ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

COVID-19: Το ζήτημα της ιχνηλάτησης επαφών και ο ρόλος των εφαρμογών στον περιορισμό της εξάπλωσης του ιού.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Μαρίας Καργάκη

Επιβλέπουσα: Μήτρου Ευαγγελία

Σάμος, 7 Ιουνίου, 2021

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο του 10ου εξαμήνου του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου στην Σάμο. Η ενασχόληση χρονολογείται στην διάρκεια του ακαδημαϊκού έτους 2020-2021 με ημερομηνία αφετηρίας της τον Οκτώβριο.

Θα ήθελα να ευχαριστήσω ιδιαίτερα την επιβλέπουσα καθηγήτρια, κυρία Μήτρου Ευαγγελία που με τις συμβουλές της και την καθοδήγηση της, συνέβαλε στην περάτωση της εργασίας αυτής.

Καργάκη Μαρία

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

Λίστα Εικόνων

Λίστα Πινάκων

.

Περίληψη

Η παρούσα εργασία επικεντρώνεται στον περιορισμό της εξάπλωσης του COVID-19, μέσα από εφαρμογές ιχνηλάτησης επαφών, με την εφαρμογή των νομικών βάσεων για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Γίνεται αναφορά των επιφυλάξεων που υπάρχουν για την χρήση εφαρμογών ιχνηλάτησης επαφών, αναλύονται διεξοδικά, οι τεχνολογίες που χρησιμοποιούνται για την καταπολέμηση του COVID-19 και γίνεται σύγκριση μεταξύ τους. Γίνεται περιγραφή των αρχιτεκτονικών των συστημάτων, αλλά και κατηγοριοποίηση των πρωτοκόλλων, ανάλογα με το είδος της προσέγγισης, κεντρικής και αποκεντρωμένης.

Επίσης, παρέχεται εκτενής ανάλυση, σε νέες τεχνολογίες οι οποίες μπορούν να συμβάλλουν στην βελτίωση της COVID-19 εποχής. Τέλος, γίνεται ανάλυση των εφαρμογών παρακολούθησης επαφών που υπάρχουν μέχρι στιγμής στην ΕΕ με στόχο των περιορισμό της εξάπλωσης, επισημαίνοντας κυρίως τα δικαιώματα πρόσβασης ανά εφαρμογή.

1

Εισαγωγή

1.1 Το ζήτημα της ιχνηλάτησης επαφών και ο ρόλος των εφαρμογών στον περιορισμό της εξάπλωσης του ιού.

Η παρούσα εργασία επικεντρώνεται στον περιορισμό της εξάπλωσης του COVID-19, μέσα από εφαρμογές ιχνηλάτησης επαφών, με την εφαρμογή ωστόσο, των νομικών βάσεων για την επεξεργασία τόσο των γενικών, όσο και των ειδικών δεδομένων των ατόμων.

1.2 Αντικείμενο διπλωματικής

Αντικείμενο της παρούσας διπλωματικής εργασίας είναι ο περιορισμός της εξάπλωσης του COVID-19, με την βοήθεια εφαρμογών ιχνηλάτησης επαφών. Όσον αφορά την ιχνηλάτηση των επαφών, γίνεται διαχωρισμός στην ιχνηλάτηση των επαφών σε χώρες εντός, αλλά και εκτός της Ευρωπαϊκής Ένωσης. Σχετικά με τον περιορισμό της εξάπλωσης του ιού μέσω εφαρμογών ιχνηλάτησης επαφών, αναφέρονται οι επιφυλάξεις που υπάρχουν για τις νέες αυτές τεχνολογίες που καλούμαστε να χρησιμοποιήσουμε, τις απαιτήσεις που είναι απαραίτητο να ανταποκρίνονται οι εφαρμογές και το πως τελικά οι εφαρμογές αυτές λειτουργούν.

1.3 Δομή της διπλωματικής

Η παρούσα διπλωματική εργασία αποτελείται από έντεκα ενότητες, στη δεύτερη ενότητα αναλύονται οι πράξεις νομοθετικού περιεχομένου στην Ελλάδα που έχει προκαλέσει η πανδημία στην ιδιωτική ζωή των ατόμων, μέσω της παραπληροφόρησης. Στην τρίτη ενότητα προσφέρεται μια πλήρης αναφορά, στο ζήτημα της επεξεργασίας των δεδομένων των χρηστών και παρέχονται οι νομικές

βάσεις για ειδικά και γενικά δεδομένα, καθώς και οι βασικές αρχές και οι περιπτώσεις επεξεργασίας των δεδομένων υγείας.

Στην τέταρτη ενότητα αναφέρεται η ιχνηλάτηση των επαφών και στην πέμπτη αναλύονται διεξοδικά, οι τεχνολογίες που χρησιμοποιούνται για την καταπολέμηση του COVID-19 και γίνεται σύγκριση μεταξύ τους. Στην έκτη ενότητα γίνεται περιγραφή των αρχιτεκτονικών των συστημάτων, αλλά και κατηγοριοποίηση των πρωτοκόλλων, ανάλογα με το είδος της προσέγγισης, κεντρικής και αποκεντρωμένης. Ενώ στην έβδομη, αναλύονται νέες τεχνολογίες οι οποίες μπορούν να συμβάλλουν στον περιορισμό της εξάπλωσης του COVID-19. Επιπλέον στην όγδοη ενότητα περιγράφονται οι εφαρμογές που βασίζονται στο 5G, με σκοπό της πρόληψη από τον COVID-19. Στην ένατη ενότητα αναλύονται διεξοδικά, όλες οι εφαρμογές ιχνηλάτησης επαφών που υπάρχουν μέχρι στιγμής στην ΕΕ. Στην ενότητα 10 αναφέρονται οι παράγοντες που επηρεάζουν την κοινωνική αποδοχή των εφαρμογών, οι κίνδυνοι – προκλήσεις που καλούνται να αντιμετωπίσουν τα άτομα και τέλος, στην τελευταία ενότητα παρουσιάζονται τα συμπεράσματα που προκύπτουν από την έρευνα αυτή

2

Πραξεις Νομοθετικου Περιεχομενου Στην Ελλαδα Για Το Ξεσπασμα Του Covid - 19

2.1 Οι τρείς πράξεις

Τα κατεπείγοντα μέτρα ελήφθησαν από την ελληνική κυβέρνηση και τις δημόσιες αρχές, για την αποφυγή και τον περιορισμό του κορωνοϊού, με τη μορφή Πράξεων Νομοθετικού Περιεχομένου, οι τέσσερις αυτές πράξεις καθορίζονται από πολλές υπουργικές αποφάσεις και εγκυκλίους.

2.1.1 Πρώτη πράξη Νομοθετικού Περιεχομένου

Η πρώτη πράξη νομοθετικού περιεχομένου, η οποία εκδόθηκε στις 25 Φεβρουαρίου 2020 (ΦΕΚ Α' 42/25-02-2020) και σχετίζεται με την υιοθέτηση μέτρων από την ελληνική κυβέρνηση και τις δημόσιες αρχές, για την αποφυγή εμφάνισης ή και διάδοσης του κορωνοϊού. Πιο συγκεκριμένα, η παρούσα πράξη εστιάζει σε προληπτικά μέτρα, υγειονομικής παρακολούθησης, όπως ιατρικοί έλεγχοι, καθώς και μέτρα περιορισμού της εξάπλωσης της νόσου, όπως είναι το κλείσιμο δημόσιων χώρων και αναστολή των καλλιτεχνικών και αθλητικών εκδηλώσεων (Πράξη Νομοθετικού Περιεχομένου της 25.02.2020 Κατεπείγοντα μέτρα αποφυγής και περιορισμού της διάδοσης κορωνοϊού., 2020).

Σύμφωνα με το πρώτο άρθρο, της πράξης νομοθετικού περιεχομένου της 25^{ης} Φεβρουαρίου 2020, τα μέτρα για την πρόληψη και τον περιορισμό της διάδοσης της νόσου συνίστανται:

1. Στην υποχρεωτική υποβολή σε κλινικό και εργαστηριακό ιατρικό έλεγχο, υγειονομική παρακολούθηση, εμβολιασμό, φαρμακευτική αγωγή και νοσηλεία προσώπων, για τα οποία υπάρχουν εύλογες υπόνοιες ότι μπορεί να μεταδώσουν άμεσα ή έμμεσα τη νόσο.
2. Στην επιβολή κλινικών και εργαστηριακών ιατρικών ελέγχων, καθώς και μέτρων προληπτικής υγειονομικής παρακολούθησης, εμβολιασμού, φαρμακευτικής αγωγής και προληπτικής νοσηλείας προσώπων που προέρχονται από περιοχές όπου έχει παρατηρηθεί μεγάλη διάδοση της νόσου,
3. στην επιβολή προληπτικών ελέγχων υγειονομικής φύσεως και κλινικών ή εργαστηριακών ελέγχων σε όλα ή επιμέρους σημεία εισόδου και εξόδου από τη χώρα μέσω αεροπορικών, θαλάσσιων, σιδηροδρομικών ή και οδικών συνδέσεων με χώρες μεγάλης διάδοσης της νόσου,
4. στον προσωρινό περιορισμό, εν όλω ή εν μέρει, των αεροπορικών, θαλάσσιων, σιδηροδρομικών ή και οδικών συνδέσεων με χώρες μεγάλης διάδοσης της νόσου,
5. στον προσωρινό περιορισμό προσώπων των περιπτώσεων (α) και (β) υπό συνθήκες που αποτρέπουν την επαφή με τρίτα πρόσωπα, από την οποία θα μπορούσε να προκληθεί μετάδοση της νόσου. Το μέτρο του προσωρινού περιορισμού δύναται να υλοποιείται σε κατάλληλο χώρο νοσοκομείου, υγειονομικής δομής, θεραπευτικού ιδρύματος, σε κατάλληλες δημόσιες ή ιδιωτικές εγκαταστάσεις προσωρινής διαμονής, ή και κατ' οίκον, ανάλογα με την απόφαση του αρμόδιου κάθε φορά οργάνου,
6. στην προσωρινή απαγόρευση της λειτουργίας σχολικών μονάδων και πάσης φύσεως εκπαιδευτικών δομών, φορέων και ιδρυμάτων, δημοσίων και ιδιωτικών, κάθε τύπου και βαθμού, χώρων θρησκευτικής λατρείας, καθώς και στην προσωρινή απαγόρευση και αναστολή μετακινήσεων για οποιονδήποτε λόγο του εκπαιδευτικού και λοιπού προσωπικού και μαθητών, σπουδαστών, φοιτητών οποιωνδήποτε εκ των ανωτέρω σχολικών μονάδων, εκπαιδευτικών δομών, φορέων και ιδρυμάτων,
7. στην προσωρινή απαγόρευση της λειτουργίας θεάτρων, κινηματογράφων, χώρων αθλητικών και καλλιτεχνικών εκδηλώσεων, αρχαιολογικών χώρων και μουσείων, καταστημάτων υγειονομικού ενδιαφέροντος, ιδιωτικών επιχειρήσεων, δημόσιων υπηρεσιών και οργανισμών, καθώς και γενικά χώρων συνάθροισης κοινού,
8. στην προσωρινή επιβολή μέτρων περιορισμού της κυκλοφορίας μέσων μεταφοράς εντός της επικράτειας,
9. στην προσωρινή επιβολή περιορισμού κατ'οίκον σε ομάδες προσώπων προς αποφυγή ενεργειών που θα μπορούσαν να προκαλέσουν τη διάδοση της νόσου. Το μέτρο του προσωρινού περιορισμού ευρύτερων ομάδων προσώπων δύναται να προσδιορίζεται με αναφορά σε συγκεκριμένες γεωγραφικές περιοχές. Στα πρόσωπα της περίπτωσης αυτής

δύνανται να επιβάλλονται και τα υπό περιπτώσεις (α) και (β) μέτρα (Πράξη Νομοθετικού Περιεχομένου της 25.02.2020 Κατεπείγοντα μέτρα αποφυγής και περιορισμού της διάδοσης κορωνοϊού., 2020).

Ύστερα από την επιβολή της πράξης αυτής, το Υπουργείο Παιδείας και Θρησκευμάτων, προχώρησε στο κλείσιμο όλων των εκπαιδευτικών ιδρυμάτων, έως τις 24 Μαρτίου 2020. Σύμφωνα με την Πράξη Νομοθετικού Περιεχομένου στις 25.02.2020 για τα κατεπείγοντα μέτρα αποφυγής και περιορισμού της διάδοσης κορωνοϊού και τις κοινές Υπουργικές Αποφάσεις: ΦΕΚ 855/Β/13-3-2020 (Επιβολή του μέτρου της προσωρινής απαγόρευσης λειτουργίας επιμέρους ιδιωτικών επιχειρήσεων, μουσείων, αρχαιολογικών και ιστορικών χώρων, αθλητικών εγκαταστάσεων, καθώς και γενικά χώρων συνάθροισης κοινού, στο σύνολο της Επικράτειας, για το χρονικό διάστημα από 14.3.2020 έως και 27.3.2020.), 18152/2020 - ΦΕΚ 857/Β/14-3-2020 (Επιβολή του μέτρου της προσωρινής απαγόρευσης λειτουργίας εποχικών τουριστικών καταλυμάτων από 15.3.2020 έως και 30.4.2020.), ΦΕΚ 915/Β/17-3-2020 (Επιβολή του μέτρου της προσωρινής απαγόρευσης λειτουργίας ιδιωτικών επιχειρήσεων, στο σύνολο της Επικράτειας, για το χρονικό διάστημα από 18.3.2020 έως και 31.3.2020, προς περιορισμό της διασποράς του κορωνοϊού COVID-19.) και την εγκύκλιο 5/2020/18-3-2020, εκδόθηκαν με εντολή του αποτελεσματικού οριζόντιου κλεισίματος όλων των λιανικών επιχειρήσεων, εστιατορίων, καφέ μπαρ, κινηματογράφων, θεάτρων, γυμναστήρια, μουσεία, εστίαση και τουριστικές επιχειρήσεις έως τις 31 Μαρτίου 2020. Το ίδιο μέτρο επιβάλλεται για τις επιχειρήσεις τουριστικών καταλυμάτων έως τις 30 Απριλίου 2020. Επιτρέπεται στις επιχειρήσεις τροφοδοσίας και λιανικής να διατηρούν υπηρεσίες delivery και take away.

2.1.2 Δεύτερη Πράξη Νομοθετικού Περιεχομένου

Η Δεύτερη Πράξη Νομοθετικού Περιεχομένου (ΦΕΚ Α' 55/11-03-2020), η οποία δημοσιοποιήθηκε στις 11 Μαρτίου 2020 και στην οποία αναφέρονται τα κατεπείγοντα μέτρα για την αντιμετώπιση των αρνητικών συνεπειών εμφάνισης του κορωνοϊού COVID -19 και της ανάγκης περιορισμού της διάδοσης του. Στη συγκεκριμένη πράξη, προβλέπονται μέτρα τα οποία σχετίζονται με παράταση προθεσμιών για αποπληρωμή τόσο σε φορολογούμενος, όσο και σε επιχειρήσεις και αναστολή υποχρεώσεων αποπληρωμής του χρέους. Ως προς την αγορά εργασίας, λήφθησαν μέτρα τα οποία σχετίζονται με αναστολή της υποχρέωσης του εργοδότη να καταχωρεί στο Πληροφοριακό Σύστημα «ΕΡΓΑΝΗ» αλλαγές ή τροποποιήσεις στα προγράμματα των εργαζομένων, με άδειες ειδικού σκοπού για τους εργαζομένους οι οποίοι είναι γονείς και με δυνατότητα εξ αποστάσεως εργασίας, κυρίως σε άτομα που ανήκουν σε ευπαθείς ομάδες κατόπιν

αιτήματος τους. Επιπλέον, προβλέπονται μέτρα για υποχρέωση τόσο των ραδιοφωνικών όσο και των τηλεοπτικών σταθμών να μεταδίδουν ενημερωτικά μηνύματα διάρκειας ενός λεπτού για την αποφυγή της διασποράς του κορωνοϊού COVID-19 (11.03.2020, 2020).

