ως προς την επίτευξη της προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων στην περίπτωση της Ολλανδίας, πέραν των όσων αναφέρθηκαν παραπάνω ισχύει επίσης και Ανεξάρτητη Αρχή Προστασίας Δεδομένων (Autoriteit Persoonsgegevens), θεσμικός έλεγχος της

διασύνδεσης των συστημάτων με σκοπό την αποφυγή της υπέρ το δέον συγκέντρωσης πληροφορίας και της συνεπακόλουθης εξουσίας, ενώ σε τεχνολογικό επίπεδο παρατηρούμε την ύπαρξη privacy by default [17], δηλαδή την ύπαρξη πρόβλεψης για την προστασία των δεδομένων μέσα στην αρχιτεκτονική των πληροφοριακών συστημάτων που σχεδιάζονται για τη διαχείριση των ανοιχτών δεδομένων.

Ο τρόπος με τον οποίο η Ολλανδία επιλέγει να αντιμετωπίσει το ζήτημα δίνει βάση στο να αποτραπεί η κατάχρηση της εξουσίας μέσω της συγκέντρωσης πληροφορίας. Όντως τα προσωπικά δεδομένα και τα υποκείμενά τους είναι πολύ καλά προστατευμένα, αλλά στον αντίποδα έχουμε καθυστέρηση της επαναχρησιμοποίησης της πληροφορίας λόγω της ύπαρξης πολλών ρυθμίσεων, κάτι το οποίο δύναται να περιορίσει κατά πολύ την πρόοδο και την αποτελεσματικότητα της καινοτομίας [15], ειδικά όταν οι αιτούντες την πρόσβαση είναι μικροί φορείς και ερευνητικά έργα.

6.4.2 Θεωρητικά Οφέλη της Ελεγχόμενης Διαλειτουργικότητας

Συμπληρωματικά σε όσα αναφέρθηκαν παραπάνω, η ύπαρξη της ελεγχόμενης διαλειτουργικότητας που συναντάμε στην περίπτωση της Ολλανδίας είναι ένας πολύ ισχυρός παράγοντας προστασίας των προσωπικών δεδομένων. Η αποκέντρωση βάση της οποίας δομούνται οι βάσεις δεδομένων των φορέων μειώνουν σημαντικά τον ενδεχόμενο κίνδυνο παρακολούθησης των πολιτών ή της αυθαίρετης κατηγοριοποίησής τους. Περιορίζονται κατά αυτό τον τρόπο οι καταχρήσεις πληροφορίας, καθώς κανένας φορέας δεν δύναται να δημιουργήσει φακέλους με προφίλ πολιτών χωρίς να υφίσταται θεσμικός έλεγχος. Υπάρχει επίσης και κεντρικός έλεγχος για την κατάχρηση εξουσίας, με την αρχή προστασίας δεδομένων της χώρας να έχει την εποπτεία όλων των μορφών σύνδεσης μητρώων [16], [17].

6.4.3 Συμπεράσματα της Περίπτωσης

Συνολικά η περίπτωση της Ολλανδίας είναι ένα παράδειγμα θεσμικά ώριμης προστασίας δεδομένων, με την ιδιωτικότητα να θεωρείται δικαίωμα ελέγχου και διαμοιρασμού της πληροφορίας [12], [28], με τους κρατικούς μηχανισμούς να λειτουργούν από θέση άμυνας απέναντι στην διαφάνεια, υστερώντας όμως ως προς αυτή σε σχέση με τα ευρωπαϊκά πρότυπα. Ταυτόχρονα, η πολύπλοκη φύση των ρυθμίσεων που υφίστανται για την πρόσβαση σε ανοιχτά δεδομένα καθιστά δύσκολη την ανάλυσή τους και την πρόοδο της καινοτομίας, ειδικά σε περιπτώσεις που ο αιτών την πρόσβαση είναι μικρός σε μέγεθος φορέας. Θεωρητικά, ο προσανατολισμός της Ολλανδίας στην προστασία των θεμελιωδών δικαιωμάτων προστατεύει του πολίτες στην, πρακτικά όμως δύναται να περιορίσει την ευκολία και την ταχύτητα με την οποία αυτοί εξυπηρετούνται [14].

6.5 Η Περίπτωση της Ελλάδας-Διαύγεια

Αναφορικά με την περίπτωση της Ελλάδας, παρουσιάζουμε την πλατφόρμα «Διαύγεια». Πρόκειται για ένα πρωτοποριακό εγχείρημα προώθησης της διαφάνειας, μέσα από το οποίο αναρτώνται δημόσια όλες οι διοικητικές και οικονομικές πράξεις των δημόσιων φορέων της χώρας [41]. Στόχος είναι η επίτευξη της λογοδοσίας και συγχρόνως η καλλιέργεια της εμπιστοσύνης των πολιτών προς τους θεσμούς [42]. Η χρήση της όμως εγείρει σοβαρά ερωτήματα

όσον αφορά την ιδιωτικότητα των ατόμων που βρίσκονται να αναφέρονται μέσα στην πλατφόρμα και ειδικά σε περιπτώσεις που περιλαμβάνονται στα δεδομένα που δημοσιεύονται και προσωπικά [43].

6.5.1 Νομικό και Τεχνολογικό Υπόβαθρο

Όπως έχει αναφερθεί σε προηγούμενο κεφάλαιο, η Ελλάδα ως μέλος της Ευρωπαϊκής Ένωσης υποχρεούται σε συμμόρφωση με τον Κανονισμό για την προστασία προσωπικών δεδομένων GDPR [2], και έχει ψηφίσει νόμους που διέπουν την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων σύμφωνα με αυτόν.

Όσον αφορά τη Διαύγεια, η πολιτική απορρήτου που διέπει την πλατφόρμα βασίζεται στον Νόμο 2472/1997, ο οποίος αναφέρεται στην προστασία των προσωπικών δεδομένων και ενσωματώνει βασικές αρχές διεθνώς αποδεκτές, όπως η ελαχιστοποίηση των δεδομένων, η ακρίβεια των πληροφοριών καθώς και η ασφάλειά τους [44]. Στην πράξη όμως, καθώς η πλατφόρμα επιβάλλει την ανάρτηση των δεδομένων ως έχουν, χωρίς καμία πρότερη τεχνική επεξεργασία όπως η ανωνυμοποίηση ή η ψευδονυμοποίηση [45], υφίστανται περιπτώσεις όπου αναρτώνται ακόμα και φωτογραφίες, ονόματα ή άλλα ταυτοποιήσιμα στοιχεία που ολοφάνερα υπονομεύουν την ιδιωτικότητα των υποκειμένων καθώς και αφαιρούν από αυτά το δικαίωμα άρνησης χρήσης των προσωπικών δεδομένων τους. Ταυτόχρονα με αυτό, ο διαχειριστής της πλατφόρμας δεν φέρει καμία νομική ευθύνη σε περίπτωση που επαναχρησιμοποιηθούν τα δεδομένα που αναρτώνται ως ανοιχτά [46], με όποιες συνέπειες μπορεί αυτό να έχει για τα υποκείμενα.

6.5.2 Κριτική Ανάλυση και Σημεία Προβληματισμού. Σημεία βελτίωσης

Τα όσα αναφέρθηκαν ως εδώ για την περίπτωση της Ελλάδας και της ψηφιακής πλατφόρμας ανοιχτών δεδομένων «Διαύγεια», αποτελούν χαρακτηριστικό παράδειγμα της αντίθεσης που χαρακτηρίζει το αντικείμενο της παρούσης εργασίας, δηλαδή το ζήτημα της εξισορρόπησης των εννοιών της ιδιωτικότητας με τα ανοιχτά και συνδεδεμένα δεδομένα [3]. Ενσαρκώνεται ξεκάθαρα η σύγκρουση μεταξύ της ζητούμενης διαφάνειας της διοίκησης και της προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας των πολιτών [41]. Καθότι η δημοσίευση των δεδομένων αυτών γίνεται χωρίς να έχουν υποστεί την οποιαδήποτε επεξεργασία, τίθενται σε άμεσο κίνδυνο τα υποκείμενα των εν λόγω δεδομένων [47].

Ελλείψεις παρατηρούνται και στην κατηγοριοποίηση των ευαίσθητων δεδομένων [48]. Τα υφιστάμενα συστήματα αξιολόγησης του κινδύνου επαναπροσδιορισμού των ατόμων, σύμφωνα με όσα προτείνονται από τις διεθνείς πρακτικές, δεν εφαρμόζονται ανά τύπο των δεδομένων που δημοσιεύονται [49], με αποτέλεσμα να μην χαρακτηρίζονται αυτά ως χαμηλού ή υψηλού κινδύνου και να αντιμετωπίζονται με τον ίδιο ακριβώς τρόπο.