2.1.3 Τρίτη Πράξη Νομοθετικού Περιεχομένου

Η Τρίτη Πράξη Νομοθετικού Περιεχομένου (ΦΕΚ Α' 64/14-03-2020) η οποία εκδόθηκε στις 14 Μαρτίου 2020, περιέχει επιπρόσθετα μέτρα αντιμετώπισης της ανάγκης περιορισμού της διασποράς του κορωνοϊού COVID – 19. Η συγκεκριμένη πράξη αποτελείται από 32 άρθρα, από τα οποία τα πιο σημαντικά που αξίζει να αναφερθούν είναι τα ακόλουθα

Αρχικά, είναι απαραίτητο τόσο τα supermarkets όσο και τα φαρμακεία, τα οποία προμηθεύουν το κοινό με προϊόντα υγιεινής και αντισηπτικών, να ενημερώνουν σχετικά με το απόθεμα, στην αρμόδια αρχή. Ωστόσο, η μη υποβολή ή υποβολή ανακριβούς δήλωσης, έχεις ως αποτέλεσμα την επιβολή κατάλληλων κυρώσεων (forin.gr, 2020):

1. κατάσχεση των ειδών (χειρουργικές μάσκες, αντισηπτικά διαλύματα και αντισηπτικά μαντηλάκια), στο μέτρο που δεν έχουν δηλωθεί ή έχουν δηλωθεί ανακριβώς και
2. διοικητικό πρόστιμο ύψους από χίλια (1.000) έως εκατό χιλιάδες (100.000) ευρώ, ανάλογα με τη βαρύτητα της παράβασης.

Επίσης, στο άρθρο 13 παράγραφος 1, σχετικά με τον μηχανισμό στήριξης των εργαζομένων, θεσπίζεται ένας μηχανισμός «ανακούφισης», στον οποίο περιλαμβάνεται αποζημίωση 800 ευρώ σε εργαζόμενους, που εργάζονται σε επιχειρήσεις που ανέστειλαν την λειτουργία τους. Ωστόσο, οι εργαζόμενοι που συνεχίζουν να εργάζονται μέσω τήλε εργασίας, ή βρίσκονταν ήδη σε κάποια άδεια, όπως είναι η άδεια μητρότητας, δεν λαμβάνουν την αποζημίωση που δίνεται από τον μηχανισμό στήριξης (Πράξη Νομοθετικού Περιεχομένου της 14.03.2020 Κατεπείγοντα μέτρα αντιμετώπισης της ανάγκης περιορισμού της διασποράς του κορωνοϊού COVID-19, 2020).

2.1.4 Τέταρτη Πράξη Νομοθετικού Περιεχομένου

Η Τέταρτη Πράξη Νομοθετικού Περιεχομένου (ΦΕΚ Α' 75/30-03-2020) η οποία εκδόθηκε στις 30 Μαρτίου 2020, περιέχει μέτρα αντιμετώπισης της πανδημίας του κορωνοϊού COVID – 19 και άλλες κατεπείγουσες διατάξεις. Η συγκεκριμένη πράξη αποτελείται από 39 άρθρα, τα οποία χωρίζονται σε 14 μέρη. Τα μέτρα αυτά πάρθηκαν, για την αντιμετώπιση της πανδημίας, ούτως ώστε να περιοριστούν τα προβλήματα που δημιουργήθηκαν στην οικονομία και στην αγορά εργασίας. Επίσης, στα μέτρα αυτά αναφέρεται η αγορά αγαθών πρώτης ανάγκης και η ενίσχυση του Εθνικού Συστήματος Υγείας, ώστε να αντιμετωπιστούν τα πιθανά κρούσματα κορωνοϊού

COVID - 19. Οι διατάξεις αυτές, αφορούν τις διατάξεις αρμοδιότητας του κάθε υπουργείου, όπως για παράδειγμα του υπουργείο οικονομικών, με μέτρα που αφορούν παράταση και αναστολή προθεσμιών ή και ρύθμιση τους, εκπτώσεις για δόσεις βεβαιωμένων οφειλών επιχειρήσεων και ενίσχυση προσωπικού νοσοκομείων ή του υπουργείου ανάπτυξης και επενδύσεων, με μέτρα αναφορικά με την λειτουργία υπεραγορών και λαϊκών αγορών και την υιοθέτηση επιπλέον μέτρων για την εξασφάλιση της επάρκειας μέσων ατομικής προστασίας και προσωπικής υγιεινής. Ωστόσο, υπάρχουν επιπρόσθετες διατάξεις και από άλλα υπουργεία, όπως είναι το υπουργείο υγείας, το υπουργείο ψηφιακής διακυβέρνησης (δυνατότητα τηλεδιάσκεψης), υπουργεία εσωτερικών, μετανάστευσης και ασύλου και προστασίας του πολίτη, καθώς και όλων των υπόλοιπων υπουργείων (διατάξεις., 2020).

2.2 Ελεύθερη Κυκλοφορία

Σύμφωνα με την κατάσταση της κάθε περιοχής και ανάλογα με τα κρούσματα που παρουσιάζονται καθημερινά, υπάρχει περίπτωση επιβολής προσωρινών μέτρων καραντίνας, τα οποία μπορούν να επιβληθούν σε άτομα ή ομάδες ατόμων. Τα μέτρα που εφαρμόζονται θα πρέπει πάντα να συνάδουν με την αρχή της αναλογικότητας και το κράτος δικαίου. Με βάση την αρχή της αναλογικότητας (Τσιλιώτης, 2020), οι περιορισμοί που επιβάλλονται από το κράτος (απαγόρευση της κυκλοφορίας) θα πρέπει να είναι κατάλληλοι, αναγκαίοι και αναλογικοί για την επίτευξη αυτού σκοπού (τον περιορισμό της εξάπλωσης του κορωνοϊού), για τον λόγο αυτό, επιβλήθηκε καθολικό lockdown σε ολόκληρη την ελληνική επικράτεια, για τον περιορισμό της εξάπλωσης του ιού. Ο σκοπός επιβολής ενός τέτοιου μέτρου, εξυπηρετεί την προστασία των θεμελιωδών δικαιωμάτων των πολιτών.

Ο οριζόντιος προσωρινός περιορισμός της κυκλοφορίας επιβλήθηκε για πρώτη φορά στις 22 Μαρτίου 2020 έως τις 5 Απριλίου 2020 και για δεύτερη φορά από τις 7 Νοεμβρίου 2020 έως και τις 30 Νοεμβρίου του 2020 με κοινή υπουργική απόφαση για τους κατοίκους ολόκληρης της ελληνικής επικράτειας, ωστόσο στο δεύτερο περιορισμό της κυκλοφορίας, η Σάμος λόγω σεισμού εξαιρείται από τους περιορισμούς στις μετακινήσεις. Ο περιορισμός της κυκλοφορίας επιβλήθηκε ως μέτρο πρόληψης, ούτως ώστε να μειωθεί ο κίνδυνος διασποράς του κορωνοϊού COVID – 19.

Ωστόσο, με την απαγόρευση οποιασδήποτε μορφής κυκλοφορίας, είναι απαραίτητη η χορήγηση ειδικής άδειας για συγκεκριμένους σκοπούς. Πιο συγκεκριμένα, είναι απαραίτητη η άδεια μετακίνησης, για μετάβαση από και προς την εργασία για τις εργάσιμες και μόνο ώρες, όπου απαιτείται βεβαίωση τύπου Α, η οποία χορηγείται είτε μέσω του Πληροφοριακού Συστήματος ΕΡΓΑΝΗ ή συμπληρώνοντας το έντυπο «Βεβαίωση Κυκλοφορίας Εργαζομένου» .Στην πρώτη

περίπτωση, η βεβαίωση έχει ισχύ 14 ημέρες, ενώ στην δεύτερη περίπτωση έχει πάγια ισχύ. Σε περίπτωση δήλωσης ψευδών στοιχείων, επιβάλλεται διοικητικό πρόστιμο ύψους 300 ευρώ στον εργαζόμενο/η και 500 ευρώ στον εργοδότη.

Οι μετακινήσεις τύπου Β, αφορούν μεμονωμένες μετακινήσεις και υπάρχουν τρεις επιλογές επιβεβαίωσης: SMS στο 13033, εκτυπωμένο και συμπληρωμένο έντυπο βεβαίωσης κίνησης, ή και χειρόγραφη βεβαίωση κίνησης. Οι μετακινήσεις αφορούν μόνο τις παρακάτω μεταβάσεις, για μετάβαση σε φαρμακείο ή επίσκεψη σε γιατρό, μετάβαση σε καταστήματα αγαθών πρώτης ανάγκης, μετάβαση σε δημόσια υπηρεσία ή τράπεζα, μετάβαση για παροχή βοήθειας σε ανθρώπους, μετάβαση σε τελετή κηδείας υπό τους όρους που προβλέπει ο νόμος, καθώς και σε περιπτώσεις σωματικής άσκησης ή κίνησης με κατοικίδιο ζώο, ατομικά ή ανά τρία άτομα, τηρώντας ωστόσο στην τελευταία περίπτωση την αναγκαία απόσταση του 1,5 μέτρου.

Τέλος, ειδική άδεια χορηγείται και στις μετακινήσεις των μαθητών (στο δεύτερο lockdown), σε οποιαδήποτε άλλη περίπτωση, η οποία δεν αφορά την υγεία κάποιου προσώπου απαγορεύεται η κυκλοφορία.

2.3 Επιπτώσεις στην ιδιωτική ζωή και διάδοση παραπληροφόρησης

Στο άρθρο 5 στην Πράξη Νομοθετικού Περιεχομένου της 14 Μαρτίου 2020, για τα κατεπείγοντα μέτρα αντιμετώπισης της ανάγκης περιορισμού της διασποράς του κορωνοϊού COVID – 19, αναφέρει τα έκτακτα μέτρα ιχνηλάτησης των κρουσμάτων και πιο συγκεκριμένα επιβάλλει τη συλλογή των προσωπικών δεδομένων δυνητικά ή πραγματικά μολυσμένων ατόμων από τον Εθνικό Οργανισμό Υγείας (Ε.Ο.Δ.Υ.) και την παροχή τους στη Γενική Γραμματεία Πολιτικής Προστασίας (Γ.Γ.Π.Π.).

Σκοπός της συγκεκριμένης επεξεργασίας είναι η επιχειρησιακή προετοιμασία και ο συντονισμός μεταξύ του Ε.Ο.Δ.Υ. και της Γ.Γ.Π.Π. για την αντιμετώπιση των συνεπειών του κορωνοϊού COVID-19 και την καταγραφή της διασποράς των κρουσμάτων για λόγους προστασίας της δημόσιας υγείας.

Τα δεδομένα που δίνονται (ονοματεπώνυμο, φύλο, ηλικία, τηλέφωνο επικοινωνίας, ακριβή διεύθυνση κατοικίας, εισαγωγή ή μη σε νοσοκομείο, νοσοκομείο εισαγωγής και διεύθυνση προσωρινού περιορισμού, αν δεν είναι ίδια με τη διεύθυνση κατοικίας), είναι ψευδωνυμοποιημένα και σε περίπτωση που κριθεί απαραίτητη η επικοινωνία με τα υποκείμενα, μπορεί να αρθεί η ψευδωνυμοποίηση. Στην περίπτωση ψευδωνυμοποίησης (άρθρο 4 στοιχείο 5) των δεδομένων, τα δεδομένα προσωπικού χαρακτήρα δεν μπορούν να αποδοθούν σε συγκεκριμένο υποκείμενο, χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι συμπληρωματικές πληροφορίες

διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα, προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (δηλαδή πολίτες που νοσούν από COVID – 19).

Σύμφωνα με το Άρθρο 5 παράγραφο 2 της πράξης ΦΕΚ Α '64 / 14-3-2020 για τη διαφύλαξη των συμφερόντων των υποκειμένων λαμβάνονται, κατ΄ ελάχιστον, τα παρακάτω μέτρα:

1. Η πρόσβαση στα δεδομένα και η επεξεργασία επιτρέπεται μόνο με χρήση καταλλήλων διαπιστευτηρίων από προσωπικό που διαθέτει τις κατάλληλες εξουσιοδοτήσεις.
2. Οι διαβιβάσεις των δεδομένων μεταξύ Ε.Ο.Δ.Υ. και Γ.Γ.Π.Π. πραγματοποιούνται με κρυπτογράφηση.
3. Τηρούνται επικαιροποιημένα αρχεία καταγραφής των ενεργειών που εκτελούνται σε προσωπικά δεδομένα. Στα αρχεία αυτά καταγράφονται το όνομα χρήστη και ο χρόνος συμβάντος, καθώς και οι ακόλουθες τουλάχιστον ενέργειες: εισαγωγή, πρόσβαση, εξαγωγή, τροποποίηση και διαγραφή προσωπικών δεδομένων.
4. Ενημερώνεται και ευαισθητοποιείται το προσωπικό που ασχολείται με τη συγκεκριμένη επεξεργασία.

Τα δεδομένα τηρούνται από τη Γ.Γ.Π.Π. έως και έναν (1) μήνα μετά από τη λήξη της περιόδου εφαρμογής των κατεπειγόντων μέτρων για την αποφυγή της διασποράς του κορωνοϊού COVID-19 και πάντως όχι πέραν της 31ης Δεκεμβρίου 2020. Μετά από την πάροδο του χρόνου αυτού, τα δεδομένα μπορεί να ανωνυμοποιηθούν για σκοπούς έρευνας και καλύτερης οργάνωσης του συστήματος πολιτικής προστασίας.

Το γραφείο τύπου δημοσίευσε συγκεκριμένες οδηγίες σχετικά με ζητήματα προστασίας δεδομένων, όσον αφορά τον κορωνοϊό COVID – 19. Μέχρι και σήμερα, τα μόνα στοιχεία που αναφέρθηκαν στα ΜΜΕ, ήταν του πρώτου νεκρού από κορωνοϊό, πιο αναλυτικά, αναφέρθηκε το όνομα, η ηλικία και τα προσωπικά του στοιχεία, όπως οικογενειακή κατάσταση και φωτογραφίες. Οι πληροφορίες που δημοσιεύονται θα πρέπει να περιορίζονται στα απολύτως απαραίτητα στοιχεία δημογραφικού και στατιστικού χαρακτήρα. Τα μόνα δηλαδή στοιχεία τα οποία μπορούν να αποκαλυφθούν είναι η ηλικία, το φύλο και ο τόπος μόνιμης κατοικίας των ασθενών ή των νεκρών ατόμων, ούτως ώστε να μην υπάρξει κοινωνικός στιγματισμός ή αποκλεισμός των νοσούντων ή ακόμα και αυτών που περιθάλπουν και φροντίζουν τους ασθενείς.

Κρίνεται απαραίτητη η ενημέρωση των πολιτών από τα ΜΜΕ και η αποφυγή διάδοσης ψευδών στοιχείων από τα ΜΜΕ. Είναι απαραίτητη η ύπαρξη διαφάνειας και ο περιορισμός των ψευδών ειδήσεων «fake news», για τον αριθμό αλλά και τα στοιχεία των νοσούντων, ούτως ώστε να αποφευχθεί ο πανικός που ενδεχομένως προκύψει. Για τον σκοπό αυτό, είναι απαραίτητη η

παρέμβαση του Εθνικού Συμβουλίου Ραδιοτηλεόρασης, όταν τα ΜΜΕ υπερβαίνουν βασικούς κανόνες δεοντολογίας. Σύμφωνα με το Άρθρο 15 παράγραφος 2 του Συντάγματος, τονίζεται η αντικειμενική μετάδοση πληροφοριών και ειδήσεων, με σεβασμό στην αξία του ανθρώπου.

3

COVID-19 και Επεξεργασία Δεδομένων

3.1 Το ζήτημα της επεξεργασίας

Τα δεδομένα προσωπικού χαρακτήρα διακρίνονται σε δύο κατηγορίες, στα απλά και στα ευαίσθητα προσωπικά δεδομένα. Τα δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποίσιμο εν ζωή άτομο. Ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

Στις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα (ευαίσθητα δεδομένα), ανήκει κάθε πληροφορία που αφορά στη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν στην υγεία ή δεδομένων που αφορούν στη σεξουαλική ζωή φυσικού προσώπου ή στον γενετήσιο προσανατολισμό προσωπικού χαρακτήρα. Στα ευαίσθητα προσωπικά δεδομένα, ανήκουν και τα δεδομένα τα οποία αφορούν την υγεία του υποκειμένου. Δεδομένα προσωπικού χαρακτήρα δηλαδή, που σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του

Τα προσωπικά δεδομένα τα οποία συλλέγονται από τους ασθενείς που νοσούν από κορωνοϊο COVID – 19, ανήκουν και στις δύο κατηγορίες δεδομένων, που αναφέρθηκαν παραπάνω. Τα δεδομένα που δίνονται από τους ασθενείς, όπως το ονοματεπώνυμο, η ηλικία του ασθενούς, το τηλέφωνο επικοινωνίας, η διεύθυνση μόνιμης κατοικίας και η οικογενειακή κατάσταση, αποτελούν απλά δεδομένα προσωπικού χαρακτήρα. Αλλά τα δεδομένα που σχετίζονται με τα συμπτώματα που εμφανίζουν οι ασθενείς, το ιατρικό ιστορικό τους, την φαρμακευτική περίθαλψη, την πιθανή εισαγωγή τους στο νοσοκομείο, όπως και κάθε άλλη πληροφορία που ορίζεται από το Άρθρο 4 παράγραφος 1 του ΓΚΠΔ και αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»), αποτελούν ευαίσθητα προσωπικά δεδομένα.

Σύμφωνα με το Άρθρο 4 παράγραφος 2, του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ, Άρθρο 4 παράγραφος 7), η επεξεργασία δεδομένων ορίζεται ως κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή[1]. Συνεπώς, το δικαίωμα της προστασίας προσωπικών δεδομένων δεν είναι απόλυτο και θα πρέπει να συνεκτιμάται με άλλα θεμελιώδη δικαιώματα, όπως είναι η ζωή και η υγεία.

3.2 Νομικές Βάσεις για ειδικά και γενικά δεδομένα

Υπάρχουν οι νομιμοποιητικές αρχές σύμφωνα με το Άρθρο 6 παράγραφο 1 του ΓΚΠΔ και είναι απαραίτητο να εφαρμόζεται τουλάχιστον μία εξ αυτών στην επεξεργασία προσωπικών δεδομένων. Οι νόμιμες βάσεις είναι οι ακόλουθες:

- Συγκατάθεση του υποκειμένου·
- Ανάγκη εκτέλεσης σύμβασης του ασθενούς με τον γιατρό·
- Ανάγκη συμμορφώσεως με την έννομη υποχρέωση του ιατρού να μεριμνά για την κατάλληλη ιατροφαρμακευτική φροντίδα του ασθενούς του.
- Διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.
- Εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον από το γιατρό·

[1] ΚΑΝΟΝΙΣΜΌΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΎ ΚΟΙΝΟΒΟΥΛΊΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΊΟΥ της 27ης Απριλίου 2016. Άρθρο 4 παράγραφος 2. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679#d1e1488-1-1

Η επεξεργασία είναι αναγκαία για τους σκοπούς των έννομων συμφερόντων που επιδιώκει είτε ο υπεύθυνος επεξεργασίας είτε κάποιος τρίτος. Υπεύθυνος επεξεργασίας όπως ορίζεται στον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ), είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

Όταν πρόκειται για ευαίσθητα προσωπικά δεδομένα, όπως είναι τα δεδομένα υγείας, με σκοπό τη διάγνωση, τον περιορισμό της εξάπλωσης και την θεραπεία από τον κορωνοϊό COVID - 19, είναι απαραίτητη η εφαρμογή τουλάχιστον μίας από τις ακόλουθες νόμιμες βάσεις επεξεργασίας, που ορίζονται στο Άρθρο 9 παράγραφος 2 του ΓΚΠΔ: στην συγκατάθεση του υποκειμένου, στην προστασία των ζωτικών συμφερόντων του υποκειμένου του υποκειμένου των δεδομένων, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί, την κοινοποίηση των δεδομένων υγείας από το υποκείμενο των δεδομένων σε κάποιο γιατρό, την επεξεργασία για λόγους δημοσίου συμφέροντος στον τομέα της δημόσιας υγείας, την ανάγκη ασκήσεως προληπτικής ή επαγγελματικής ιατρικής, ιατρικής διαγνώσεως, παροχής υγειονομικής περίθαλψης ή θεραπείας.

3.3 Βασικές Αρχές επεξεργασίας των δεδομένων υγείας

Η επεξεργασία των δεδομένων θα πρέπει να στηρίζεται σε κάποιες βασικές αρχές, οι οποίες ορίζονται στα άρθρα 5 και 6 του ΓΚΠΔ. Στην αρχή της νομιμότητας, όπου είναι αναγκαίο τα δεδομένα να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο, στην αρχή της διαφάνειας, θα πρέπει το υποκείμενο που τα δεδομένα του υπόκεινται επεξεργασία (δηλαδή οι ασθενείς που νοσούν από κορωνοϊό) και να είναι πλήρως ενημερωμένο για την επεξεργασία που πρόκειται να γίνει (Άρθρο 5 παρ. 1 α).

Άλλες νομικές αρχές στις οποίες είναι αναγκαίο να στηρίζεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα, είναι η αρχή του σκοπού (Άρθρο 5 παρ. 1 β), τα δεδομένα θα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία, κατά τρόπο ασύμβατο με τους σκοπούς αυτούς. Είναι απαραίτητο δηλαδή να βασίζονται για σκοπούς που σχετίζονται με τον περιορισμό της εξάπλωσης και την θεραπεία από τον COVID – 19. Την αρχή της ελαχιστοποίησης των δεδομένων (Άρθρο 5 παρ. 1 γ), τα δεδομένα να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς

που υποβάλλονται σε επεξεργασία, στην προκειμένη περίπτωση θα πρέπει να περιορίζονται στο αναγκαίο για την πρόληψη, τον περιορισμό και την θεραπεία από τον COVID – 19.

Στην αρχή της χρονικά περιορισμένης διατήρησης των δεδομένων (Άρθρο 5 παρ. 1 ε), τα δεδομένα να διατηρούνται μόνο για το χρονικό διάστημα που είναι αναγκαία. Στην Ελλάδα για τις μετακινήσεις των πολιτών, για ένα πολύ σημαντικό χρονικό διάστημα ήταν απαραίτητη η χρήση της υπηρεσίας αποστολής SMS στο 13033, για όσους μετακινούνταν εντός της Ελληνικής επικράτειας. Η Πολιτική Προστασίας Προσωπικών Δεδομένων αναφέρει ότι «τα δεδομένα τηρούνται από την ΓΓΠΠ για το χρονικό διάστημα από την αποστολή του γραπτού μηνύματος του πολίτη στο 13033 και μέχρι την απάντηση που λαμβάνει ο πολίτης. Όταν ο πολίτης λαμβάνει την απάντηση στο κινητό του τα προσωπικά του δεδομένα είτε διαγράφονται, είτε ανωνυμοποιούνται και τηρούνται αποκλειστικά για στατιστικούς σκοπούς». Με βάση την παραπάνω αναφορά, προκύπτει ότι δε ρυθμίζεται ο ακριβής ή ο μέγιστος χρόνος διατήρησης των προσωπικών δεδομένων έως τη διαγραφή τους, εφόσον το υποκείμενο των δεδομένων ενδέχεται να μην παραλάβει άμεσα την απάντηση εάν έχει απενεργοποιημένο το κινητό του ή εάν το δίκτυο κινητής τηλεφωνίας παρουσιάζει βλάβες στη λειτουργία του, ώστε το μήνυμα παραμένει στο κέντρο διαβιβάσεως μηνυμάτων (Short Message Service Center -SMSC) ή στην κεραία τηλεπικοινωνιών (Homo Digitalis, 2020).

Επίσης, θα πρέπει να στηρίζεται στην αρχή της ακρίβειας (Άρθρο 5 παρ. 1 δ), τα δεδομένα υγείας είναι αναγκαίο να είναι ακριβή και σε περίπτωση ανακρίβειας, να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση σε σχέση με τους σκοπούς επεξεργασίας. Εάν για παράδειγμα κάποιος νόσησε από κορωνοϊό και θεραπεύτηκε, να γίνει άμεση διόρθωση και καταγραφή του γεγονότος. Ωστόσο στο σημείο αυτό αξίζει να σημειωθεί, ότι με την κατάσταση που επικρατεί αυτή τη στιγμή· η αρχή της ακρίβειας δεν μπορεί να εφαρμοστεί ακριβώς όπως αναφέρεται παραπάνω. Έχουμε τα πιστοποιητικά νόσησης που παρέχονται σε πολίτες οι οποίοι υπήρξαν θετικοί στον ιό ή ακόμα και τα πιστοποιητικά εμβολιασμού που παρέχονται σε όσους έχουν ολοκληρώσει τον εμβολιασμό τους. Τα πιστοποιητικά αυτά συμβάλλουν στην επανένταξη των ατόμων στην κοινωνία και τους διευκολύνουν στις μετακινήσεις τους, με αποτέλεσμα η διόρθωση ή η διαγραφή των δεδομένων που σχετίζονται με το εάν ένα άτομο που νόσησε να μην έχει κάποιο νόημα αυτή τη στιγμή. Επίσης, όσον αφορά την χρήση της υπηρεσίας αποστολής SMS στο 13033 και την διατήρηση των δεδομένων, δεν παρατίθενται τα κριτήρια βάσει των οποίων γίνεται η επιλογή διαγραφής ή ανωνυμοποίησης των προσωπικών δεδομένων, δημιουργώντας έλλειψη προβλεψιμότητας και ανασφάλεια δικαίου. Εξάλλου, η διαδικασία ανωνυμοποίησης είναι εξαιρετικά δυσχερής, καθώς εάν δεν είναι αποτελεσματική τα δεδομένα

μπορούν να επαναπροσδιοριστούν ως προσωπικά μέσω διαδικασίας γνωστής ως 'de-anonymization' ΄ή 're-identification' και έτσι να χάσουν την προστασία που τους παρέχει η ανωνυμοποίηση (Homo Digitalis, 2020).

Τέλος θα πρέπει να στηρίζεται στην αρχή της ακεραιότητας (Άρθρο 5 παρ. 1 στ), να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα και την προστασία από παράνομη ή μη εξουσιοδοτημένη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρήση κατάλληλων τεχνικών ή οργανωτικών μέτρων.

3.4 Περιπτώσεις επεξεργασίας των δεδομένων υγείας

Το ζήτημα της προστασίας των δεδομένων υγείας, έχει αποκτήσει ιδιαίτερη σημασία, λόγω της πανδημίας του COVID – 19, καθώς και των έκτακτων μέτρων που είναι αναγκαίο να ληφθούν, για την μείωση των κρουσμάτων. Στην εποχή αυτή λοιπόν, τα περισσότερα κράτη μέλη έχουν ήδη εγκρίνει νομοθετικές πράξεις έκτακτης ανάγκης, που περιλαμβάνουν και την επεξεργασία ειδικών κατηγοριών δεδομένων για ερευνητικούς σκοπούς.

Για τον λόγο αυτό, η έννοια της έρευνας, αναφέρεται ρητά ως η εξαίρεση στην απαγόρευση επεξεργασίας δεδομένων προσωπικού χαρακτήρα και είναι απαραίτητο να είναι ανάλογη με τον επιδιωκόμενο στόχο (Άρθρο 9, παράγραφος 2, στοιχείο ι)). Ωστόσο, το πρόβλημα το οποίο προκύπτει στην επεξεργασία δεδομένων για ερευνητικούς σκοπούς, είναι ο περιορισμός του σκοπού. Η αρχή του σκοπού στην έρευνα μπορεί να είναι περιορισμένη, αλλά είναι απαραίτητη η ύπαρξη κατάλληλων εγγυήσεων, που μπορεί να περιλαμβάνουν την ψευδωνυμοποίηση ή ακόμα και την ανωνυμοποίηση των δεδομένων.

Στην περίπτωση της ψευδωνυμοποίησης (ΓΚΠΔ, Άρθρο 4, παρ. 5), γίνεται επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο, χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

Σύμφωνα με τον Γενικό Κανονισμό Προσωπικών Δεδομένων (GDPR), ως ανωνυμοποίηση ορίζεται η διαδικασία διαγραφής των αναγνωριστικών προσωπικού χαρακτήρα σε εγγραφές αποθηκευμένων δεδομένων, έτσι ώστε να μην είναι πλέον δυνατόν τα δεδομένα αυτά να συσχετιστούν με το υποκείμενο των δεδομένων το οποίο αφορούν. Η χρήση της ανωνυμοποίησης διαφέρει από αυτή της ψευδωνυμοποίησης, διότι καθιστά θεωρητικά αδύνατο να προσδιοριστεί το

υποκείμενο των δεδομένων, σε αντίθεση με την τεχνική της ψευδωνυμοποίησης με την οποία δεν διαγράφεται η ταυτότητα, αλλά αντικαθίσταται με τέτοιο τρόπο ώστε να απαιτούνται επιπλέον πληροφορίες για να είναι δυνατή η αναγνώριση των αρχικών υποκειμένων (GDPR, n.d.).

4

Ιχνηλάτηση Επαφών

4.1 Ιχνηλάτηση των επαφών των ασθενών

Για την προσπάθεια περιορισμού της εξάπλωσης του κορωνοϊού, τίθεται προς συζήτηση η μέθοδος της ιχνηλάτησης των επαφών των ασθενών. Η ιχνηλάτηση των επαφών ενός κρούσματος γίνεται με σκοπό την αποφυγή διασποράς του ιού και συνήθως οι λειτουργίες περιλαμβάνουν την ενημέρωση, την αυτοαπομόνωση (καραντίνα) και την υποβολή των ατόμων σε εξετάσεις, αν κριθεί απαραίτητο.