Ταυτόχρονα, οι πολίτες που θα έπρεπε να έχουν τη δυνατότητα πλήρους ελέγχου των δεδομένων τους, όπως και θεωρείται αναφαίρετο δικαίωμά τους [50], στην περίπτωση της Διαύγειας έχουν μηδαμινή επιλογή τροποποίησης ή αφαίρεσής τους ακόμα και σε περίπτωση που θίγεται η ιδιωτική τους ζωή [51]. Για παράδειγμα, αν υποθέσουμε ότι έχουμε περίπτωση μετακίνησης δημοτικού υπάλληλου από την υπηρεσία που απασχολείται σε άλλη, η απόφαση που εκδίδεται σχετικά θα πρέπει να αναρτηθεί στην πλατφόρμα. Η απόφαση βάσει νόμου θα

δημοσιευτεί ως έχει, και άρα θα περιλαμβάνει το όνομα του υπάλληλου, τον αριθμό ταυτότητάς του, τη θέση που απασχολείται και τη μελλοντική του θέση καθώς και πληροφορίες σχετικές με τους οικογενειακούς λόγους της μετάθεσης [43]. Μία απλή αναζήτηση στο διαδίκτυο θα φέρει στο φως τα προσωπικά στοιχεία του δημοτικού υπάλληλου μαζί με προσωπικά δεδομένα για την οικογενειακή του κατάσταση με αποτέλεσμα να αισθανθεί ότι παραβιάζεται η ιδιωτικότητά του. Σε περίπτωση που αποφασίσει να απευθυνθεί στον αρμόδιο φορέα και να ζητήσει τη διαγραφή των δεδομένων ή έστω την απόκρυψή τους από το έγγραφο, θα λάβει την απάντηση ότι η ανάρτηση στη Διαύγεια είναι υποχρεωτική και μη αναστρέψιμη και ότι δεν προβλέπεται από το νομικό πλαίσιο κανένας μηχανισμός τροποποίησης ή διαγραφής της απόφασης, αφού αυτό θα παραβίαζε την αρχή της διαφάνειας [52]. Ο πολίτης λοιπόν δεν έχει στη διάθεσή του κανένα απολύτως εργαλείο ελέγχου ή ανάκλησης [53]. Δεν μπορεί να παρέμβει νομικά ακριβώς λόγω της σύγκρουσης μεταξύ διαφάνειας και ιδιωτικότητας.

Το παράδειγμα αυτό μπορεί να φέρει στην επιφάνεια τα προβλήματα που θα πρέπει να αντιμετωπιστούν στην περίπτωση της πλατφόρμας [54]. Δεν υφίσταται το δικαίωμα της λήθης [2], δεν υπάρχουν μηχανισμοί διόρθωσης ενώ σαφώς απαιτείται η δημιουργία ενός θεσμικού μηχανισμού που θα επιτρέπει τις εξαιρέσεις σε ειδικές περιπτώσεις [55]. Ξεκάθαρα, λοιπόν, παρατηρούμε ότι η ζυγαριά κλίνει κατά πολύ προς την αρχή της διαφάνειας, αφήνοντας πίσω την ανάγκη για προστασία των προσωπικών δεδομένων [3].

Πέραν του ζητήματος της διαφάνειας, η έννοια της οποίας εκθειάζεται σε βάρος της ιδιωτικότητας, εγείρονται ερωτήματα σχετικά με το πώς οι εκάστοτε κυβερνήσεις μπορούν να χρησιμοποιήσουν τεχνολογίες προσωποποίησης για πολιτικούς σκοπούς και αξιολόγηση [56], και ενισχύεται ο κίνδυνος για κοινωνικό έλεγχο και παραβίαση της ιδιωτικότητας [57], κάτι που θα οδηγήσει με μαθηματική ακρίβεια στην απώλεια της εμπιστοσύνης των πολιτών στους θεσμούς [58], σκοπό που έχει εξαρχής η πρακτική της διαφάνειας, δημιουργώντας έτσι ένα οξύμωρο σχήμα. Περιβάλλοντα διαφάνειας όπως αυτό της Διαύγειας θα πρέπει να ενσωματώνουν μηχανισμούς που θα ρυθμίζουν τον τρόπο με τον οποίο συλλέγονται, αποθηκεύονται, επεξεργάζονται και δημοσιοποιούνται τα δεδομένα ώστε να βρεθούν ένα βήμα πιο κοντά στο ζητούμενο της ισορροπίας μεταξύ της ιδιωτικότητας και της διαφάνειας [59].

Προτείνεται λοιπόν αρχικά να υφίσταται διαβάθμιση των δεδομένων ως προς την ευαισθησία τους κατά κατηγορίες πριν τη δημοσίευσή τους [48], με αξιολόγηση των πιθανών κινδύνων για την επαναταυοποίηση των υποκειμένων να είναι απαραίτητη πριν την κάθε δημοσίευση συνόλου δεδομένων [60]. Κριτικής σημασίας είναι και η χρήση εργαλείων ανωνυμοποίησης και ψευδονυμοποίησης στα έγγραφα για τους ίδιους λόγους [45]. Τέλος, ενώ μέχρι τώρα οι πολίτες δεν έχουν κανέναν έλεγχο στα δεδομένα τους τα οποία δημοσιεύονται στην πλατφόρμα, θα πρέπει να υπάρξει σεβασμός του δικαιώματος στη λήθη [2] όπως και να συμπεριλαμβάνονται οι πολίτες στη διαδικασία λήψης αποφάσεων μέσω της συγκατάθεσης ανά σκοπό [61].

Κριτική Αξιολόγηση Μελετών Περίπτωσης (Πίνακας 8)

Χώρα	**Κριτική Αξιολόγηση**	**Σημεία Βελτίωσης**
Ηνωμένο Βασίλειο	Η διαδικτυακή τοποθεσία police.uk προσφέρει προηγμένες υπηρεσίες RTLD	Ανωνυμοποίηση ανάλογα με τον πληθυσμό

	με χάρτες και API. Υπάρχουν τεχνικές ανωνυμοποίησης αλλά όρια σε μικρούς πληθυσμούς	Προσθήκη μηχανισμών συγκατάθεσης/διαβούλευσης
Εσθονία	Πρωτοποριακή αρχιτεκτονική X-Road με έλεγχο πρόσβασης, ο πολίτης δύναται να ελέγξει ποιος βλέπει τα δεδομένα του	Ενίσχυση ψηφιακής παιδείας Ανάλυση κινδύνων από αυτοματοποιημένη διαλειτουργικότητα
Φινλανδία	Θεσμικά ώριμη πολιτική ανοιχτότητας με νομική ενσωμάτωση GDPR, εστιάζει στην επαναχρησιμοποίηση των δεδομένων από ερευνητές και επιχειρηματίες	Περιορισμένη δημόσια διαβούλευση Ανάγκη για διαφάνεια στο μοντέλο αποδοχής και συγκατάθεσης των υποκειμένων όσον αφορά ευαίσθητα δεδομένα
Ολλανδία	Ελεγχόμενη διαλειτουργικότητα και κατανεμημένες βάσεις δεδομένων, ανεξάρτητη εποπτεία	Πολύπλοκη πρόσβαση στα δεδομένα και συνδυασμός δεδομένων για μικρούς φορείς Περιορισμοί στην ευρωπαϊκή διαλειτουργικότητα λόγω εσωτερικών ρυθμιστικών πρακτικών
Ελλάδα	Ανοιχτή πλατφόρμα διοικητικών πράξεων, μεγάλη έμφαση στη διαφάνεια με περιορισμένη προστασία ιδιωτικότητας	Θεσμική πρόβλεψη δικαιώματος στη λήθη Εισαγωγή μηχανισμών αξιολόγησης κινδύνου Ενίσχυση εργαλείων ανωνυμοποίησης σε δημόσια έγγραφα

Συγκρίνοντας τις πέντε αυτές ευρωπαϊκές χώρες, παρατηρούμε τον πολυδιάστατο χαρακτήρα εφαρμογής των πολιτικών διαφάνειας μέσω RTLD και της προστασίας της ιδιωτικότητας. Αν και όλες οι χώρες ως μέλη της ΕΕ οφείλουν να συμμορφώνονται με τον Κανονισμό GDPR, και δηλώνουν ότι στηρίζουν αρχές που αυτός επιβάλλει όπως η διαφάνεια και η λογοδοσία, στην πραγματικότητα η ωριμότητα των θεσμών σε κάθε μία από τις χώρες αυτές σε συνδυασμό με την τεχνολογική υποδομή που διαθέτουν αλλά και την κουλτούρα της κοινωνίας της επηρεάζουν κατά πολύ τον τρόπο με τον οποίο εφαρμόζονται αυτές οι αρχές [12], [13], [21].

Η Εσθονία και η Ολλανδία έχουν ξεκάθαρο προβάδισμα όσον αφορά τη θεσμική αρχιτεκτονική προστασίας, με βάσεις δεδομένων που είναι κατανεμημένες αποκεντρικά, με αυστηρό έλεγχο πρόσβασης και με το να δίνεται η δυνατότητα στον πολίτη να παρακολουθεί τη χρήση και επεξεργασία των δεδομένων του και παράλληλα να συμμετέχει στη λήψη αποφάσεων που αφορούν τα προσωπικά του δεδομένα [14], [19]. Στην περίπτωση βέβαια της Ολλανδίας η

στάση που τηρείται ως προς τη διαλειτουργικότητα είναι αρκετά συντηρητική, με αποτέλεσμα να μην επιτρέπεται η μεγάλη συγκέντρωση προσωπικών δεδομένων στο δημόσιο τομέα ενώ στην περίπτωση της Εσθονίας παρατηρούμε προσπάθεια λειτουργικής ενσωμάτωσης χωρίς όμως να στερούνται τα υποκείμενα των δεδομένων τον έλεγχο πάνω σε αυτά [16], [20].