Οι μέθοδοι ιχνηλάτησης μπορούν να διακριθούν σε τέσσερις κατηγορίες:

- Στην μη ψηφιακή μέθοδο της άμεσης ιχνηλάτησης. Είναι η παραδοσιακή μέθοδος, όπου ο υπεύθυνος της δημόσιας υγείας επικοινωνεί με το άτομο που βρέθηκε θετικός στον ιό, έτσι ώστε να καταγράψει τα άτομα με τα οποία ήρθε σε επαφή και εν συνεχεία να τα ενημερώσει.
- Στη ψηφιακή ιχνηλάτηση των επαφών των επιβεβαιωμένων κρουσμάτων χωρίς συγκέντρωση και κεντρική αποθήκευση των πληροφοριών των επαφών. Αυτό γίνεται μέσω εφαρμογών (applications) που εγκαθίστανται στα «έξυπνα τηλέφωνα» των πολιτών και πιο αναλυτικά, η λειτουργία και η χρήση τους θα αναφερθεί σε επόμενη ενότητα.
- Στη ψηφιακή ιχνηλάτηση των επαφών των επιβεβαιωμένων κρουσμάτων με συγκέντρωση και κεντρική αποθήκευση των πληροφοριών. Σε αυτή την μέθοδο υπάρχει η δυνατότητα ελέγχου ή ακόμα και η επιβολή μέτρων αυτοπεριορισμού ή και διαγνωστικού ελέγχου από τις δημόσιες αρχές.

- Στις υβριδικές μεθόδους ιχνηλάτησης, οι οποίες συνδυάζουν αναφορές πολιτών με τεχνολογικές εφαρμογές, όπως για παράδειγμα το GPS (ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΒΙΟΗΘΙΚΗΣ, 2020).

4.2 Ζήτημα Ιχνηλατήσεως σε χώρες εντός και εκτός ΕΕ

Πολλές χώρες έχουν ξεκινήσει την παρακολούθηση των τηλεφώνων των πολιτών και κάνουν χρήση των δεδομένων τοποθεσίας για την παρακολούθηση της εξάπλωσης του ιού, καθώς και για την επιβολή τόσο του «κλειδώματος» όσο και της πρόωρης απομόνωσης. Χώρες εκτός ΕΕ όπως είναι η Κίνα, η Σιγκαπούρη, η Ιαπωνία και το Ισραήλ, χρησιμοποιούν ακραίες μεθόδους παρακολούθησης των κινήσεων των ατόμων που έχουν προσβληθεί από τον ιό. Χαρακτηριστικά παραδείγματα ακραίων μεθόδων είναι αυτά της Νότιας Κορέας και της Κίνας.

Η Ν. Κορέα συμμετέχει σε ένα τεράστιο πρόγραμμα ελέγχων για τον ιό και διαθέτει ένα σύστημα παρακολούθησης των ασθενών μέσω των τραπεζικών καρτών και των κινητών τους τηλεφώνων. Υπάρχουν 860.000 αναμεταδότες G4 και G5 στο σύνολο της χώρας, με αποτέλεσμα το κράτος να γνωρίζει που βρίσκεται κάποιος, όταν χρησιμοποιεί το κινητό του τηλέφωνο. Εκτός των παραπάνω, οι πολίτες παρακολουθούνται επιπλέον μέσω καμερών, που είναι τοποθετημένες σε όλους τους δρόμους όλων των πόλεων και υπολογίζεται ότι ο κάθε πολίτης παρακολουθείται περίπου 90 φορές την ημέρα (Ιακωβίδης, 2020).

Η Κίνα χρησιμοποιεί δωρεάν εργαλεία που βασίζονται στο web και στον cloud για να ελέγχει και να κατευθύνει τα άτομα. Για μεγάλο χρονικό διάστημα παρακολουθούσε τα smartphones των κατοίκων χρησιμοποιώντας κάμερες με εφαρμογές αναγνώρισης προσώπου (face id) και υποχρέωνε τους πολίτες να αναφέρουν τη θερμοκρασία τους, καθώς και την ιατρική του κατάσταση. Με τον τρόπο αυτό, μπορούσαν να εντοπίσουν άμεσα τους φορείς του ιού, αλλά και να μάθουν γρήγορα με ποιους πολίτες ήρθαν σε επαφή (Παναγοπούλου-Κουντατζή, 2020). Επίσης στην Κίνα, η είσοδος σε πολλούς δημόσιους χώρους περιορίζεται σε άτομα που μπορούν να εμφανίσουν έναν πράσινο κωδικό υγείας στα smartphone τους και με τον τρόπο αυτό, να αποδείξουν ότι δεν έχουν έρθει σε επαφή με μια επιβεβαιωμένη περίπτωση COVID-19 (Johannes Abeler, et al., 2020).

Στα αεροδρόμια της Ταϊβάν, τοποθετήθηκαν υψηλής απόδοσης θερμικές κάμερες, οι οποίες χρησιμοποιούνται για την λήψη θερμικών εικόνων των ατόμων σε πραγματικό χρόνο, ώστε να εντοπίζονται γρήγορα άτομα με πυρετό. Ενώ στη Σιγκαπούρη, η θερμοκρασία των ατόμων μετρούνταν στις εισόδους των χώρων εργασίας, των σχολείων και των μέσων μαζικής μεταφοράς.

Τα δεδομένα από τα θερμόμετρα παρακολουθούνται και χρησιμοποιούνται για τον εντοπισμό πιθανών κρουσμάτων (Sera Whitelaw , et al., 2020).

Άλλη μια χώρα παράδειγμα εφαρμογής τέτοιων ακραίων μεθόδων είναι και το Ισραήλ, το οποίο διαθέτει τεχνολογία παρακολούθησης, η οποία ιχνηλατεί πληροφορίες σχετικά με την γεωγραφική τοποθεσία των επιβεβαιωμένων περιστατικών για 14 ημέρες πριν την αρχική διάγνωση. Οι πάροχοι κινητής τηλεφωνίας και άλλες εταιρείες μεταδίδουν δεδομένα κινητής τηλεφωνίας απευθείας στις αρχές υγειονομικής περίθαλψης που ασχολούνται με την πανδημία κορωνοϊού και όχι μέσω των υπηρεσιών πληροφοριών ή οργανισμών ασφαλείας (ALTSHULER & HERSHKOVITZ , 2020, p. 13).

Από την άλλη πλευρά υπάρχουν και χώρες που δεν είναι παραδείγματα τέτοιων ακραίων μεθόδων παρακολούθησης. Η Ισλανδία ξεκίνησε εκτεταμένες δοκιμές ασυμπτωματικών ατόμων (Sera Whitelaw , et al., 2020). Χρησιμοποιώντας τεχνολογία κινητής τηλεφωνίας, η Ισλανδία συλλέγει δεδομένα σχετικά με τα συμπτώματα που αναφέρθηκαν από τον ασθενή και συνδυάζει τα δεδομένα αυτά με ένα σύνολα δεδομένων, όπως κλινικά και γονιδιωματικά δεδομένα αλληλουχίας για να προκύψουν πληροφορίες σχετικά με την παθολογία και τη διάδοση του ιού (Anon., 2020).

Η Γερμανία κυκλοφόρησε μια εφαρμογή smartwatch που συλλέγει δεδομένα παλμών, θερμοκρασίας και ύπνου για να ελέγξει για σημάδια ιογενών ασθενειών. Τα δεδομένα από την εφαρμογή παρουσιάζονται σε έναν διαδικτυακό, διαδραστικό χάρτη στον οποίο οι αρχές μπορούν να εκτιμήσουν την πιθανότητα εμφάνισης COVID-19 σε ολόκληρο το έθνος (Sera Whitelaw , et al., 2020).

Στην Αυστραλία παρά τις αρχικές ανησυχίες σχετικά με την παρακολούθηση των ατόμων από την κυβέρνηση και οι ειδικοί επέκριναν την κυβέρνηση για έλλειψη διαφάνειας και μη ανταπόκρισης σε θέματα απορρήτου. Όμως με τη χρήση της εφαρμογής COVIDSafe, η οποία δεν χρησιμοποίει GPS αλλά Bluetooth, οι περισσότεροι κάτοικοι αισθάνονται ασφαλεί. Οι επαγγελματίες του απορρήτου αποδέχονται γενικά ότι η εφαρμογή COVIDSafe επιδιώκει να προστατεύσει το απόρρητο των Αυστραλών και στις 8 Μαΐου 2020, η Αυστραλιανή Κυβέρνηση κυκλοφόρησε τον πηγαίο κώδικα COVIDSafe για δημόσια επιθεώρηση, στο GitHub. Ο πηγαίος κώδικας για την εφαρμογή COVIDSafe είναι πλήρης (Nick Abrahams, et al., 2020).

5

Περιορισμός της εξάπλωσης με εφαρμογές Ιχνηλάτης Επαφών

5.1 Εφαρμογές Ιχνηλάτησης Επαφών

Σημαντικό ρόλο στον περιορισμό της εξάπλωσης του COVID-19 παίζουν οι ψηφιακές τεχνολογίες και πιο συγκεκριμένα οι εφαρμογές ιχνηλάτησης επαφών (contact tracing apps). Οι εφαρμογές αυτές, εγκαθίστανται σε έξυπνες συσκευές (smart devices), όπως για παράδειγμα έξυπνα κινητά τηλέφωνα – smartphones, έξυπνα ρολόγια και tablets. Απαραίτητη προϋπόθεση για την ορθή λειτουργία της εφαρμογής είναι να την μεταφέρει ο χρήστης μαζί του σε κάθε μετακίνηση. Ανάλογα με τα χαρακτηριστικά που διαθέτει η κάθε εφαρμογή και τον βαθμό χρησιμοποίησης της από τους πολίτες, μπορούν να παίξουν σημαντικό ρόλο στον περιορισμό της εξάπλωσης του ιού.

Υπάρχουν δύο κύριες πηγές δεδομένων θέσης διαθέσιμων για τη μοντελοποίηση της εξάπλωσης του ιού. Είναι τα δεδομένα τοποθεσίας που συλλέγονται από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών (Electronic Communication System – ECS), κατά τη διάρκεια παροχής της υπηρεσίας τους και τα δεδομένα τοποθεσίας που συλλέγονται από εφαρμογές παρόχων υπηρεσιών της κοινωνίας της πληροφορίας των οποίων η λειτουργικότητα απαιτεί τη χρήση τέτοιων δεδομένων (Guidelines, 2020).

Τα δεδομένα τοποθεσίας τα οποία συλλέγονται από παρόχους ECS μπορούν να υποβληθούν σε επεξεργασία βάση των άρθρων 6 και 9 της οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την

προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, σύμφωνα με το European Data Protection Board (EDPB).

Πρακτικά αυτό σημαίνει ότι τα δεδομένα αυτά μπορούν να διαβιβαστούν μόνο στις αρχές ή και σε τρίτους, όμως, μόνο εάν τα δεδομένα έχουν ανωνυμοποιηθεί από τον πάροχο. Ωστόσο, για τα δεδομένα που συλλέγονται απευθείας από τον τερματικό εξοπλισμό του χρήστη, ισχύει το άρθρο 5, παράγραφος 3 της οδηγίας «ePrivacy»[2]. Η αποθήκευση πληροφοριών στη συσκευή του χρήστη ή η πρόσβαση στις πληροφορίες που έχουν ήδη αποθηκευτεί επιτρέπεται μόνο εάν ο χρήστης έχει δώσει τη συγκατάθεσή του ή η αποθήκευση ή / και η πρόσβαση είναι απολύτως απαραίτητη για την ρητή αίτηση της υπηρεσίας κοινωνίας της πληροφορίας από τον χρήστη.

5.2 Επιφυλάξεις

Με την εξάπλωση του COVID – 19, παρατηρείται σε πολλά κράτη μέλη της ΕΕ να υπερτερεί η προστασία της δημόσιας υγείας έναντι της προστασίας δεδομένων προσωπικού χαρακτήρα, αφού η προστασία της ιδιωτικής ζωής δεν αποτελεί απόλυτο δικαίωμα. Προκειμένου λοιπόν η κυβέρνηση να εκπληρώσει το θεμελιώδες δικαίωμα της υγείας, είναι απαραίτητο να περιοριστούν άλλα ατομικά δικαιώματα και ελευθερίες.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι αναγκαία για την διαχείριση της πανδημίας και η προστασία των δεδομένων είναι απολύτως απαραίτητη για την οικοδόμηση εμπιστοσύνης και τη δημιουργία των προϋποθέσεων για την κοινωνική αποδοχή οποιασδήποτε λύσης, σύμφωνα με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Τα δεδομένα θα πρέπει να χρησιμοποιούνται για να προσφέρουν νέες δυνατότητες, όπως ο περιορισμός εξάπλωσης του ιού και όχι για τον έλεγχο, τον στιγματισμό ή την καταπίεση των ατόμων.

Τα κράτη μέλη και η ΕΕ έχουν περιορίσει αρκετά ατομικά δικαιώματα, με αρκετές χώρες να έχουν κηρύξει κατάσταση έκτακτης ανάγκης, με σκοπό τον περιορισμό των κρουσμάτων. Η επεξεργασία και η κοινοποίηση των δεδομένων υγείας από τα κράτη μέλη, με σκοπό την

[2] Εισαγωγή του άρθρου 5 παράγραφος 3 στην οδηγία 2002/58 («Οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες»). Το 2009, ο ευρωπαίος νομοθέτης ενέκρινε την αποκαλούμενη οδηγία για τα cookie41, η οποία τροποποίησε την οδηγία για την ηλεκτρονική ιδιωτικότητα. Διαφορετική από την προηγούμενη έκδοση της οδηγίας για την ηλεκτρονική ιδιωτικότητα, η οποία βασίστηκε σε μια απαίτηση εξαίρεσης, η οδηγία για τα cookie εισήγαγε στο άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στο ηλεκτρονικό ταχυδρομείο μια απαίτηση επιλογής για τη χρήση cookie και σχετικών τεχνολογιών στον τερματικό εξοπλισμό συνδρομητή ή χρήστη (π.χ. υπολογιστές, έξυπνα τηλέφωνα κ.λπ.), συνεπώς απαιτείται η δωρεάν, συγκεκριμένη, ενημερωμένη και σαφής συγκατάθεση για την εγκατάσταση cookie (Anon., 2016).

ανίχνευση των ατόμων τα οποία έχουν προσβληθεί από τον ιό, γίνεται χωρίς την άδεια των ασθενών (Hannah van Kolfschooten & Anniek de Ruijter, 2020). Υπό αυτές τις εξαιρετικά δύσκολες συνθήκες, η ιδιωτικότητα των ατόμων είναι περιορισμένη, αφού προέχει η προστασία ενός μεγαλύτερου μέρους του πληθυσμού.

Η επεξεργασία προσωπικών δεδομένων μπορεί να βασίζεται στη συγκατάθεση ή σε μια εναλλακτική νόμιμη βάση, όπου αυτό είναι πιο κατάλληλο, όπως η εκτέλεση μιας εργασίας για το δημόσιο συμφέρον. (Dunlop, 2020) Η χρήση μιας εφαρμογής για την καταπολέμηση της πανδημίας ενδέχεται να οδηγήσει στη συλλογή δεδομένων για την υγεία. Η επεξεργασία των δεδομένων αυτών, επιτρέπεται όταν είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, άρθρο 9 παράγραφος 2 στοιχείο θ) του ΓΚΠΔ, ή για σκοπούς υγειονομικής περίθαλψης όπως περιγράφεται στο άρθρο 9 παράγραφος 2 στοιχείο η) του ΓΚΠΔ. Ανάλογα με τη νομική βάση, μπορεί επίσης να βασίζεται σε ρητή συγκατάθεση, άρθρο 9 παράγραφος 2 στοιχείο α) του ΓΚΠΔ. Σύμφωνα με τον αρχικό σκοπό, το άρθρο 9 παράγραφος 2 στοιχείο ι) του ΓΚΠΔ επιτρέπει επίσης την επεξεργασία δεδομένων που αφορούν την υγεία, όταν αυτό είναι αναγκαίο για σκοπούς επιστημονικής έρευνας ή στατιστικούς σκοπούς.