Όσον αφορά τη Φινλανδία, έχουμε ένα θεσμικά σταθερό και με την εμπιστοσύνη της κοινωνίας μοντέλο που βασίζεται στη συνταγματική αρχή της δημοσιότητας. Απουσιάζει όμως θεσμικά η διαβούλευση με τους πολίτες, ενώ η ιδιωτικότητα ερμηνεύεται με τεχνοκρατικούς όρους με αποτέλεσμα να αποδυναμώνεται ο ρόλος του πολίτη ως συμμετέχων στη λήψη αποφάσεων [15], [18].

Το Ηνωμένο Βασίλειο από την πλευρά του υιοθετεί μία προσέγγιση που ναι μεν λειτουργικά είναι καινοτόμα αλλά ηθικά είναι τουλάχιστον αμφιλεγόμενη. Τα δεδομένα διατίθενται μαζικά χωρίς να προσαρμόζονται καταλλήλως με αποτέλεσμα να εκτίθενται ομάδες πολιτών σε κίνδυνο επαναπροσδιορισμού ταυτότητας, ειδικά σε περιπτώσεις που τα δεδομένα αφορούν πληθυσμιακές ομάδες περιορισμένου γεωγραφικά μεγέθους [17], [22].

Τέλος έχουμε την περίπτωση της Ελλάδας. Με την υιοθέτηση της Διαύγειας, επιτυγχάνεται η απόλυτη διαφάνεια για τους θεσμούς, ενώ από την άλλη η προστασία της ιδιωτικότητας είναι από περιορισμένη έως μηδαμινή. Δεν υφίστανται μηχανισμοί επανεξέτασης των δεδομένων, ούτε ανωνυμοποίηση αλλά ούτε και πρωτόκολλα διαβάθμισης κινδύνου [23]. Ουσιαστικά, η πλατφόρμα θυσιάζει κάθε μορφή ιδιωτικότητας και ελέγχου των προσωπικών δεδομένων από τα υποκείμενά τους στο βωμό της λογοδοσίας και της διαφάνειας, και έτσι καθίσταται προβληματική όταν δούμε την πρακτική αυτή στα πλαίσια του Κανονισμού της ΕΕ GDPR [24].

Συμπερασματικά, καμία από τις χώρες που είδαμε ως μελέτες περιπτώσεων δεν έχει επιτύχει την τέλεια ισορροπία μεταξύ διαφάνειας και ιδιωτικότητας. Για να θεωρείται η πολιτική μίας χώρας αποτελεσματική, θα πρέπει να υφίστανται ορισμένες προϋποθέσεις. Θα πρέπει οι τεχνολογίες που χρησιμοποιούνται να είναι άρτιες, να υφίσταται λογοδοσία σε θεσμικό επίπεδο και ως βασικό συστατικό της επιτυχίας, θα πρέπει στο πλαίσιο του δημοκρατικού πνεύματος να υπάρχει η συμμετοχή των πολιτών σε αποφάσεις που θα τους καθιστούν όχι ως παθητικά υποκείμενα των δεδομένων, αλλά ως ενδυναμωμένους πολίτες με έλεγχο πάνω στα προσωπικά τους δεδομένα [12], [21].

6.6 Συμπεράσματα Μελετών Περίπτωσης

Έχοντας προχωρήσει σε περιγραφή πέντε περιπτώσεων από χώρες της ΕΕ ως προς τον τρόπο που αντιμετωπίζονται τα προσωπικά και τα ανοιχτά δεδομένα, παρατηρούμε την πολυπλοκότητα του ζητήματος που αφορά την ισορροπία μεταξύ διαφάνειας και προστασίας της ιδιωτικότητας [13], [14]. Κατά γενική ομολογία, βασικός στόχος της δημοσίευσης των ανοιχτών δεδομένων είναι η λογοδοσία των θεσμών, αλλά ανά τις χώρες υπάρχουν διαφορετικές θεσμικές παραδόσεις και τεχνολογικές υποδομές, που σε συνδυασμό με την κουλτούρα της κάθε περιοχής οδηγούν στην ύπαρξη πολλών διαφορετικών μοντέλων εφαρμογής [15], [20].

Η Εσθονία και η Ολλανδία ενσωματώνουν τεχνικά και νομικά πρότυπα για την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας, υιοθετώντας τεχνολογικές αρχιτεκτονικές για τον έλεγχο της πρόσβασης και την αποκέντρωση της πληροφορίας [14], [19]. Η Φινλανδία

στηρίζει το μοντέλο της στην εμπιστοσύνη που δείχνουν οι πολίτες στους θεσμούς, και αυτό ενώ είναι σταθερό είναι λιγότερο συμμετοχικό δίνοντας έτσι τεχνοκρατικό χαρακτήρα στην προσέγγισή της [18]. Το Ηνωμένο Βασίλειο επικεντρώνεται στην καινοτομία και στη διάθεση της πληροφορίας, με την προστασία των υποκειμένων να έχει περιθώρια βελτίωσης [17], [22]. Όσον αφορά την Ελλάδα, παρατηρείται ακραία υπερίσχυση της διαφάνειας έναντι της προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας καθώς απουσιάζουν παντελώς διορθωτικοί μηχανισμοί και τεχνολογίες ανωνυμοποίησης των δεδομένων [23], [24].

Σε όλες τις παραπάνω χώρες που καλύπτουν εύρος περιπτώσεων από το άκρο της προστασίας της ιδιωτικότητας μέχρι την απόλυτη διαφάνεια, μπορούμε με ασφάλεια να συμπεράνουμε ότι από μόνη της η αρχή της διαφάνειας δεν αρκεί για να έχουμε μία ποιοτική πολιτική Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης [21]. Για να επιτύχουμε κάτι τέτοιο, θα πρέπει να έχουμε στην εξίσωση και πολίτες οι οποίοι θα έχουν τη δυνατότητα να ελέγχουν, να αμφισβητούν και να συναινούν στη χρήση και την επεξεργασία των δεδομένων τους, και άρα να έχουν απόλυτη γνώση σχετικά με το πώς αυτά δημοσιεύονται και πώς και από ποιους είναι προσβάσιμα [12], [13], παράλληλα με τεχνικά και οργανωτικά μέτρα προστασίας που θα καθησυχάζουν τους πολίτες πρακτικά και ουσιαστικά και μάλιστα θα εφαρμόζονται πριν από τη δημοσίευση των δεδομένων, και φυσικά τη θεσμική πρόβλεψη για πρωτόκολλα συνεχούς αξιολόγησης κινδύνου επαναταυτοποίησης των υποκειμένων των δεδομένων και τυχόν ηθικών συνεπειών που ένας τέτοιος επαναπροσδιορισμός φυσικού προσώπου δύναται να έχει [16], [20].

Καθώς η ζητούμενη ισορροπία μεταξύ διαφάνειας και ιδιωτικότητας αφορά θέμα δυναμικό και όχι στατικό, αφού οι τεχνολογία που διατίθεται και οι νομικές απαιτήσεις διαρκώς αλλάξουν και εξελίσσονται μαζί με τον τρόπο που αντιμετωπίζουν το ζήτημα και οι πολίτες, απαιτείται διαρκής επαναπροσδιορισμός του [21]. Η υπευθυνότητα στη διαχείριση των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης αποτελεί λοιπόν υπόθεση αφενός τεχνική και νομική, αφετέρου πολιτική και δημοκρατική [12], [14], [19].

7 *Συμπεράσματα*

Με την ενότητα 7 ολοκληρώνεται η μελέτη σχετικά με τα Ανοιχτά Δεδομένα και την Προστασία των Προσωπικών Δεδομένων. Αρχικά ανακεφαλαιώνονται τα βασικά ευρήματα της εργασίας, όπως επίσης αναφέρονται και οι απαντήσεις που προέκυψαν στα ερωτήματα που έχουν τεθεί στην αρχή της παρούσης. Εν συνεχεία αξιολογούνται τυχόν περιορισμοί που υφίστανται κατά την εξέλιξη της έρευνας και διατυπώνονται προτάσεις για μελλοντική έρευνα πάνω στο ζήτημα της ισορροπίας ανάμεσα στην ιδιωτικότητα και τα Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης, η οποία είναι και ο στόχος όχι μόνο της ακαδημαϊκής έρευνας, αλλά και πολιτών και θεσμών.

7.1 Ανακεφαλαίωση Βασικών Ευρημάτων

Με την παρούσα εργασία επιχειρήσαμε να διερευνήσουμε το πώς η προστασία των προσωπικών δεδομένων γίνεται ή όχι μέρος των πολιτικών και τεχνολογικών πρακτικών δημοσιοποίησης των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης, διερευνώντας ένα θεωρητικό πλαίσιο και ταυτόχρονα πραγματικές πρακτικές φορέων χωρών της ΕΕ. Ακολουθούν κατηγοριοποιημένα τα κύρια ευρήματα της παρούσης.

7.1.1 Η έννοια των RTLD εμπεριέχει εκ φύσεως κίνδυνο επαναταυτοποίησης

Από τη φύση τους, τα ανοιχτά δεδομένα αποσκοπούν στη δημοσιοποίηση δεδομένων ώστε να επιτευχθεί ην διαφάνεια των θεσμών και να αυξηθεί η εμπιστοσύνη των πολιτών σε αυτούς. Με τη δημοσίευση όμως «ωμών» δεδομένων, χωρίς να έχουν υποστεί κάποιου είδους πρακτική όπως η ανωνυμοποίηση ή η ψευδονυμοποίηση, ή ακόμα και όταν τα δεδομένα έχουν κρυπτογραφηθεί θεωρητικά, όταν λαμβάνουμε υπόψη και τη διαλειτουργικότητα και το πώς μπορούν στοιχεία από διαφορετικές βάσεις και σύνολα δεδομένων να συνδυαστούν, μπορούμε να οδηγηθούμε σε καταστάσεις επαναταυτοποίησης υποκειμένων των δεδομένων [2], [5], [9]. Αν η τεχνολογία λοιπόν που έχει επιλεγεί για την επίτευξη της ανωνυμοποίησης των δεδομένων δεν είναι εξελιγμένη και προσεκτικά δομημένη, δεν επαρκεί για να προφυλάξει τα δεδομένα και τα φυσικά πρόσωπα που αυτά αναφέρονται από τον κίνδυνο και να εγγυηθεί την ασφάλειά τους. Όσον αφορά τώρα τις τεχνικές της ανωνυμοποίησης και της ψευδονυμοποίησης, αν και αυτές προτείνονται από τον Κανονισμό της ΕΕ GDPR, από μόνες τους και χωρίς να συνδυάζονται με

πρακτικές όπως αυτή της εκτίμησης του επιπέδου κινδύνου, και ειδικά σε περιβάλλοντα όπου το επίπεδο της διαλειτουργικότητας είναι υψηλό [7], [14], δεν επαρκούν για την απόλυτη προστασία των υποκειμένων των δεδομένων.

7.1.2 Διαφοροποίηση Εθνικών Προσεγγίσεων στην ΕΕ

Με αφετηρία τις μελέτες περίπτωσης, οι οποίες στο σύνολό τους αφορούν χώρες της ΕΕ με υποχρέωση τήρησης του κανονισμού GDPR, παρατηρούμε ότι η Εσθονία, η Ολλανδία, η Φινλανδία, το Ηνωμένο Βασίλειο και τέλος η Ελλάδα, οι οποίες και μας απασχόλησαν στο κεφάλαιο 6, διαφέρουν θεσμικά, πολιτικά και τεχνικά. Στις περιπτώσεις της Εσθονίας και της Ολλανδίας έχουμε μια πιο ανθρωποκεντρική θεώρηση του ζητήματος, με αρχιτεκτονικές που έχουν ως βασικό στόχο την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων των υποκειμένων σε βάρος πολλές φορές της διαφάνειας [3], [6], [11] που δύναται να προκύψει από τη δημοσίευση και ελεύθερη διάθεση προς ανάγνωση, χρήση και επεξεργασία των δεδομένων, μαζί με την τεχνολογική, ακαδημαϊκή και οικονομική πρόοδο που μπορεί να έχει ως αφετηρία τα Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης. Από την άλλη, χώρες όπως η Ελλάδα και το Ηνωμένο Βασίλειο επιλέγουν μια πολιτική ανοιχτότητας και διάθεσης των δεδομένων ελεύθερα και σε περιπτώσεις χωρίς περιορισμούς και τεχνικές προστασίας όπως η ανωνυμοποίηση, προτείνοντας τη διαφάνεια σε αντιδιαστολή με την προστασία των προσωπικών δεδομένων η οποία είναι από περιορισμένη έως ανύπαρκτη. Απουσιάζουν λοιπόν μηχανισμοί ελέγχου της χρήσης και επεξεργασίας των δεδομένων, αφήνοντας τα υποκείμενα αυτών εκτεθειμένα σε κινδύνους επαναταυτοποίησης [8], [10], [13].

7.1.3 Απαίτηση για Ισχυρό Θεσμικό και Οργανωτικό Πλαίσιο

Με την πρόοδο της έρευνας, παρατηρήθηκε η ύπαρξη ανάγκης όχι μόνο τεχνολογικών λύσεων που θα θωρακίσουν τα προσωπικά δεδομένα των πολιτών, αλλά αυτά θα πρέπει να συνδυαστούν με οργανωτικά μέτρα. Αυτά αποτελούν ένα σύνολο μέτρων όπως η μέθοδος εκτίμησης αντικτύπου, όπου υπολογίζεται ο κίνδυνος επαναταυτοποίησης φυσικών προσώπων ανά περίπτωση, το δικαίωμα των υποκειμένων των δεδομένων να ενημερώνονται σχετικά με τη δημοσιοποίηση, χρήση και επεξεργασία των δεδομένων τους, όπως και να εναντιώνονται σε αυτή ή να ζητήσουν τη διόρθωση των στοιχείων τους ή και τη διαγραφή τους [1], [4], [12].

Επίσης, ως ένα ακόμα οργανωτικό μέτρο προτείνεται η συμμετοχή των πολιτών σε θέματα διακυβέρνησης των δεδομένων. Αυτή η πρακτική παρουσιάζει διπλά οφέλη για τους θεσμούς και τους πολίτες. Από τη μία οι πολίτες έχουν λόγο στον τρόπο με τον οποίο θα γίνεται η δημοσίευση των δεδομένων τους όπως και ποια θα είναι αυτά τα δεδομένα, από την άλλη οι θεσμοί έχουν την υποστήριξη των πολιτών στις αποφάσεις που λαμβάνονται και κατά συνέπεια νομιμοποιούνται. Σε κάθε περίπτωση, ταυτόχρονα με τα οφέλη αυτά προάγεται και η δημοκρατία [2], [15].

Τέλος, κάθε κράτος θα πρέπει να έχει σαφείς πολιτικές πρόσβασης και δημοσιοποίησης των δεδομένων που θα εμφανίζονται ως RTLD, που θα σέβονται τους νόμους σε εθνικό και ευρωπαϊκό επίπεδο και φυσικά θα προάγουν τη διαφάνεια ενώ ταυτόχρονα θα σέβονται την ιδιωτικότητα των ατόμων.

7.1.4 Ιδιωτικότητα στον Κύκλο Ζωής των RTLD

Για την καλύτερη προστασία της ιδιωτικότητας και των προσωπικών δεδομένων των υποκειμένων, φαίνεται να υπάρχει η απαίτηση για ορισμένες αρχιτεκτονικές στη δομή των πληροφοριακών συστημάτων που χειρίζονται τα δεδομένα. Μιλάμε για τις έννοιες του privacy by design και privacy by default. Αυτό που επιτυγχάνεται είναι να λαμβάνεται υπόψη η προστασία των δεδομένων όχι εκ των υστέρων, αλλά από τη φάση του σχεδιασμού και της δημιουργίας των συστημάτων αυτών και συνεχίζεται και με τη δημοσίευση και την πρόσβαση σε αυτά [5], [9], [14].

7.1.5 Ανάγκη για Εθνικές και Ευρωπαϊκές Κατευθυντήριες Γραμμές

Τα ανοιχτά δεδομένα είναι κατά τον ορισμό τους διαθέσιμα μέσω μίας απλής σύνδεσης στο ίντερνετ από το οποιοδήποτε άτομο σε όλο τον κόσμο. Για την καλύτερη προστασία όμως των ατόμων που τα δεδομένα αυτά αφορούν, υφίστανται νόμοι και κανονισμοί σε εθνικό και ευρωπαϊκό επίπεδο που ρυθμίζουν την πρόσβαση σε αυτά όχι μόνο εντός της επικράτειάς τους αλλά και σε περιπτώσεις που τα δεδομένα θα φύγουν σε τρίτες χώρες που δεν διέπονται από τον Κανονισμό του GDPR. Εντός της ΕΕ, ενώ όπως είπαμε ισχύει για όλες τις χώρες μέλη ο Κανονισμός για την προστασία των δεδομένων, δεν υφίστανται ενιαίες κατευθυντήριες γραμμές για τις πρακτικές που ακολουθούνται για την διαχείριση των RTLD από τα κράτη-μέλη. Η έλλειψη ισχυρού νομικού πλαισίου αποτελεί ανασταλτικό παράγοντα για τους φορείς προκειμένου να ανοίξουν τα δεδομένα [3], [6], [10]. Θα πρέπει να υπάρξει λοιπόν τυποποιημένος οδηγός συμβατότητας με τον GDPR που θα προσαρμόζεται παράλληλα στο εκάστοτε επίπεδο κινδύνου, ώστε να καμφθούν οι αντιστάσεις και να προστατεύονται καλύτερα τα δεδομένα και τα υποκείμενά τους, ενώ παράλληλα να προαχθεί η διαφάνεια και οι δημοκρατικές πρακτικές μέσω των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης [7], [11], [15].