Επιπλέον, το ΕΣΠΔ επισημαίνει ότι η χρήση εφαρμογών ιχνηλάτησης επαφών που πραγματοποιείται σε οικειοθελή βάση δεν εγγυάται ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα θα βασιστεί αναγκαστικά στη συγκατάθεση. Όταν οι δημόσιες αρχές παρέχουν υπηρεσίες βάσει εντολής που τους έχει ανατεθεί από τον νόμο και σύμφωνα με τις απαιτήσεις που ορίζει αυτός, παρατηρείται ότι η κατάλληλη νομική βάση για την επεξεργασία είναι η αναγκαιότητα για την εκτέλεση καθήκοντος προς το δημόσιο συμφέρον, δηλαδή το άρθρο 6 παράγραφος 1 στοιχείο ε) του ΓΚΠΔ (Dunlop, 2020). Η νομική βάση ή το νομοθετικό μέτρο που παρέχει τη νόμιμη βάση για τη χρήση των εφαρμογών ιχνηλάτησης επαφών είναι απαραίτητο, να περιλαμβάνει ουσιαστικές διασφαλίσεις, συμπεριλαμβανομένης της αναφοράς στον οικειοθελή χαρακτήρα της εφαρμογής. Είναι αναγκαίο, να περιλαμβάνεται σαφής προσδιορισμός του σκοπού και ρητοί περιορισμοί σχετικά με την περαιτέρω χρήση των δεδομένων προσωπικού χαρακτήρα. Επίσης, θα πρέπει η ταυτοποίηση του υπεύθυνου ή των υπευθύνων επεξεργασίας να είναι σαφής και να προσδιορίζονται οι κατηγορίες δεδομένων, καθώς και οι οντότητες στις οποίες (και οι σκοποί για τους οποίους) μπορούν να γνωστοποιούνται τα δεδομένα προσωπικού χαρακτήρα. Ανάλογα με το επίπεδο της παρέμβασης, θα πρέπει να ενσωματώνονται πρόσθετες διασφαλίσεις, λαμβάνοντας υπόψη τη φύση, το πεδίο και τους σκοπούς της επεξεργασίας.

Επίσης, όσον αφορά την προστασία της ιδιωτικής ζωής και των δεδομένων, ιατρικοί ερευνητές αλλά και επιστήμονες δεδομένων είναι πιθανό να χρησιμοποιούν δεδομένα υγείας ασθενών για

σκοπούς, διαφορετικούς από τον αρχικό σκοπό της απλής παροχής υπηρεσιών υγείας. Επιπλέον, οι ερευνητές ενδέχεται να αναλύσουν δεδομένα τηλεπικοινωνιών, όπως δεδομένα τοποθεσίας, (Janosch Delcker & Stephen Brown, 2020) από ασθενείς (ή μόνο από πολίτες της πληγείσας περιοχής) για να κατανοήσουν τις κινήσεις τους και την εξάπλωση του ιού (Board, 2020). Επίσης, πέρα από την έρευνα, αυτά τα δεδομένα έχουν υψηλές δυνατότητες για περαιτέρω σκοπούς (κρατική επιτήρηση σε μολυσμένα άτομα, επιβολή κανόνων κοινωνικής απόστασης κ.λπ.) (Malgieri, 2020).

Επιπλέον, είναι δυνατόν να εξαπατηθούν και να πλαστογραφηθούν συστήματα στα οποία παραλείπονται τα σχετικά δεδομένα ή προστίθενται ψευδή δεδομένα. Οι άνθρωποι θα μπορούσαν να επιλέξουν να απενεργοποιήσουν τη λειτουργία τοποθεσίας στο τηλέφωνό τους ή να μην ενεργοποιήσουν το Bluetooth ή να αφήσουν το τηλέφωνό τους στο σπίτι ή ακόμα να χρησιμοποιήσουν μια δευτερεύουσα συσκευή ή να δανειστούν κάποια άλλη. Διαφορετικά, θα μπορούσαν να μην κοινοποιήσουν πληροφορίες, σε περίπτωση που παρουσιάσουν συμπτώματα ή προσπαθούν να αποφύγουν την δοκιμή (Kitchin, 2020). Επιπλέον, υπάρχει μεγάλος κίνδυνος για εμφάνιση ψευδοθετικών αποτελεσμάτων, με αποτέλεσμα τα άτομα να είναι αναγκαίο να παραμείνουν σε αυτοαπομόνωση (EDPB: Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 2020).

Μία ακόμα βασική επιφύλαξη, η οποία σχετίζεται και με το απόρρητο των δεδομένων και την συμμόρφωση με τον ΓΚΠΔ, είναι ότι οι άνθρωποι διστάζουν να μοιραστούν τις πληροφορίες τους, καθώς δεν είναι σίγουροι ότι δεν θα χρησιμοποιηθούν τα δεδομένα τους, παρά την θέληση τους. Επίσης, δεν μπορούν να γνωρίζουν ποιος είναι ο υπεύθυνος επεξεργασίας, αλλά ούτε και για πόσο καιρό τα δεδομένα τους θα διατηρηθούν στην εκάστοτε βάση δεδομένων. Υπάρχει επιφύλαξη σχετικά με το θέμα των δεδομένων, αφού κάθε άτομο ενδεχομένως να μπορεί να ταυτοποιηθεί είτε άμεσα, είτε έμμεσα, μέσω ενός αναγνωριστικού, όπως το όνομα, τα δεδομένα τοποθεσίας, ο αριθμός προσωπικού αναγνωριστικού ή μέσω ορισμένων συγκεκριμένων παραγόντων που σχετίζονται με το φυσική, γενετική, οικονομική ή κοινωνική ταυτότητα του ατόμου.

Επίσης, επιφύλαξη υπάρχει σχετικά με τα άτομα που ελέγχουν τα δεδομένα, καθώς και τα άτομα που τα επεξεργάζονται. Για τα πρώτα, είναι αναγκαίο να γίνει γνωστό ότι είναι οι κύριοι υπεύθυνοι που ελέγχουν τον λόγο και τον σκοπό της συλλογής δεδομένων και της μεθόδου επεξεργασίας τους. Για τα δεύτερα, είναι τα άτομα που εργάζονται σύμφωνα με τις οδηγίες που λαμβάνουν από τους υπεύθυνους επεξεργασίας δεδομένων, για την επεξεργασία των δεδομένων. Σε αυτό το σημείο είναι σημαντικό να αναφερθούν τα δικαιώματα που παρέχει ο ΓΚΠΔ στους

χρήστες και σχετίζονται με τα δεδομένα και το απόρρητο. Το δικαίωμα πρόσβασης (άρθρο 15 ΓΚΠΔ), το άτομο έχει δικαίωμα πρόσβασης στα προσωπικά του δεδομένα, όπως επίσης έχει το δικαίωμα να γνωρίζει πως εκείνα χρησιμοποιούνται, επεξεργάζονται, αποθηκεύονται και μεταφέρονται σε άλλους οργανισμούς. Το δικαίωμα ενημέρωσης (άρθρο 12 ΓΚΠΔ), τα άτομα έχουν το δικαίωμα ενημέρωσης πριν από τη συλλογή και την επεξεργασία δεδομένων. Το δικαίωμα μεταφοράς δεδομένων, το άτομο έχει το δικαίωμα να μεταφέρει τα δεδομένα του από έναν πάροχο υπηρεσιών σε έναν άλλο ανά πάσα στιγμή. Το δικαίωμα διαγραφής («Δικαίωμα στη λήθη») (Άρθρο 17 ΓΚΠΔ), τα άτομα έχουν το δικαίωμα να διαγράψουν τα δεδομένα τους, εφόσον στερούνται νόμιμης βάσης, ή η διαγραφή επιβάλλεται εκ του νόμου, ή ασκείται λυσιτελώς το δικαίωμα εναντίωσης στην επεξεργασία, χωρίς όμως να ξεχνάμε ότι το δικαίωμα διαγραφής δεν είναι απεριόριστο (άρθρο 8). Το δικαίωμα εναντίωσης, τα άτομα έχουν το δικαίωμα να αντιταχθούν στη χρήση ή την επεξεργασία των δεδομένων τους. Το δικαίωμα περιορισμού της επεξεργασίας, τα άτομα μπορούν να ζητήσουν να σταματήσουν την επεξεργασία συγκεκριμένου είδους δεδομένων. Το δικαίωμα ειδοποίησης, τα άτομα έχουν το δικαίωμα να ειδοποιούνται με 72 ώρες σε περίπτωση παραβίασης των προσωπικών τους δεδομένων. Και το δικαίωμα διόρθωσης τα άτομα έχουν το δικαίωμα να ζητήσουν τον ελεγκτή δεδομένων για ενημέρωση, τροποποίηση ή διόρθωση των δεδομένων τους.

Επιπλέον, άτομα που έχουν προσβληθεί από τον ιό, έχουν επιφυλάξεις σχετικά με λεπτομέρειες που αφορούν την τοποθεσία τους και το εάν τα δεδομένα αυτά, μεταδίδονται δημόσια. Ωστόσο, η πραγματική ταυτότητα των χρηστών δεν αποκαλύπτεται, αλλά λόγω των λίγων ατόμων που θα μετέφεραν τον ιό στην συγκεκριμένη τοποθεσία, μπορεί να χαρτογραφηθεί εύκολα η περιοχή. Με αποτέλεσμα να αναγνωριστούν τα άτομα και να ξεκινήσουν τις εικασίες για την προσωπική τους ζωή και να αναπτύξουν μια λανθασμένη αντίληψη.

Σχετικά με την ποιότητα και τη διαφάνεια των δεδομένων, εξαιτίας της πανδημίας, έχουν δημιουργηθεί τεράστιες «ποσότητες» δεδομένων, όπως πληροφορίες μολυσμένων ατόμων, ποσοστά θανάτων, λεπτομέρειες εξάπλωσης του ιού κ.λπ. Επομένως, είναι σημαντικό τα δεδομένα που αναλύονται να είναι ακριβή και να διασφαλίζεται η ποιότητα τους. Η προέλευση και η δημιουργία των δεδομένων πρέπει να είναι γνωστά στον ερευνητή - χρήστες προκειμένου να αυξηθεί η εμπιστοσύνη και να αποφευχθεί η διάδοση ψευδών πληροφοριών ή πανικού.

Όπως θα αναφερθεί σε παρακάτω ενότητες, υπάρχουν ορισμένες τεχνολογικές λύσεις που βασίζονται σε GPS ή Bluetooth, για την παρακολούθηση των ατόμων με COVID-19. Ωστόσο, αυτά τα συστήματα έρχονται αντιμέτωπα με κάποιες προκλήσεις, όπως η νομοθεσία του Ισραήλ που επέτρεψε στους κυβερνητικούς αξιωματούχους να παρακολουθούν τα δεδομένα των κινητών

τηλεφώνων των ατόμων που αμφισβητούνται ότι έχουν μολυνθεί. Ομοίως για την Ν. Κορέα, δημιουργήθηκε μια δημόσια βάση δεδομένων από την κυβέρνηση της χώρας, η οποία αποτελείται από προσωπικά στοιχεία των μολυσμένων ατόμων, όπως η εργασία τους, οι διαδρομές που έχουν στην διάρκεια της ημέρας, το φύλο τους, η ηλικία τους κ.λπ. (Sheikh Mohammad Idrees, et al., 2020)

Επιπλέον, οι εφαρμογές που βασίζονται στο GPS καταγράφουν και μεταδίδουν τις λεπτομέρειες τοποθεσίας των χρηστών και εισβάλλουν στο απόρρητο των ατόμων. Επομένως, απαιτείται η διαχείριση των πληροφοριών που κοινοποιούνται από τους χρήστες νόμιμα και με τη συγκατάθεση τους, έτσι ώστε να μην υπάρχουν επιφυλάξεις κατά την χρήση της κάθε εφαρμογής από τον τελικό χρήστη. Τέλος, είναι πιθανό ένα άτομο να είχε έρθει σε επαφή με μολυσμένο άτομο, αλλά η εφαρμογή να μην ειδοποιήσει το άτομο, επομένως ο χρήστης να μην γνωρίζει για την έκθεση και να μην ακολουθήσει το προληπτικό μέτρο με τον τρόπο που πρέπει να ακολουθείται (Sheikh Mohammad Idrees, et al., 2020).

5.3 Απαιτήσεις για την εφαρμογή

Παρόλα αυτά, είναι πάντοτε απαραίτητο να πληρούνται οι απαιτήσεις της αναλογικότητας και της αναγκαιότητας των δεδομένων, ούτως ώστε η επεξεργασία των δεδομένων να περιορίζεται σε όσα παρουσιάζουν άμεση συνάφεια προς τον συγκεκριμένο σκοπό που επιδιώκεται με την επεξεργασία. Η εφαρμογή θα πρέπει να έχει ως μοναδικό σκοπό την ιχνηλάτηση επαφών, ώστε τα άτομα που ενδέχεται να έχουν εκτεθεί στον ιό, να μπορούν να ειδοποιηθούν και να λάβουν περίθαλψη.

Τα κράτη μέλη, θα πρέπει να κοινοποιούν τα προσωπικά δεδομένα μέσω του συστήματος ανταλλαγής πληροφοριών EWRS, το οποίο είναι ένα σύστημα έγκαιρης προειδοποίησης και απόκρισης. Το συγκεκριμένο σύστημα μπορεί να είναι χρήσιμο, όταν ένα άτομο έχει ταξιδέψει σε ένα άλλο κράτος μέλος ή εάν είχε κάποια επαφή με άτομα που διαμένουν σε κάποιο άλλο κράτος μέλος της ΕΕ.

Τα κράτη μέλη, θα πρέπει να ενημερώνουν τα υποκείμενα των δεδομένων σχετικά με την επεξεργασία των προσωπικών τους δεδομένων, εκτός κι εάν αυτό επηρεάζει την αποτελεσματικότητα του μέτρου για τον επιδιωκόμενο σκοπό. Επίσης, θα πρέπει να αιτούνται τα υποκείμενα επεξεργασίας, δηλαδή οι ασθενείς, την διόρθωση ή την διαγραφή των προσωπικών τους δεδομένων, σε συνεννόηση με τα κράτη μέλη που κοινοποιούν τα δεδομένα υγείας, ούτως ώστε τα δεδομένα να διαγράφονται ή να διορθώνονται και από το EWRS, αλλά και από τα άλλα κράτη μέλη. Επιπλέον, τα κράτη μέλη θα πρέπει να κατηγοριοποιήσουν την φύση των δεδομένων,

έτσι ώστε ανάλογα με την κατηγορία στην οποία ανήκουν, να είναι διαφορετική και η διατήρηση τους στο σύστημα (Hannah van Kolfschooten & Anniek de Ruijter, 2020).