7.2 Απαντήσεις στα Ερευνητικά Ερωτήματα

Τα ερωτήματα που εξ αρχής τέθηκαν ως στόχοι της παρούσης εργασίας αφορούν την κατανόηση των κινδύνων που υπάρχουν όσον αφορά την προστασία των προσωπικών δεδομένων στο πλαίσιο των Συνδεδεμένων Προσωπικών Δεδομένων και στις πρακτικές, θεσμικές ή τεχνικές, που θα μπορούσαν να συμβάλλουν ως προς το στόχο της διασφάλισης της ιδιωτικότητας των ατόμων [2], [5], [9]. Τα ερευνητικά ερωτήματα που τέθηκαν απαντώνται ως εξής:

Όσον αφορά τους βασικούς κινδύνους για την ιδιωτικότητα των υποκειμένων κατά τη δημοσίευση, χρήση και επεξεργασία των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης, αναδεικνύονται ως σημαντικότεροι η πιθανότητα επαναταυτοποίησης ατόμων μέσω της διασταύρωσης των υφιστάμενων ανοιχτών δεδομένων με άλλα διαθέσιμα σύνολα δεδομένων [3], [6], [14], η πιθανότητα να αποκαλυφθούν ευαίσθητες για τα υποκείμενα πληροφορίες ακόμα και όταν τα δεδομένα τους τα οποία δεν θεωρούνται προσωπικά συνδυαστούν με άλλες πηγές [7], [12], καθώς και η κατάχρηση των RTLD από τρίτα μέρη χωρίς να υφίσταται νομικός ή και ηθικός περιορισμός [8], [10], εκθέτοντας έτσι τα υποκείμενα. Η ένταση του κινδύνου είναι ανάλογη των λεπτομερειών που διατίθενται μέσω των βάσεων δεδομένων, ειδικά όταν αυτές ανανεώνονται συχνά ή συνδέονται με γεωγραφικό προσδιορισμό των δεδομένων [4], [15].

Όταν εξετάζονται οι τεχνικές και οργανωτικές πρακτικές που μπορούν να βοηθήσουν στην προστασία των δεδομένων από τους προαναφερθέντες κινδύνους, εντοπίζονται ως κρίσιμες πρακτικές αρχικά οι τεχνικές της ανωνυμοποίησης και ψευδονυμοποίησης των δεδομένων βασιζόμενοι πάντα στη φύση του πιθανού κινδύνου του συνόλου των δεδομένων που δημοσιεύονται [5], [9], ενώ έχουμε και τα πρωτόκολλα εκτίμησης του αντικτύπου στην ιδιοτικότητα [7], [13]. Επίσης, προτείνεται η χρήση αρχιτεκτονικών privacy by design και privacy by default κατά το σχεδιασμό των πληροφοριακών συστημάτων [2], [14] που θα χρησιμοποιούνται για την αποθήκευση και διανομή των δεδομένων, όπως και η θέσπιση νομικού πλαισίου κανόνων πρόσβασης στα δεδομένα και περιορισμών στη διασύνδεσή τους με άλλες βάσεις δεδομένων [1], [11], μειώνοντας έτσι τον κίνδυνο επαναταυτοποίησης φυσικών προσώπων. Όσον αφορά τον τρόπο με τον οποίο θα αξιολογείται ο πιθανός κίνδυνος και ο αντίκτυπος που θα έχει στα υποκείμενα, προτείνεται η δημιουργία και συμμετοχή στις διαδικασίες ανεξάρτητων επιτροπών αξιολόγησης με συμμετέχοντες με τεχνολογικό, θεσμικό, νομικό και ηθικό υπόβαθρο [3], [6].

Με βάση τις μελέτες περιπτώσεων που συναντήσαμε, βλέπουμε ότι οι εθνικές προσεγγίσεις ακόμα και χωρών που ανήκουν στην ίδια συνομοσπονδιακή ένωση όπως κράτη-μέλη της Ευρωπαϊκής Ένωσης, παρουσιάζονται διαφοροποιημένες σε μεγάλο βαθμό όσον αφορά τη διαχείριση των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης και της ιδιωτικότητας. Παρουσιάζονται περιπτώσεις χωρών που δίνουν μεγάλη βαρύτητα στο ζήτημα της προστασίας των προσωπικών δεδομένων και των υποκειμένων τους, με συστημικά εργαλεία προστασίας να ενσωματώνονται στη δημόσια διοίκηση, όπως οι χώρες της Εσθονίας και της Ολλανδίας, έχουμε επίσης χώρες που έχουν ήδη χτίσει την απαραίτητη εμπιστοσύνη των πολιτών στους θεσμούς και αυτό φαίνεται και στον τρόπο που διαχειρίζονται το ζήτημα ισορροπίας μεταξύ ιδιωτικότητας και προστασίας των προσωπικών δεδομένων [3], [6], [11], όπως και η Φινλανδία, αν και η προσέγγιση είναι περισσότερο τεχνοκρατική και λιγότερο ανθρωποκεντρική με απουσία διαβούλευσης με τους πολίτες [8], [12], και τέλος έχουμε και περιπτώσεις χωρών όπως το Ηνωμένο Βασίλειο και η Ελλάδα που δίνουν βάση στην επίτευξη της διαφάνειας και δημοσιοποιούν δεδομένα χωρίς να υφίστανται επαρκείς έλεγχοι ή και ανωνυμοποίηση των εν λόγω δεδομένων, αφήνοντας πολλά να πρέπει να γίνουν για την προστασία των υποκειμένων, που σε περιπτώσεις δεν μπορούν να κάνουν κάποια θεσμική ενέργεια για να αντιστρέψουν την έκθεση στην οποία υπόκεινται. Ειδικά η Ελλάδα δεν δίνει καμία δυνατότητα να γίνει επανεξέταση των δημοσιοποιημένων δεδομένων κατά περίπτωση ή έστω να δοθεί συγκατάθεση για τη δημοσιοποίησή τους, όπως φάνηκε κατά την περιγραφή της πλατφόρμας δημοσίευσης διοικητικών πράξεων «Διαύγεια» [4], [10], [13].

Τέλος, αναφερόμενοι στο ζητούμενο της έρευνας που είναι η εύρεση ισορροπίας μεταξύ της διαφάνειας των θεσμών και της προστασίας των προσωπικών δεδομένων και των υποκειμένων τους στα πλαίσια των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης, θεωρούμε πως ναι, υφίσταται ως πιθανότητα αλλά υπό προϋποθέσεις [2], [7], [15]. Αυτές είναι ο θεσμικός σχεδιασμός και η συνεχής αξιολόγηση των κινδύνων που παρουσιάζονται διαρκώς, ειδικά με την πρόοδο των τεχνολογικών μέσων που είναι διαθέσιμα. Σε θεωρητικό επίπεδο, η διαφάνεια θα πρέπει να πάψει να ορίζεται ως απεριόριστη δημοσιοποίηση δεδομένων. Πρακτικές χωρών που έχουν σημειώσει επιτυχία δείχνουν ότι μπορεί να υπάρξει δημοσίευση δεδομένων που θα έχει συγκεκριμένο στόχο και σκοπό, τα δεδομένα αυτά θα έχουν υποστεί την απαραίτητη επεξεργασία

για να επιτευχθεί ο στόχος της προστασίας των ατόμων και επίσης αυτά να δημοσιεύονται υπό συγκεκριμένους όρους. Έτσι επιτυγχάνεται ο δημόσιος έλεγχος χωρίς όμως να θυσιάζεται η ιδιωτικότητα.

7.3 Περιορισμοί της Έρευνας

Όπως σε κάθε επιστημονική εργασία, έτσι και για την παρούσα μελέτη υφίστανται ορισμένοι μεθοδολογικοί και εννοιολογικοί περιορισμοί, με συνέπεια τον επηρεασμό της δυνατότητας γενίκευσης των συμπερασμάτων. Οι βασικοί περιορισμοί εντοπίζονται ως εξής:

Αρχικά, τα αποτελέσματα της εργασίας βασίζονται σε ανάλυση επιστημονικής βιβλιογραφίας, πολιτικών εγγράφων και κανονιστικών πλαισίων, όπως επίσης και σε μελέτες περίπτωσης από εθνικούς και διεθνείς φορείς, που και πάλι βασίζονται σε επιστημονική βιβλιογραφία. Δεν υφίσταται πρωτογενές ερευνητικό υλικό όπως συνεντεύξεις με φορείς και ερωτηματολόγια προς δημόσιους υπάλληλους και πολίτες. Περιορίζεται κατά αυτό τον τρόπο η πρόσβαση σε βιωματικές αναφορές ή επιχειρησιακά δεδομένα.

Όσον αφορά τις μελέτες περιπτώσεων και τη συγκριτική μελέτη μεταξύ των πέντε Ευρωπαϊκών χωρών που επιλέξαμε, και συγκεκριμένα της Ελλάδας, της Ολλανδίας, του Ηνωμένου Βασιλείου, της Εσθονίας και της Φινλανδίας, περιορίζει το εύρος της συγκριτικής ανάλυσης και ενδέχεται να μην αποδίδει την πλήρη παγκόσμια εικόνα του τρόπου που διαφοροποιούνται οι πολιτικές και οι τεχνολογίες που χρησιμοποιούνται για τη δημοσιοποίηση, χρήση και επεξεργασία των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης ανά τον κόσμο. Θα μπορούσαν βέβαια να είναι αντιπροσωπευτικά της ευρωπαϊκής περίπτωσης, αλλά βασίστηκαν σε κριτήρια διαθεσιμότητας και όχι στατιστικά.

Επιπλέον περιορισμοί της έρευνας αφορούν το χρονικό πλαίσιο των πληροφοριών που συνελέγησαν και το κατά πόσο ήταν επίκαιρες. Κάποιες από τις πολιτικές ή τις πλατφόρμες στις οποίες αναφερθήκαμε όπως η police.uk και η Διαύγεια μπορεί να έχουν μεταβληθεί πρόσφατα ως προς το νομικό ή τεχνολογικό ή θεσμικό τους πλαίσιο, και άρα λόγω του δυναμικού χαρακτήρα των νέων τεχνολογιών και της διαρκούς εξέλιξής τους, υπάρχει η πιθανότητα να μην αποτυπώνονται επαρκώς οι πιο πρόσφατες εξελίξεις από τα ευρήματα της παρούσης εργασίας.

Τέλος, αναφέρουμε πως καθώς η εργασία αποτυπώνεται σε θεωρητικό επίπεδο, οι τεχνικές μέθοδοι που συναντάμε κατά τη θεώρηση των τεχνολογικών παραμέτρων που άπτονται του ζητήματος, όπως οι τεχνολογίες της ανωνυμοποίησης και της ψευδονυμοποίησης, ο περιορισμός πρόσβασης και άλλες, προσεγγίζονται και αυτές σε θεωρητικό και μόνο επίπεδο με αναφορά μόνο στην έννοια της κάθε τεχνικής και στον τρόπο με τον οποίο λειτουργεί, και δεν υλοποιούνται ή αξιολογούνται συγκεκριμένα τεχνολογικά εργαλεία. Έτσι, η αξιολόγηση των κινδύνων βασίζεται στα πλαίσια της έρευνας σε υποθετικά και θεωρητικά σενάρια και βιβλιογραφικές εκτιμήσεις.

Παρά τους όσους περιορισμούς, θεωρούμε πως προσφέρεται μέσω της παρούσης εργασίας μία πολύπλευρη κατανόηση του ζητήματος που μπορεί να αποτελέσει τη βάση για εμβάθυνση μέσω μελλοντικής έρευνας.

7.4 Προτάσεις για Μελλοντική Έρευνα

Με την παρούσα εργασία ανοίγει το πεδίο για την πολυδιάστατη θεώρηση των ζητημάτων που αφορούν την προστασία της ιδιωτικότητας στο πλαίσιο των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης ή RTLD. Με βάση τα ευρήματα και τους περιορισμούς που έχουν εδώ αναφερθεί, παρουσιάζονται ορισμένες προτάσεις και κατευθυντήριες γραμμές για μελλοντική έρευνα.

Αρχικά κρίνεται αναγκαία ποιοτική και ποσοτική εμπειρική έρευνα σε επίπεδο τόσο διοίκησης όσο και πολιτών. Αυτό μπορεί να επιτευχθεί μέσω συνεντεύξεων στελεχών της δημόσιας διοίκησης που είναι σε θέσεις που διαχειρίζονται τα RTLD, με ερωτηματολόγια προς τους πολίτες σχετικά με την επίγνωση που διαθέτουν γύρω από τη δημοσιοποίηση των προσωπικών τους δεδομένων και τη σχετική τους στάση, καθώς και με μελέτες περίπτωσης εντός της ελληνικής διοίκησης για τη συγκεκριμένη περίπτωση της Ελλάδας με την ανάλυση πραγματικών εγγράφων ή βάσεων δεδομένων.

Κρίσιμη είναι και η τεχνική αξιολόγηση των μηχανισμών ανωνυμοποίησης και πρόσβασης σε δεδομένα, καθώς η θεωρητική προσέγγιση όπως η παρούσα εργασία δύναται να ενισχυθεί από τεχνικά πειράματα πάνω στη μοντελοποίηση RDF συνόλων δεδομένων με ενσωματωμένους περιορισμούς πρόσβασης, όπως και πάνω στη χρήση εργαλείων όπως differential privacy, k-anonymity και risk estimation tools, και να αναλυθούν πραγματικές περιπτώσεις επαναταυτοποίησης.

Θα ήταν επίσης χρήσιμη η ανάπτυξη εθνικών πλαισίων ταξινόμησης κινδύνου στα Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης, όπως η τυπολογία κατηγοριοποίησης δεδομένων κατά επίπεδο κινδύνου επαναταυτοποίησης, που θα προσαρμόζεται στις ιδιαιτερότητες της εκάστοτε χώρας. Ιδανικά θα μπορούσε να συνδυαστεί με οδηγίες πολιτικής για ανωνυμοποίηση και διαβούλευση με τους πολίτες.

Προτείνεται επίσης η συγκριτική ανάλυση με χώρες εκτός ΕΕ, όπου εφαρμόζονται διαφορετικές αρχές προστασίας των δεδομένων, ώστε να εντοπιστούν εναλλακτικά μοντέλα προσέγγισης της ζητούμενης ισορροπίας μεταξύ της διαφάνειας και της προστασίας των δεδομένων.

Τέλος, θα είχε ιδιαίτερο ενδιαφέρον μία μελέτη των ηθικών διαστάσεων της χρήσης των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης από τρίτα μέρη. Η Χρήση των RTLD από εφαρμογές τρίτων που τα χρησιμοποιούν για την ανάλυση της εγκληματικότητας, τις αξιολογήσεις σχολείων ή άλλες περιπτώσεις, εγείρει νέα ηθικά διλήμματα σχετικά με την παρακολούθηση, το στιγματισμό περιοχών και την έμμεση διάκριση.

Η έρευνα γύρω από τα Ανοιχτά Δεδομένα με δυνατότητα διασύνδεσης εξελίσσεται διαρκώς. Η περαιτέρω διερεύνηση των παραπάνω προτάσεων μπορεί να συμβάλλει στη διαμόρφωση περισσότερο ώριμων, υπεύθυνων και ισορροπημένων πολιτικών για τα δεδομένα σε επίπεδο τόσο εθνικό όσο και διεθνές.

7.5 Επίλογος

Η παρούσα διπλωματική εργασία διερεύνησε ένα ζήτημα ιδιαίτερης σημασίας για τη σύγχρονη ψηφιακή διακυβέρνηση, το οποίο είναι η ισορροπία της διαφάνειας με την προστασία της

ιδιωτικότητας στο πλαίσιο των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης. Στη σημερινή εποχή, όπου από τη διοίκηση επιδιώκεται η λογοδοσία, η τεκμηρίωση και η επαναχρησιμοποίηση της πληροφορίας, η διαφάνεια ανάγεται σε θεμελιώδη αξία της δημοκρατίας. Όμως η χωρίς όρια δημοσιοποίηση των δεδομένων θέτει σε κίνδυνο το δικαίωμα των πολιτών στην ιδιωτικότητα, βάλλοντας έτσι την εμπιστοσύνη στον ίδιο το θεσμό της διακυβέρνησης.

Μέσω της παρούσης αναδεικνύονται οι τεχνολογικές, ηθικές και νομικές προκλήσεις που συναντάμε με την υλοποίηση πολιτικών ανοιχτών δεδομένων, ειδικά στην περίπτωση που αυτά είναι διασυνδεδεμένα και μπορεί να περιέχουν άμεσα ή έμμεσα προσωπικά στοιχεία των πολιτών. Συγκρίνοντας περιπτώσεις εντός της ευρωπαϊκής επικράτειας παρατηρούνται διαφορετικά επίπεδα θεσμικής ωριμότητας και ευαισθησίας σε πρακτικό επίπεδο, συμπεραίνοντας έτσι ότι για την επιτυχή διαχείριση των Ανοιχτών Δεδομένων με δυνατότητα διασύνδεσης απαιτείται και τεχνική επάρκεια και δημοκρατική και θεσμική πρόνοια.

Στην περίπτωση της Ελλάδας ειδικά μέσω της εξέτασης της πλατφόρμας Διαύγεια βλέπουμε πως υφίσταται η τάση να υπερισχύει η διαφάνεια χωρίς καμία ύπαρξη μηχανισμών ελέγχου ή επανεξέτασης. Σε αντίθετη περίπτωση, χώρες όπως η Εσθονία και η Ολλανδία δίνουν μεγαλύτερη έμφαση στην προστασία της ιδιωτικότητας, με τεχνολογικά ώριμες και νομικά εναρμονισμένες πολιτικές δεδομένων.

Το συμπέρασμα της εργασίας εντοπίζεται στο σημείο που η προστασία της ιδιωτικότητας και η διαφάνεια δεν είναι αμοιβαία αποκλειόμενες έννοιες, αλλά δύνανται να συνυπάρξουν. Η ισορροπία μεταξύ τους μπορεί να οδηγήσει σε μία ώριμη και αξιόπιστη μορφή ηλεκτρονικής διακυβέρνησης. Η πρόκληση που εντοπίζεται για τους δημόσιους φορείς μαζί με τους νομοθέτες αλλά και τους πολίτες έγκειται στο σχεδιασμό μηχανισμών που θα προωθούν τη διαφάνεια όπου χρειάζεται, χωρίς όμως να εκθέτουν την ιδιωτικότητα των φυσικών προσώπων.

Η διαρκής εξέλιξη των νέων τεχνολογιών και η αξία των δεδομένων που διαρκώς αυξάνεται αποδεικνύουν πως το πόσο ανοιχτά θα είναι τα δεδομένα δεν αποτελεί τεχνικό μόνο ερώτημα αλλά και πολιτικό. Η απάντηση θα βρεθεί μόνο μέσα από το συνδυασμό διαλόγου, θεσμικών πλαισίων και σεβασμού προς το άτομο.