Παρακάτω περιγράφονται και αναλύονται οι συστάσεις και οι λειτουργικές απαιτήσεις σύμφωνα με το European Data Protection Board (EDPB), σχετικά με την χρήση των δεδομένων τοποθεσίας και των εργαλείων παρακολούθησης επαφών.

Οι εφαρμογές ιχνηλάτησης επαφών είναι απαραίτητο να είναι εθελοντικές ως προς την χρήση τους και να μην απαιτούν από τον πληθυσμό την καταναγκαστική εγκατάσταση τους. Τα άτομα θα πρέπει να έχουν τον πλήρη έλεγχο των δεδομένων τους, ανά πάσα στιγμή. Υπάρχουν επιφυλάξεις για το πόσο θα διατηρούνται τα δεδομένα των χρηστών στην εφαρμογή ιχνηλάτησης επαφών. Οπότε όταν ένας χρήστης διαγιγνώσκεται ως προσβεβλημένος από τον ιό, είναι αναγκαίο να ειδοποιούνται μόνον τα άτομα με τα οποία ο χρήστης έχει έρθει σε στενή επαφή, εντός της περιόδου που τα δεδομένα θα διατηρούνται. Οι εφαρμογές ιχνηλάτησης επαφών θα πρέπει να παρέχουν μια λειτουργία που να επιτρέπει την ειδοποίηση των χρηστών, που ενδέχεται να έχουν εκτεθεί στον ιό, με βάση το πόσο κοντά βρέθηκαν σε κάποιο προσβεβλημένο χρήστη, εντός διαστήματος Χ ημερών πριν από τη θετική εξέταση διαλογής (η τιμή Χ καθορίζεται από τις υγειονομικές αρχές). Επίσης, οι εφαρμογές θα πρέπει να παρέχουν συστάσεις στους χρήστες που ενδέχεται να είναι θετικοί στον ιό και είναι αναγκαίο να τους παρέχει οδηγίες σχετικά με περαιτέρω ενέργειες. Η εφαρμογή θα πρέπει να είναι διαλειτουργική με άλλες εφαρμογές που αναπτύσσονται σε κράτη μέλη, ώστε οι χρήστες που ταξιδεύουν σε άλλα κράτη μέλη να μπορούν να ειδοποιούνται αποτελεσματικά.

Σύμφωνα με την Αρχή της Αναλογικότητας «Ελαχιστοποίηση των Δεδομένων» (Άρθρο 5 1(γ), Γενικός Κανονισμός για την Προστασία Δεδομένων), τα δεδομένα που υπόκεινται επεξεργασία είναι αναγκαίο να μειωθούν στο ελάχιστο. Οι εφαρμογές ιχνηλάτησης επαφών είναι απαραίτητο να μην συλλέγουν μη σχετικές ή μη απαραίτητες πληροφορίες, οι οποίες μπορεί να περιλαμβάνουν αναγνωριστικά επικοινωνίας, μηνύματα, αρχεία καταγραφής κλήσεων, δεδομένα τοποθεσίας ή αναγνωριστικά συσκευών. Επίσης, τα δεδομένα που μεταδίδουν οι εφαρμογές, είναι αναγκαίο να περιλαμβάνουν μοναδικά αναγνωριστικά, τα οποία παράγονται από την ίδια την εφαρμογή. Τα ψευδοτυχαία αναγνωριστικά πρέπει να ανανεώνονται τακτικά, με συχνότητα επαρκή ώστε να περιορίζεται ο κίνδυνος εκ νέου ταυτοποίησης, φυσικής παρακολούθησης ή αποανωνυμοποίησης των ατόμων μέσω διασύνδεσης στοιχείων, από οποιονδήποτε, συμπεριλαμβανομένων των χειριστών των κεντρικών εξυπηρετητών, άλλων χρηστών της εφαρμογής ή κακόβουλων τρίτων. Τα αναγνωριστικά πρέπει να παράγονται από την εφαρμογή του χρήστη με τυχαίο τρόπο και να παρέχονται από τον κεντρικό εξυπηρετητή. (EDPB:

Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 2020).

Η εφαρμογή πρέπει να μπορεί να μεταδίδει και να λαμβάνει δεδομένα μέσω τεχνολογιών επικοινωνίας γειτνίασης, όπως η τεχνολογία Bluetooth Low Energy, ώστε να είναι δυνατή η ιχνηλάτηση επαφών. Τα εν λόγω εκπεμπόμενα δεδομένα πρέπει να περιλαμβάνουν ψευδοτυχαία αναγνωριστικά με ισχυρή κρυπτογράφηση, που να παράγονται από την εφαρμογή και να είναι ειδικά για αυτήν. Ο κίνδυνος μεταξύ ψευδοτυχαίων αναγνωριστικών θα πρέπει να είναι αρκετά χαμηλός. Τα ψευδοτυχαία αναγνωριστικά είναι απαραίτητο να ανανεώνονται τακτικά, ώστε να περιορίζεται ο κίνδυνος εκ νέου ταυτοποίησης, φυσικής παρακολούθησης ή αποανωνυμοποίησης των ατόμων μέσω διασύνδεσης στοιχείων, από οποιονδήποτε, συμπεριλαμβανομένων των χειριστών των κεντρικών εξυπηρετητών, άλλων χρηστών της εφαρμογής ή κακόβουλων τρίτων. Τα αναγνωριστικά πρέπει να παράγονται από την εφαρμογή του χρήστη, ενδεχομένως βάσει «φύτρων» (seeds) που παρέχονται από τον κεντρικό εξυπηρετητή (Sheikh Mohammad Idrees, et al., 2020) (EDPB: Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 2020).

Επίσης, η εφαρμογή δεν θα πρέπει να συλλέγει δεδομένα θέσης με σκοπό την ιχνηλάτηση των επαφών. Η χρήση δεδομένων θέσης επιτρέπεται αποκλειστικά για τον σκοπό της αλληλεπίδρασης με παρόμοιες εφαρμογές σε άλλες χώρες και η ακρίβειά της θα πρέπει να περιορίζεται στην απολύτως αναγκαία για τον συγκεκριμένο σκοπό. Επίσης, δεν θα συλλέγει δεδομένα υγείας πέραν από εκείνα που είναι απολύτως απαραίτητα για τους σκοπούς της εφαρμογής. Επιπλέον είναι απαραίτητο οι χρήστες να ενημερώνονται για όλα τα δεδομένα προσωπικού χαρακτήρα που θα συλλέγονται και να συλλέγονται μόνο με την άδεια του χρήστη. Οι ανταλλαγές δεδομένων θα πρέπει να σέβονται την ιδιωτική ζωή των χρηστών και να τηρούν την αρχή της ελαχιστοποίησης των δεδομένων.

Η εφαρμογή δεν θα πρέπει να επιτρέπει την άμεση ταυτοποίηση των χρηστών κατά την χρήση της, αλλά ούτε να επιτρέπει την παρακολούθηση των κινήσεων των χρηστών. Η εφαρμογή θα πρέπει να αποκαλύπτει στον χρήστη μόνο το εάν αυτός έχει εκτεθεί στον ιό και, χωρίς να αποκαλύπτει πληροφορίες για άλλους χρήστες, όπως, σε ποιο μέρος ή σε ποιες ημερομηνίες εκτέθηκε. Οι πληροφορίες που παρέχονται από την εφαρμογή δεν πρέπει να επιτρέπουν στους χρήστες να ταυτοποιούν χρήστες που είναι θετικοί στον ιό, ούτε να γνωρίζουν τις μετακινήσεις τους, αλλά ούτε στις υγειονομικές αρχές να ταυτοποιούν χωρίς την συγκατάθεση των χρηστών.

Για την αναφορά χρηστών της εφαρμογής, ως μολυσμένων με COVID – 19, είναι απαραίτητη η ύπαρξη κατάλληλης εξουσιοδότησης. Για παράδειγμα η ύπαρξη ενός μοναδικού κωδικού,

μοναδικής χρήσης, που συνδέεται με μια «ψευδώνυμη» ταυτότητα του μολυσμένου ατόμου και συνδέεται με ένα υγειονομικό κέντρο ή επαγγελματία του τομέα της υγείας. Εάν η επιβεβαίωση δεν μπορεί να ληφθεί με ασφαλή τρόπο, δεν θα πρέπει να πραγματοποιηθεί και επεξεργασία των δεδομένων.

Επίσης, ο υπεύθυνος επεξεργασίας δεδομένων, σε συνεργασία με τις δημόσιες αρχές, είναι αναγκαίο να ενημερώσει με σαφήνεια σχετικά με τον σύνδεσμο (link), για τη λήψη της επίσημης εθνικής εφαρμογής ανίχνευσης επαφών, προκειμένου να μετριάσει τον κίνδυνο ότι οι χρήστες δεν χρησιμοποιούν μια third-party εφαρμογή, η οποία μπορεί να προκαλέσει σωρεία προβλημάτων (EDPB: Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 2020).

Οι χρήστες θα πρέπει να μπορούν να επιβεβαιώνουν τον τρόπο χρήσης των δεδομένων τους. Οι υποσχέσεις των προγραμματιστών της εφαρμογής για διαγραφή δεδομένων δεν επαρκούν. Θα πρέπει οι χρήστες, να είναι σε θέση να ασκούν τα δικαιώματα τους μέσω της εφαρμογής και να υπάρχει δυνατότητα του χρήστη να την διαγράψει, ώστε να διαγράφονται και όλα τα δεδομένα που έχουν συλλεχθεί σε τοπικό επίπεδο. Οι χρήστες θα πρέπει να μπορούν να ελέγχουν με ακρίβεια ποια δεδομένα τοποθεσίας έχουν συλλεχθεί και αποθηκευτεί και να επιβεβαιώσουν ότι τα δεδομένα τους δεν είναι πλέον διαθέσιμα, μετά την προθεσμία για τη διαγραφή (περίοδος επώασης της νόσου, 14 έως 37 ημέρες για τον κορωνοϊό). Οι εφαρμογές πρέπει να λάβουν τη μη αναγκαστική και ενημερωμένη συγκατάθεση των χρηστών για οποιαδήποτε αποκάλυψη των δεδομένων τους (Sheikh Mohammad Idrees, et al., 2020).

Επίσης, είναι αναγκαίο οι προγραμματιστές των εφαρμογών να αναλύσουν τις λειτουργίες επεξεργασίας που εμπλέκονται στις προτεινόμενες εφαρμογές ανίχνευσης επαφών στα επιμέρους στοιχεία τους, την εκτίμηση και την αναλογικότητα, τη νόμιμη βάση και τον αντίκτυπο των χρηστών.

Όσον αφορά την ασφάλεια, είναι απαραίτητη η ύπαρξη ενός μηχανισμού που να επαληθεύει την κατάσταση των χρηστών που δηλώνονται θετικοί στην εφαρμογή, για παράδειγμα με έναν κωδικό μιας χρήσης. Εάν δεν είναι δυνατή η λήψη επιβεβαίωσης με ασφαλή τρόπο, τα δεδομένα δεν θα πρέπει να υποβάλλονται σε επεξεργασία. Τα δεδομένα που αποστέλλονται στον κεντρικό εξυπηρετητή πρέπει να διαβιβάζονται μέσω ασφαλούς διαύλου. Η χρήση υπηρεσιών ειδοποίησης που προσφέρονται από παρόχους πλατφορμών λειτουργικών συστημάτων θα πρέπει να αξιολογείται προσεκτικά και δεν θα πρέπει να οδηγεί σε αποκάλυψη οποιωνδήποτε δεδομένων σε τρίτους.

Είναι αναγκαίο να εφαρμόζονται εξελιγμένες τεχνικές κρυπτογράφησης για την προστασία της ανταλλαγής πληροφοριών, που βρίσκονται αποθηκευμένες στις εφαρμογές και στον εξυπηρετητή. Παραδείγματα τεχνικών που μπορούν να χρησιμοποιηθούν είναι: συμμετρική και ασύμμετρη κρυπτογράφηση, συναρτήσεις κατακερματισμού, έλεγχος ιδιωτικής συμμετοχής (private membership test), τομή ιδιωτικών συνόλων (private set intersection), φίλτρα Bloom, ιδιωτική ανάκτηση πληροφοριών, ομομορφική κρυπτογράφηση κ.λπ (EDPB: Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 2020).

Επίσης, αρκεί η ανταλλαγή ψευδώνυμων αναγνωριστικών μεταξύ των κινητών συσκευών των χρηστών (υπολογιστές, ταμπλέτς, συνδεδεμένα ρολόγια κ.λπ.), για παράδειγμα μέσω εκπομπής (π.χ. με τεχνολογία Bluetooth χαμηλής κατανάλωσης ενέργειας). Τα αναγνωριστικά πρέπει να ανανεώνονται τακτικά ώστε να περιορίζεται ο κίνδυνος παρακολούθησης του φυσικού προσώπου ή επιθέσεων αποανωνυμοποίησης μέσω διασύνδεσης στοιχείων (linkage attacks). Επίσης, η εφαρμογή δεν θα πρέπει να παρέχει στους χρήστες πληροφορίες που τους επιτρέπουν να μαθαίνουν την ταυτότητα ή τη διάγνωση άλλων (Sheikh Mohammad Idrees, et al., 2020). Ο κεντρικός εξυπηρετητής δεν θα πρέπει ούτε να ταυτοποιεί τους χρήστες ούτε να συλλέγει πληροφορίες σχετικά με αυτούς. Η εφαρμογή θα πρέπει να είναι διαλειτουργική με άλλες εφαρμογές που αναπτύσσονται σε άλλα κράτη μέλη, ώστε οι χρήστες που ταξιδεύουν σε κράτη μέλη της ΕΕ να μπορούν να ειδοποιούνται αποτελεσματικά.

Κάθε διακομιστής που συμμετέχει στο σύστημα παρακολούθησης - ιχνηλάτησης επαφών θα πρέπει να συλλέγει τα άκρως απαραίτητα δεδομένα, τα οποία είναι το ιστορικό των επαφών και το αναγνωριστικό του χρήστη που έχει διαγνωστεί θετικός στον ιό. Εναλλακτικά, ο εξυπηρετητής πρέπει να τηρεί κατάλογο με τα ψευδώνυμα - αναγνωριστικά των προσβεβλημένων χρηστών ή το ιστορικό επαφών τους, μόνο για όσο χρόνο χρειάζεται για να ενημερώσει τους δυνητικά προσβεβλημένους χρήστες, για την έκθεσή τους. Και δεν θα πρέπει να προσπαθεί να ταυτοποιήσει τους δυνητικά προσβεβλημένους χρήστες. Σε περίπτωση που απαιτούνται επιπλέον πληροφορίες, αυτές θα πρέπει να παραμένουν στον τερματικό εξοπλισμό του χρήστη και να υποβάλλονται σε επεξεργασία μόνο όταν κρίνεται απολύτως απαραίτητο και δίνεται η συγκατάθεση του (EDPB: Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 2020).

Επιπλέον, ο κεντρικός εξυπηρετητής δεν θα πρέπει να τηρεί τα αναγνωριστικά σύνδεσης δικτύου (π.χ. διευθύνσεις IP) των χρηστών, συμπεριλαμβανομένων εκείνων που έχουν διαγνωστεί ως θετικοί και οι οποίοι έχουν διαβιβάσει το ιστορικό των επαφών τους ή τα δικά τους

αναγνωριστικά. Τα δεδομένα αυτά θα πρέπει να περιορίζονται στο ελάχιστο και δεν επιτρέπεται η αποστολή τους στον εξοπλισμό του χρήστη.