Βιβλιογραφία

[1]Borgesius, FZ, Gray, J & van Eechoud, M 2016, Open Data, Privacy and Fair Information Principles: Towards a Balancing Framework. In: Berkeley Technology Law Journal, vol. 30, no.2, University of Bath.

[2]Ben Green, Gade Cunningham, Ariel Ekblaw, Paul Kominers, Andrew Linzer, Susan Crawford, Open Data Privacy (2017), Berkman Klein Center for Internet & Society at Harvard University, Research Publication No. 2017-1, February 2017.

[3]Tomas Knap, Martin Necasky, Martin Svoboda, A Framework for Storing and Providing Aggregated Governmental Linked Open Data. In: EGOVIS/EDEM 2012, LNCS 7542, pp. 264-270, 20212, Springer-Verlag Berlin, Heidelberg 2012.

[4]Christos Kalloniatis, Evangelia Kavakli, Stefanos Gritzalis, Security Requirements Engineering for e-Government Applications: Analysis of Current Frameworks, R. Traunmuller (Ed.): EGOV 2004, LNCS 3183, pp.66-71, 2004. Springer-Verlag Berlin Heidelberg 2004.

[5]M. Suresh Babu, K. Bhavana Raj, D. Asha Devi, Data Security and Sensitive Data Protection using Privacy by Design Technique. In: A. Haldorai et al. (eds.), 2nd EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing, EAI/Springer Innovations in Communication and Computing, Springer Nature Switzerland AG 2021.

[6]Aristomenis Gritzalis, Aggeliki Tsohou, Costas Lambrinoudakis, Transparency-Enabling Systems for Open Governance: Their Impact on Citizens' Trust and the Role of Information Privacy. In: Springer International Publishing AG 2017, S.K. Katsikas and V. Zorkadis (Eds.): E-Democracy 2017, CCIS 792, pp. 47-63,2017.

[7]Marijn Janssen, Jeroen van den Hoven, Big and Open Linked Data (BORTLD) in government: a challenge to transparency and privacy?. In: Government Information Quarterly, Elsevier Inc, 2015.

[8]Paola Mavriki, Maria Karyda, Using Personalization Technologies for Political Purposes: Privacy Implications. In: Springer International Publishing AG 2017, S.K. Katsikas and V. Zorkadis (Eds.): E-Democracy 2017, CCIS 792, pp. 33-46, 2017.

[9]Keiran Hardy, Alana Maurushat, Opening up government data for Big Data analysis and public benefit. In: Computer Law and Security Review 33 (2017), Published by Elsevier Ltd.

[10]Amr Ali-Eldin, Anneke Zuiderwijk, Marijn Janssen, A Privacy Risk Assessment Model for Open Data. In: Springer International Publishing AG, part of Springer Nature 2018. B. Shishkov (Ed.): BMSD 2017, LNBIP 309, pp. 186-201, 2018.

[11]Mei Chen, Yuyan Cao, Yikai Liang, Determinants of open government data usage: Integrating trust theory and social cognitive theory. In: Government Information Quarterly, Elsevier Inc. June 2023.

[12]F. Buccafurri, L. Fotia, G. Lax, Allowing Continuous Evaluation of Citizen Opinions. In: A. Ko at al. (Eds.): EGOVIS/EDEM 2012, LNCS 7452, pp. 242-253, 2012. Springer-Verlag Berlin Heidelberg 2012.

[13]Michelle Anna Ruesh, Sebastian Basedow, Jan-Henning Korte, From E to O. Towards Open Participation as a Guiding Principle of Open Government. In: A. Ko at al. (Eds.): EGOVIS/EDEM 2012, LNCS 7452, pp. 254-263, 2012. Springer-Verlag Berlin Heidelberg 2012.

[14]Alexander Breil, Patrik Hitzalberger, Paulo da Silva Carvalho, Fernard Feltz, Exploring Data Integration Strategies for Public Sector Cloud Solutions. In: A. Ko at al. (Eds.): EGOVIS/EDEM 2012, LNCS 7452, pp. 271-278, 2012. Springer-Verlag Berlin Heidelberg 2012.

[15]Xingsen Zhang, A more secure framework for open government data sharing based on federated learning. In: Government Information Quarterly, Elsevier Inc, November 2024.

[16]Luciano Floridi, Open Data, Data Protection, and Group Privacy. In: Springer Science+Business Media Dordrecht 2014. Published online: 18 February 2014.

[17]Ronald Meijer, Peter Cornadie, Sunil Choenni, Reconciling Contradictions of Open Data Regarding Transparency, Privacy, Security and Trust. In: Journal of Theoretical and Applied Electronic Commerce Research, ISSN 0718-1876 Electronic Version, VOL 9/ISSUE 3/ September 2014/ 32-44. 2014 Universidad de Talca-Chile.

[18]Barbara Ubaldi, Open Government Data : Towards Empirical Analysis of Open Government Data Initiatives, OECD Working Papers on Public Governance No 22. https://dx.doi.org/10.1787/5k46bj4f03s7-en

[19]Jae-Seong Lee, Seung-Pyo Jun, Privacy-preserving data mining for open government data from heterogenous sources. In: Government Information Quarterly, Elsevier Inc, November 2020.

[20]Judie Attard, Fabrizio Orlandi, Simon Scerri, Soren Auer, A systematic review of open government data initiatives, In: Government Information Quarterly 32, Elsevier Inc, 2015 399-418

[21]Meg Young, Luke Rodriguez, Emily Keller, Feiyang Sun, Boyang Sa, Jan Whittington, Bill Howe, Beyond open vs closed: Balancing individual privacy and public accountability in data sharing. In: FAT 19: Conference on Fairness, Accountability and Transparency, January 29-31, 2019, Atlanta, GA, USA.

[22]Nicolas Gonzalvew-Gallego, Laura Nieto-Torrejon, Government data openness and coverage. How do they affect trust in European countries? In: Journal of Data and Information Science, 6(1), 139-153. November 2020.

[23]Abdullah Almuqrin, Ibrahim Mutambik, Abdulazaz Alomran, Jeffrey Gauthier, Majed Abusharhah, Factors influencing public trust in Open Government Data. In:Sustainability 2022, 14, 9765. August 2022.

[24]Keiron O'Hara, Transparency, Open Data and Trust in Government: Shaping the infosphere. In: WebSci 2012, June 22-24, 2012, Evanston, Illinois, USA.

[25]Micah Altman, Alexandra Wood, David R. O'Brien, Sahil Vadhan, Urs Gasser, Towards a Modern Approach to Privacy-Aware Government Data Releases. In: Berkeley Technology Law Journal, Vol. 30, No. 3 (2015), pp. 1967-2072. Published by: University of California, Berkeley, School of Law

[26]Narayanan A., Huey J., Felten E.W. (2016) A precautionary approach to big data privacy. In: Gutwirth A., Leenes R., De Hert P. (eds) Data Protection on the Move. Law, Governance and Technology Series, vol. 24. Springer, Dortrecht.

[27]Zuiderwijk A., Jeffrey K., Janssen M., (2012) The Potential of Metadata for Linked Open Data and its Value for Users and Publishers. JeDEM-Ejournal of democracy and Open Government, 4(2), 222-244

[28]Micah Altman, Alexandra Wood, Davi R O'Brien, Urs Gasser, Practical approaches to big data privacy over time, International Data Privacy Law, Volume 8, Issue 1, February 2018, pp. 29-51

[29]Konstantinos Angelopoulos, Vasiliki Diamantopoulou, Haralambos Mouratidis, Michalis Pavlidis, Mattia Salnitri, Paolo Giorgini, Jose F. Ruiz. 2017. A Holistic Approach for Privacy Protection in E-Government. In: Proceeding of the 12th International Conference on Availiability, Reliability and Security (ARES '17) Association for Computing Machinery, New York, NY, USA, Article 17, 1-10.

[30]Gerhard Steinke, Data Privacy Approaches from US and EU Perspectives. In: Telematics and Informatics, Vol. 19, Issue 2, 2002, pp 193-200

[21]Combe C. (2009) Observations on the UK transformational government strategy relative to citizen data sharing and privacy. In: Transforming Government: People, Process and Policy, vol. 3 no. 4, pp. 394-405. Emerald Group Publishing Limited

[32]Belanger F., Hiller J.S., (2016) A Framework for e-government: privacy implication. In: Business Process Management Journal, Vol. 12 No. 1, pp. 48-60. Emereld Group Publishing Limited

[33]Drogkaris P., Gritzalis A. (2015) A privacy preserving framework for big data in e-government environments. In: Fischer-Hubner, S. Lambrinoudakis, C. Lopez, J. (eds) Trust, Privacy and Security in Digital Business. TrustBus 2015. Lecture notes in computer science vo. 9264. Springer, Cham.

[34]Sarjito, A. (2024). Data security and privacy in the digital era: Challenges for modern government. JIAN (Jurnal Ilmiah Administrasi Negara), 8(3), 01-13

[35]Ira S. Rubinstein, Gregory T. Nojeim, Ronald D. Lee, Systematic government access to personal data: a comparative analysis. In: International Data Privacy Law, Volume 4, Issue 2, May 2014, pp. 96-119

[36]Simpson, Andrew C. 2011. On privacy and public data: a study of data.gov.uk. In: Journal of Privacy and Confidentiality 3 (1).

[37]Cullen, R. (2009), Culture, identity and information privacy in the age of digital government. In: Online Information Review, Vol. 33 No. 3, pp.405-421. Emerald Group Publishing Limited

[38]Huang, R., Huang, P., and Wen, L. (2025) Influencing factors of personal privacy protection in open government data: an interpretive structural modeling approach. In: Aslib Journal of Information Management, Vol. ahead of print No. ahead of print. Emerald Publishing Limited.

[39]S. Prabowo et al., Privacy -Preserving Tools and Technologies: Government Adoption and Challenges. In: IEEE Access, vol. 13, pp. 33904-33934, 2025

[40]Q.Tan and F. Pivot, Big Data Privacy: Changing Perception of Privacy, 2015 IEEE International Conference on Smart City/Social Com/SustainCom (Smart City), Chengdu, China, 2015, pp. 860-865

[41]Paola Vavriki and Maria Karyda, Big Data Analytics in e-government and e-democracy applications: privacy threats, implications and mitigation. In: International Journal of Electronic Governance, Vol. 14, No 1-2, pp. 58-82, May 2022

[42]Carter, L. and McBride, A. (2010), Information Privacy Concerns and e-Government: a Research agenda. In: Transforming Government: People, Process and Policy. Vol. 4 No 1, pp. 10-13. Emerald Group Publishing Limited.

[43]Yunjie Tang, Privacy protection framework for open data: Constructing and assessing an effective approach. In: Library and Information Science Research, Vol. 46, Issue 3, 2024.

War[44]er, Janice and Chun, Soon Ae, A citizen privacy protection model for e-government mashup services. 2008. Digital Government Society of North America.

[45]Davis, C.N. (2005). Reconciling Privacy and Access Interests in E-Government. In: International Journal of Public Administration, 28(7-8), 567-580

[46]Dasom Lee, David J. Hess, Data privacy and residential smart meters: Comparative analysis and harmonization potential. In: Utilities Policy, Elsevier, Vol. 70, 2021

[47]Chao Wu, Data Privacy: From transparency to fairness. In: Technology in society, vol. 76, 2024, 102457, Elsevier

[48]N. Azam, L. Michala, S. Ansari and N.B. Truong, Data privacy threat modelling for autonomous systems: A survey from the GDPR's perspective. In: IEEE Transactions on Big Data, vol. 9, no. 2, pp. 388-414, April 2023

[49]Davis, J.S., Osoba, O. Improving privacy preservation policy in the modern information age. In: Health Technol. 9, 65-75 (2019)

[50]Tore, D., Alferez, M., Soltana, G. et al. Modeling data protection and privacy: application and experience with GDPR. In: Softw Syst Model 20, 2071-2087 (2021).

[51]Quarati, A., Albertoni, R. Linked Open Government Data: Still a Viable Option for Sharing and Integrating Public Data? In: Future Internet 2024, 16, 99.

[52]Wieczorkowski, Jundefineddrzej. Barriers to using open government data. 2019In: Association for computing machinery, New York, NY, USA

[53]Sansonetti, G., Gasparetti, F., Micarelli, A. et al. Enhancing cultural recommendations through social and Linked Open Data. In: User Model User-Adap Inter 29, 121-159 (2019)

[54]Christina Tikkinen-Piri, Anna Rohuen, Jouni Markkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies. In: Computer Law and Security Review, vol. 34, issue 1, 2018, pp. 134-153

[55]Janis Wong, Tristan Henderson, The right to data portability in practice: exploring the implications of the technologically neutral GDPR. In: International Data Privacy Law, volume 9, issue 3, August 2019, pages 173-191

[56]Ali, Mohsan and Alexopoulos, Charalampos and Charalabidis, Yannis, A comprehensive review of open data platforms, prevalent technologies, and functionalities. 2022. In: Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance. Pp. 203-214. Association for Computing Machinery, New York, NY, USA

[57]Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Γενικός κανονισμός

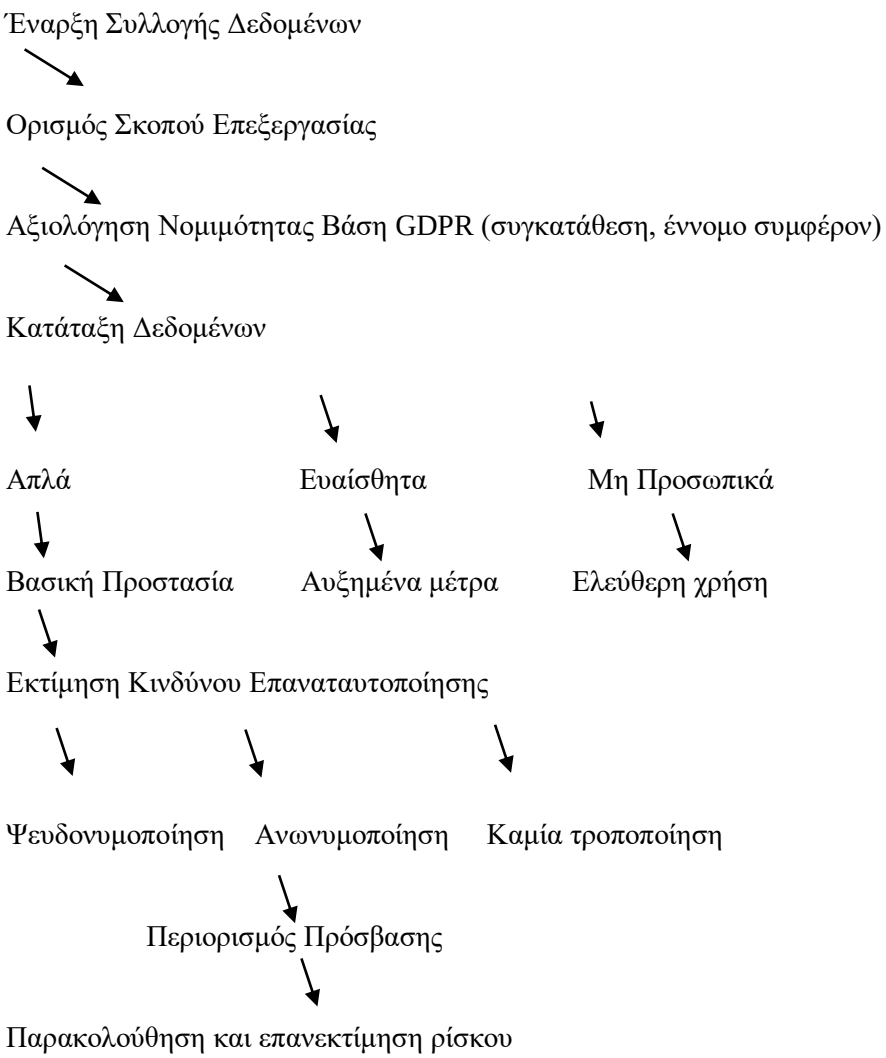
για την Προστασία Δεδομένων-GDPR). Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 119, 4.5.2016, σ. 1-88

[58]Νόμος 4624/2019, Εφαρμογή του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΕΕ) 2016/679 και ενσωμάτωση της Οδηγίας (ΕΕ) 2016/680. ΦΕΚ Α' 137/29.08.2019

[59]Νόμος 108/1981, Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για την προστασία των προσώπων έναντι της αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα. ΦΕΚ Α' 43/15.04.1981

[60]Νόμος 4624/2019, Κύρωση του Πρωτοκόλλου για την Τροποποίηση της Σύμβασης για την Προστασία των Προσώπων έναντι της Αυτοματοποιημένης Επεξεργασίας Προσωπικών Δεδομένων (Σύμβαση 108+). ΦΕΚ Α' 141/29.08.2019

Παράρτημα Ι ΒΑΣΙΚΟ ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ, ΔΙΑΧΕΙΡΙΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ



Παράρτημα ΙΙ ΕΠΕΞΗΓΗΣΕΙΣ ΒΑΣΙΚΩΝ ΒΗΜΑΤΩΝ ΑΣΦΑΛΟΥΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΔΗΜΟΣΙΕΥΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Ορισμός σκοπού. Σύμφωνα με την αρχή του σκοπού, τα δεδομένα συλλέγονται για συγκεκριμένο, ρητό και νόμιμο σκοπό.

Κατάταξη δεδομένων. Τα δεδομένα αξιολογούνται ως απλά, ευαίσθητα ή μη προσωπικά για την κατάλληλη εφαρμογή προστασίας.

Ψευδονυμοποίηση. Μειώνει τον κίνδυνο ταυτοποίησης χωρίς να αφαιρεί πλήρως τη δυνατότητα επανασυσχέτισης.

Ανωνυμοποίηση. Πλήρης αποσύνδεση των δεδομένων από την ταυτότητα του προσώπου. Χρήσιμη για ανοιχτά δεδομένα.

Επανεκτίμηση ρίσκου. Απαιτείται περιοδικός έλεγχος για τυχόν νέες απειλές ή μεταβολές στην τεχνολογία.

Παράρτημα ΙΙΙ ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ. ΝΟΜΙΜΗ ΧΡΗΣΗ RTLD ΜΕ ΒΑΣΗ ΤΟΝ GDPR