Τέλος, για να αποφευχθεί η πλαστοπροσωπία ή η δημιουργία ψεύτικων χρηστών, ο εξυπηρετητής πρέπει να πραγματοποιεί επαλήθευση ταυτότητας της εφαρμογής. Η εφαρμογή πρέπει να πραγματοποιεί επαλήθευση ταυτότητας του κεντρικού εξυπηρετητή. Η πρόσβαση σε όλα τα δεδομένα που αποθηκεύονται στον κεντρικό εξυπηρετητή και δεν είναι δημόσια, πρέπει να περιορίζεται μόνο στα εξουσιοδοτημένα πρόσωπα. Ο διαχειριστής αδειών της συσκευής, σε επίπεδο λειτουργικού συστήματος, πρέπει να ζητά μόνο τις άδειες που είναι απαραίτητες για την πρόσβαση και τη χρήση των υπομονάδων επικοινωνίας, όποτε χρειάζεται, για την αποθήκευση των δεδομένων στον τερματικό εξοπλισμό και για την ανταλλαγή πληροφοριών με τον κεντρικό εξυπηρετητή. Τα δεδομένα που περιέχονται στα αρχεία καταγραφής των εξυπηρετητών πρέπει να περιορίζονται στο ελάχιστο δυνατό και πρέπει να συμμορφώνονται με τις απαιτήσεις προστασίας των δεδομένων.

5.4 Λειτουργία Εφαρμογών

Σύμφωνα με τον Παγκόσμιο Οργανισμό Υγείας, η μετάδοση του κορωνοϊού COVID – 19, γίνεται από απόσταση ενός περίπου μέτρου (W.H.P, 2020). Για τον λόγο αυτό κρίνεται απαραίτητη η χρήση εφαρμογών, που η λειτουργία τους βασίζεται στη χρήση διαφόρων τεχνολογιών, όπως για παράδειγμα Bluetooth, NFC, WiFi, GPS, που προσφέρουν μεγαλύτερη ακρίβεια στη συλλογή δεδομένων θέσης, σε σχέση με τις πληροφορίες που συλλέγονται μέσω των δικτύων κινητής τηλεφωνίας (Αντιγόνη Λογοθέτη, et al., 2020).

Για να θεωρηθεί έκθεση υψηλού κινδύνου, θα πρέπει να υπάρξει επαφή διάρκειας μεγαλύτερης των 15 λεπτών και σε απόσταση μικρότερη των 2 μέτρων, με τις ακριβείς παραμέτρους να καθορίζονται από τις εθνικές υγειονομικές αρχές (Comission, 2020).

Τα απαραίτητα στοιχεία για την ορθή λειτουργία των εφαρμογών που βασίζονται στην συγκεκριμένη τεχνολογία, είναι τέσσερα. Αρχικά ο χρήστης είναι απαραίτητο να εγκαταστήσει την σχετική εφαρμογή στο smartphone ή οποιαδήποτε άλλη συσκευή χρησιμοποιεί και να την έχει πάντα μαζί του στις μετακινήσεις του. Όταν ο χρήστης βρεθεί σε απόσταση μερικών μέτρων, από άτομο που έχει εγκαταστήσει την ίδια εφαρμογή, θα πρέπει να γίνει «σύνδεση» και να καταγραφεί το γεγονός της επαφής αυτής. Σε περίπτωση αδιαθεσίας, είναι απαραίτητο να υποβάλλεται σε σχετικές εξετάσεις, ούτως ώστε να γνωρίζει εάν έχει μολυνθεί από τον ιό και σε περίπτωση μόλυνσης, να ενημερώνει την εφαρμογή και να ειδοποιούνται τα άτομα με τα οποία ήρθε σε επαφή (Αντιγόνη Λογοθέτη, et al., 2020).

Μετά την εγκατάσταση της εφαρμογής, κάθε χρήστης διαθέτει ένα συγκεκριμένο κλειδί, αποτελούμενο από μια τυχαία ακολουθία γραμμάτων και αριθμών, το οποίο μεταδίδεται από τη μια «έξυπνη συσκευή» στην άλλη, κάθε φορά που οι δύο χρήστες έρχονται σε επαφή. Εάν κάποιος διαγνωστεί θετικός στον ιό, τότε το κλειδί στην εφαρμογή θα προβάλει όλες τις επαφές με τις οποίες έχει έρθει σε επαφή τις τελευταίες 14 ημέρες. Τα κλειδιά ανταλλάσσονται μέσω Bluetooth, μεταξύ κοντινών συσκευών που διαθέτουν την αντίστοιχη εφαρμογή και αποθηκεύονται για 14 ημέρες. Μόλις ο χρήστης εγκρίνει τη συμμετοχή του στο σύστημα ειδοποιήσεων ως προς την έκθεσή του, το σύστημα θα δημιουργήσει ένα τυχαίο αναγνωριστικό στη συσκευή (Τσιάκα, 2020).

Τα αναγνωριστικά που δημιουργούνται, είναι τυχαία, αλλάζουν σε περιοδική βάση με αποτέλεσμα να μην είναι δυνατή η ταυτοποίηση ενός μεμονωμένου ατόμου. Οι εφαρμογές παράγουν ψευδοτυχαία, προσωρινά και περιοδικά μεταβαλλόμενα αναγνωριστικά (των συσκευών που έρχονται σε επαφή με την συσκευή του χρήστη). Υπάρχουν δύο επιλογές, η μια επιλογή είναι η αποθήκευση των αναγνωριστικών στη συσκευή του χρήστη, η λεγόμενη αποκεντρωμένη επεξεργασία. Ενώ η άλλη επιλογή μπορεί να προβλέπει ότι τα εν λόγω αυθαίρετα αναγνωριστικά αποθηκεύονται στον διακομιστή στον οποίο έχουν πρόσβαση οι υγειονομικές αρχές (η λεγόμενη λύση του διακομιστή backend). Η αποκεντρωμένη λύση συνάδει περισσότερο με την αρχή της ελαχιστοποίησης (Επίσηση Εφημερίδα της Ευρωπαϊκής Ένωσης, 2020).

Οι εφαρμογές τέτοιου τύπου, λειτουργούν στο παρασκήνιο της εφαρμογής, χωρίς να απαιτείται κάποια επιπλέον ενεργοποίηση, αφού οι ειδοποιήσεις γίνονται αυτόματα. Όταν η συσκευή εντοπίσει κάποιο αναγνωριστικό από μία κοντινή συσκευή, το αποθηκεύει.

Σε περίπτωση που ο χρήστης βρεθεί θετικός και ενημερώσει σχετικά με την κατάσταση της υγείας του την εφαρμογή και το αναγνωριστικό του έχει αποθηκευτεί στην συσκευή του άλλου χρήστη, η εφαρμογή θα τον ειδοποιήσει και θα τον ενημερώσει για τα επόμενα βήματα που πρέπει να ακολουθήσει, καθώς και τον βαθμό κινδύνου. Επίσης, είναι πιθανό να δώσει επιπρόσθετες πληροφορίες, σχετικά με την ημέρα που έγινε η επαφή, την διάρκεια της, καθώς και την ισχύ του σήματος Bluetooth της συγκεκριμένης επαφής (Τσιάκα, 2020).

Η εφαρμογή υπολογίζει τον βαθμό κινδύνου ενός χρήστη, ο οποίος μπορεί να λάβει ειδοποίηση έκθεσης αν πληρούνται τα κριτήρια (Comission, 2020). Ο προσδιορισμός του κινδύνου είναι δυνατός εντός 24 ωρών από την εγκατάσταση, οπότε οι πληροφορίες για την τρέχουσα κατάσταση που εμφανίζονται μεταβάλλονται από «άγνωστος κίνδυνος» σε «χαμηλός κίνδυνος» ή «αυξημένος κίνδυνος» (Comission, 2020). Χαμηλός κίνδυνος, είναι όταν ένας χρήστης της εφαρμογής δεν είχε κοντινή επαφή για αρκετό χρονικό διάστημα. Αυξημένος κίνδυνος, είναι όταν

ο χρήστης ενημερώθηκε ότι τις τελευταίες 14 ημέρες ήρθε σε επαφή με ένα τουλάχιστον άτομο που είναι θετικός στον ιό. Και ο άγνωστος κίνδυνος, όταν ο χρήστης δεν έχει ενεργοποιήσει τον προσδιορισμό του κινδύνου για αρκετά μεγάλο χρονικό διάστημα και δεν μπορεί να υπολογιστεί ο κίνδυνος λοίμωξης. Αξίζει σε αυτό το σημείο να αναφερθεί ότι το σύστημα ειδοποιήσεων έκθεσης, δεν αποθηκεύει ούτε χρησιμοποιεί δεδομένα σχετικά με την τοποθεσία των χρηστών.

5.5 Τι χρησιμοποιούν οι εφαρμογές ιχνηλάτησης επαφών

Οι εφαρμογές ανίχνευσης επαφών απαιτούν τη χρήση μιας πηγής δεδομένων για να συναχθεί η επαφή μεταξύ δύο ατόμων: δύο από τις πιο χρήσιμες, είναι τα δεδομένα θέσης GPS (location data GPS) και η μετάδοση μέσω Bluetooth. Παρακάτω παρουσιάζονται αναλυτικά και οι δυο από αυτές.

5.6 Bluetooth Χαμηλής Ενέργειας (Bluetooth Low Energy)

Η πιο δημοφιλής μέθοδος που χρησιμοποιείται σε εφαρμογές ανίχνευσης επαφών, είναι η τεχνολογία Bluetooth Low Energy (BLE), οι εφαρμογές αυτές, βασίζονται σε τεχνολογίες μικρής εμβέλειας και χωρίς να ανιχνεύεται η θέση του χρήστη, κοινοποιούν ανώνυμα στα υγιή άτομα εάν είχαν στενή επαφή με άτομο το οποίο επιβεβαιώθηκε ότι έχει μολυνθεί από τον ιό, χωρίς να μεταφέρονται τα δεδομένα, ούτε να αποθηκεύονται σε κάποιον online server. Τα σήματα Bluetooth, που μεταδίδονται από τα τηλέφωνα ενός ατόμου, μπορούν να χρησιμοποιηθούν για την προστασία της εγγύτητας με άλλα άτομα.

Η τεχνολογία Bluetooth Low Energy, παρέχει μειωμένη κατανάλωση ενέργειας και κόστος, σε σχέση με το Bluetooth Classic (Energy, n.d.). Στο BLE, οι συσκευές μπορούν να υποστηρίξουν έναν από τους δύο ρόλους, περιφερειακούς ή κεντρικούς και αναγνωρίζονται από την διεύθυνση της συσκευής. Μόλις συνδεθεί ένα περιφερειακό, με ένα κεντρικό, μπορούν να επικοινωνήσουν ανταλλάσσοντας πακέτα (packets), μέσω των καναλιών δεδομένων BLE (Mathieu Cunche, et al., 2020).

Είναι η λιγότερο ενοχλητική μορφή «παρακολούθησης», δεδομένου ότι βασίζεται στην εγγύτητα με άλλα τηλέφωνα που χρησιμοποιούν την εφαρμογή και όχι στην πραγματική τοποθεσία (δεδομένα GPS). Είναι μία από τις πιο ακριβείς τεχνολογίες όσον αφορά την αναγνώριση εγγύτητας (primer, 2020).

Επίσης, είναι ιδιαίτερα θορυβώδες, χαρακτηριστικό θετικό, αφού πρόκειται για τεχνολογία παρακολούθησης της τοποθεσίας. Επιπλέον, για την προστασία των χρηστών από το να

παρακολουθούνται, το Bluetooth Low Energy υποστηρίζει την τυχαιοποίηση των διευθύνσεων, καθορίζοντας ιδιωτικές διευθύνσεις που παράγονται τυχαία και εναλλάσσονται περιοδικά.

Η χρήση της εφαρμογής δεν απαιτεί μόνιμη σύνδεση στο Διαδίκτυο, χρησιμοποιεί το Bluetooth για το εντοπισμό εγγύτητας με άλλους χρήστες που διαθέτουν την εφαρμογή. Παρόλα αυτά απαιτείται η σύνδεση στο διαδίκτυο τουλάχιστον για μια φορά την ημέρα, έτσι ώστε η εφαρμογή να κατεβάσει τις απαραίτητες πληροφορίες και να γίνει έλεγχος για το εάν ο χρήστης ήρθε σε επαφή με μολυσμένους χρήστες.

5.6.1 Μέτρηση εγγύτητας στην παρακολούθηση επαφών με βάση το BLE

Η μέτρηση της εγγύτητας για δύο συσκευές που χρησιμοποιούν την τεχνολογία BLE, γίνεται μετρώντας τον δείκτη ισχύος λήψης του σήματος (“RSSI”) μιας δεδομένης σύνδεσης Bluetooth για την εκτίμηση της απόστασης μεταξύ των συσκευών, δηλαδή όσο ισχυρότερο είναι το σήμα, τόσο πιο κοντά είναι οι συσκευές μεταξύ τους. Οι συσκευές που υποστηρίζουν το Bluetooth LE μπορούν να αλλάξουν την ισχύ μετάδοσης και συνεπώς να περιορίσουν σημαντικά το εύρος του σήματος (primer, 2020). Το RSSI εξαρτάται από πολλούς παράγοντες, οι οποίοι μπορούν να επηρεάσουν σημαντικά την εγγύτητα και να οδηγήσουν σε ανακριβείς μετρήσεις και μπορούν να κατηγοριοποιηθούν σε εσωτερικούς και εξωτερικούς παράγοντες (Qingchuan Zhao, et al., 2020).

Στους εξωτερικοί παράγοντες, ανήκουν τα αόρατα ραδιοκύματα (Invisible radio waves) και τα ορατά εμπόδια (Visible physical obstacles). Στα αόρατα, τα σήματα Bluetooth μπορούν να παρεμβληθούν από άλλους τύπους ραδιοκυμάτων, όπως για παράδειγμα εάν το WiFi δεν έχει ρυθμιστεί σωστά για να χρησιμοποιεί κανάλια που αλληλεπικαλύπτονται με κανάλια που χρησιμοποιούνται στο Bluetooth, και τα δύο σήματα ενδέχεται να αλληλεπιδρούν μεταξύ τους (beacons?, 2020), με αποτέλεσμα η ληφθείσα τιμή RSSI να είναι λιγότερο ακριβής. Στα ορατά, τα εμπόδια στο transmission path, είναι πιθανό να οδηγήσουν σε διακυμάνσεις RSII. Διαφορετικά υλικά όπως ξύλο, νερό και γυαλί, καθώς και διαφορετικές υφές στην επιφάνεια αντικειμένων μπορούν να οδηγήσουν σε διαφορετικά επίπεδα παρεμβολών σήματος, όπως απορρόφηση, παρεμβολή και περίθλαση, με αποτέλεσμα το RSSI να γίνει ασταθές (What are broadcasting power, 2020).

5.6.2 Διαφήμιση

Το πλαίσιο επικοινωνίας BLE, αποτελείται από 40 κανάλια συχνότητας (frequency channels), εκ των οποίων τα 3 είναι για «διαφήμιση» (advertisement channels) και τα υπόλοιπα 37 είναι κανάλια δεδομένων (data channels) (Mathieu Cunche, et al., 2020). Χρησιμοποιούν broadcast advertising, δηλαδή «διαφημίζουν» τον εαυτό τους, για να ανακοινώσουν την παρουσία τους σε

άλλες συσκευές Bluetooth LE που βρίσκονται σε κοντινή απόσταση. Η μετάδοση αυτή γίνεται σε σταθερό χρονικό διάστημα, μεταξύ 20 ms και 10.24 s, ανάλογα με το πόσο επείγουσες είναι αυτές οι συνδέσεις (primer, 2020).

Η «διαφήμιση» περιέχει πληροφορίες σχετικές με την παρακολούθηση, την συσκευή (και τον τύπο της), την διεύθυνση MAC, καθώς και ένα «ωφέλιμο φορτίο» με τα δεδομένα που «διαφημίζονται». Οι συσκευές BLE μεταδίδουν κάποιες πληροφορίες για να ενημερώσουν οποιαδήποτε άλλη κοντινή συσκευή για την παρουσία της (Introduction, 2020). Στην περίπτωση του COVID-19, αυτό το «ωφέλιμο φορτίο», είναι ένα καθολικά μοναδικό αναγνωριστικό UUID (Universally Unique Identifier) (primer, 2020). Ένα UUID, είναι μια σειρά από 128 bit, που αντιπροσωπεύεται σε 32 δεκαεξαδικούς χαρακτήρες, είναι ένας αριθμός ταυτοποίησης και συνεχούς αναφοράς σε μία μόνο συσκευή, που θα προσδιορίσει μοναδικά κάτι, που είναι υπολογιστικά δύσκολο να το «μαντέψουν» (overflow, n.d.). Τα UUID είτε δημιουργούνται ψευδό τυχαία, είτε προέρχονται από μία ιδιότητα της συσκευής, όπως για παράδειγμα αριθμό τηλεφώνου, διεύθυνση MAC, IMEI και την ώρα της παραγωγής.

5.6.3 ATT: Attribute Protocol

Το Bluetooth LE φέρει δύο βασικές προδιαγραφές το πρωτόκολλο ATT και το Generic Attribute Profile CATT). Το πρωτόκολλο ATT είναι ένα πρωτόκολλο, το οποίο καθορίζει τη βασική δομή του τρόπου αποθήκευσης και ανταλλαγής δεδομένων της τεχνολογίας BLE. Διαθέτει έναν πίνακα βάσεις δεδομένων με καταχωρήσεις, με ειδική μορφή και πεδία. Κάθε καταχώρηση αποτελείται από το Attribute Handle, το Attribute Type, το Attribute Value και το Attribute Permission ((ATT), n.d.). Το Attribute Handle αποτελείται από 2 bytes και είναι το μοναδικό αναγνωριστικό για κάθε καταχώρηση, το Attribute Type, που είναι ένας μοναδικός αριθμός, το UUID, για να δείξει το είδος του Attribute Value και το Attribute Permission που ορίζει εάν επιτρέπεται η πρόσβαση ανάγνωσης ή εγγραφής για ένα δεδομένο χαρακτηριστικό (Introduction, 2020). Τα παραπάνω χαρακτηριστικά οργανώνονται σε ένα προφίλ GATT (Προφίλ Γενικού Χαρακτηριστικού).

Το πρωτόκολλο ATT απαιτεί σύνδεση μεταξύ δύο συσκευών, αλλά αυτή η σύνδεση δεν απαιτεί απαραίτητα σύζευξη και μπορεί να γίνει χωρίς έλεγχο ταυτότητας. Ως αποτέλεσμα, δύο συσκευές μπορούν να χρησιμοποιήσουν το πρωτόκολλο ATT για ανταλλαγή πληροφοριών ευκαιριακά και χωρίς παρέμβαση του χρήστη (Mathieu Cunche, et al., 2020).

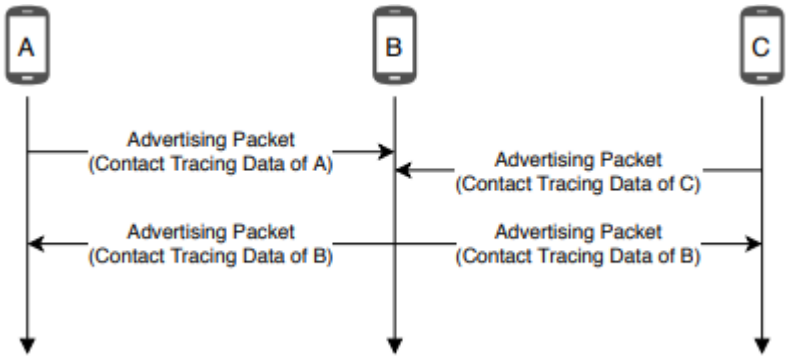
Η συσκευή που περιέχει αυτήν τη βάση δεδομένων για πρόσβαση ονομάζεται διακομιστής, ενώ η συσκευή για πρόσβαση σε αυτήν την απομακρυσμένη βάση δεδομένων ονομάζεται πελάτης. Ο

διακομιστής περιέχει μια σειρά χαρακτηριστικών, και εδώ το «Προφίλ GATT», διαμορφώνει και οριοθετεί τη χρήση των χαρακτηριστικών. Το GATT είναι ένα βασικό προφίλ για όλα τα κορυφαία προφίλ LE. Καθορίζει πώς ένα σύνολο χαρακτηριστικών ATT ομαδοποιούνται σε σημαντικές υπηρεσίες. Δεδομένου ότι η GATT θέτει όλες τις λεπτομέρειες υπηρεσίας στο ATT, δεν υπάρχει ανάγκη για ξεχωριστό πρωτόκολλο εντοπισμού υπηρεσιών (Service Discover Protocol - SDP) (GATT, n.d.).

5.6.4 Μοντέλα για ανίχνευση επαφών με Bluetooth LE

Για την ανίχνευση μέσω της τεχνολογίας BLE, των ατόμων που έχουν προσβληθεί από τον ιό, υπάρχουν δύο μοντέλα. Το συνδεδεμένο μοντέλο (Connected Model), στο οποίο δύο συσκευές δημιουργούν σύνδεση για την ανταλλαγή δεδομένων και το μοντέλο μετάδοσης (Broadcast Model), στο οποίο οι συσκευές μεταδίδουν και συλλέγουν μη κατευθυνόμενα μηνύματα.

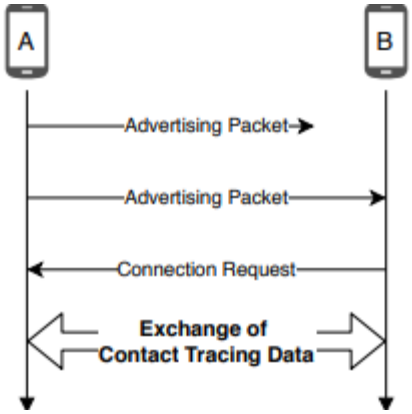
Το Broadcast Model αξιοποιεί τον «διαφημιστικό» μηχανισμό της BLE για μεταφορά δεδομένων παρακολούθησης επαφών σε «διαφημιστικά» πακέτα. Κάθε συσκευή εκπέμπει περιοδικά διαφημιστικά πακέτα που περιέχουν τα δεδομένα παρακολούθησης επαφών που μεταφέρονται μέσα σε ένα στοιχείο δεδομένων διαφήμισης. Ταυτόχρονα, κάθε συσκευή συλλέγει εισερχόμενα πακέτα διαφήμισης και εξάγει-καταγράφει τα δεδομένα παρακολούθησης επαφών (Mathieu Cunche, et al., 2020). Όπως βλέπουμε και στην παρακάτω εικόνα από το On using Bluetooth Low Energy for contact tracing:



Εικόνα 1 Broadcast Model για ανίχνευση επαφών με βάση το Bluetooth Low Energy

Στην παραπάνω εικόνα παρατηρούμε ότι κάθε μία από τις συσκευές μεταδίδουν πακέτα διαφήμισης που φέρουν τα δεδομένα παρακολούθησης επαφών. Τα διαφημιστικά μπορούν να ληφθούν από διάφορες συσκευές σε εύρος.

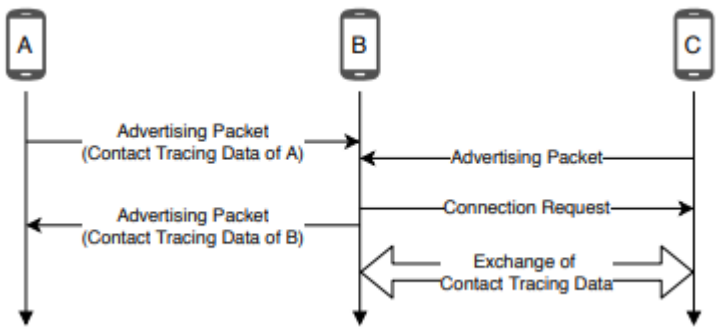
Στο Connected Model, δύο συσκευές δημιουργούν σύνδεση για την ανταλλαγή δεδομένων που αφορούν τις επαφές, όπως φαίνεται και στην Εικόνα 2.



Εικόνα 2 Connected Model για ανίχνευση επαφών με βάση το Bluetooth LE

Κάθε συσκευή διαφημίζει την υποστήριξή της στο σύστημα παρακολούθησης επαφών συμπεριλαμβάνοντας την αντίστοιχη UUID υπηρεσίας στα πακέτα διαφήμισης. Μόλις εντοπιστεί μια κοντινή συσκευή που υποστηρίζει την υπηρεσία, μια συσκευή θα δημιουργήσει μια σύνδεση και θα ανταλλάξει δεδομένα ανίχνευσης επαφών με την απομακρυσμένη συσκευή. Αυτό βλέπουμε να συμβαίνει και στην παραπάνω εικόνα, η συσκευή A ανακοινώνεται μέσω της εκπομπής πακέτων «διαφήμισης», συμπεριλαμβανομένου του UUID. Όταν και αφού λάβει κάποιο από αυτά τα πακέτα η B, ξεκινά μια σύνδεση με το B και, στη συνέχεια, οι A και B ανταλλάσσουν τα δεδομένα ανίχνευσης επαφών μέσω αυτής της σύνδεσης (Mathieu Cunche, et al., 2020).

Ωστόσο, τα δύο παραπάνω μοντέλα, μπορούν να χρησιμοποιηθούν ταυτόχρονα και να αποτελέσουν ένα υβριδικό μοντέλο (hybrid model), στο οποίο οι συσκευές A και B ανταλλάσσουν τα δεδομένα ανίχνευσης επαφών τους σύμφωνα με το μοντέλο μετάδοσης. Λόγω περιορισμών του λειτουργικού συστήματος, η συσκευή C δεν μπορεί να χρησιμοποιήσει το μοντέλο μετάδοσης. Επομένως, οι συσκευές B και C θα χρησιμοποιήσουν το συνδεδεμένο μοντέλο για να ανταλλάξουν τα δεδομένα παρακολούθησης επαφών τους. Όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 3 Hybrid Model για ανίχνευση επαφών με βάση το Bluetooth LE

Το καθένα από τα μοντέλα εκπομπής και σύνδεσης έχει πλεονεκτήματα και περιορισμούς. Πρώτον, όσον αφορά την ποσότητα των δεδομένων, το μοντέλο εκπομπής περιορίζεται στη χωρητικότητα ενός πακέτου διαφήμισης που προσφέρει το πολύ 25 bytes χρήσιμων δεδομένων. Ενώ στο συνδεδεμένο μοντέλο, το ποσό των δεδομένων που μπορούν να ανταλλαχθούν περιορίζεται μόνο από το εύρος ζώνης και τη διάρκεια της σύνδεσης. Μια δεύτερη πτυχή που διαφέρει μεταξύ των δύο μοντέλων είναι η επεκτασιμότητα. Στο μοντέλο εκπομπής, ένα μόνο πακέτο διαφήμισης είναι δυνητικά αρκετό για τη μετάδοση δεδομένων παρακολούθησης επαφών σε όλες τις κοντινές συσκευές. Ενώ με το συνδεδεμένο μοντέλο, είναι απαραίτητο να δημιουργηθεί σύνδεση για κάθε κοντινή συσκευή. Επομένως, το μοντέλο εκπομπής είναι πιο επεκτάσιμο από το συνδεδεμένο μοντέλο (Mathieu Cunche, et al., 2020).

5.6.5 Επισκόπηση υπαρχουσών εφαρμογών ιχνηλάτησης επαφών που βασίζονται στο BLE

Για τον περιορισμό και την αντιμετώπιση της πανδημίας, έχουν δημιουργηθεί πολλές εφαρμογές ιχνηλάτησης επαφών, που βασίζονται στο Bluetooth LE. Στον παρακάτω πίνακα, παρουσιάζεται μια λίστα με αναγνωρισμένες εφαρμογές παρακολούθησης επαφών (Patrick Howell O'Neill , et al., 2020):

Country	System	Voluntary	Limited	Data destruction	Minimized	Transparent
UK	NHS Covid App	✓	✓	✓	✓	✓
Αυστραλία	COVIDSafe	✓	✓	✓	✓	
Αυστρία	Stopp Corona	✓	✓	✓	✓	✓
Β. Ιρλανδία	StopCOVID NI	✓				
Β. Μακεδονία	StopKorona	✓	✓	✓	✓	✓
Βέλγιο	Coronaalert	✓	✓	✓	✓	✓
Βιετνάμ	BlueZone	✓				✓
Γαλλία	StopCovid	✓	✓	✓	✓	✓
Γερμανία	Coroca-Warn-App	✓	✓	✓	✓	✓
Γιβραλτάρ	Beat Covid Gibraltar	✓	✓	✓		✓

Δανία	Smittestopp	✓	✓	✓	✓	✓
Ελβετία	SwissCovid	✓	✓	✓	✓	✓
Εσθονία	*Esthonia's App	✓			✓	
Ιαπωνία	COCOA	✓	✓	✓	✓	✓
Ινδία	Aarogya Setu		✓	✓		
Ινδονησία	PeduliLindungi	✓				
Ιρλανδία	Covid Tracker	✓	✓	✓	✓	✓
Ιταλία	Immuni	✓	✓	✓	✓	✓
Καναδάς	COVID Alert	✓	✓	✓	✓	✓
Κατάρ	Ehteraz					
Μαλαισία	MyTrace	✓				
Μεξικό	CovidRadar	✓				
Μπαχρέιν	BeAware	✓	✓			
Ν. Ζηλανδία	NZ COVID Tracer	✓	✓	✓		✓
Νορβηγία	Smittestopp	✓	✓	✓		
Ουγγαρία	VirusRadar	✓		✓	✓	✓
Πολωνία	ProteGo	✓		✓	✓	✓
Σαουδική Αραβ.	Tabaud	✓		✓	✓	✓
Σιγκαπούρη	TraceTogether		✓	✓	✓	✓
Ταϊλάνδη	MorChana					
Τουρκία	Hayat Eve Sigar				✓	
Τσεχία	eRouska	✓	✓	✓	✓	✓
Τυνησία	E7mi	✓	✓	✓		

Φιλιππίνες	StaySafe	✓				
Φίτζι	CareFiji	✓			✓	✓

Πίνακας 1 Εφαρμογές ιχνηλάτησης επαφών που βασίζονται στο BLE *(Patrick Howell O'Neill , et al., 2020)*

Στον παραπάνω πίνακα, υπάρχουν πέντε κατηγορίες στις οποίες μπορεί να ανταποκρίνονται οι εφαρμογές ιχνηλάτησης. Η κατηγοριοποίηση γίνεται με βάση το εάν η χρήση της εφαρμογής είναι εθελοντική (voluntary), αφού σε πολλές περιπτώσεις χωρών οι πολίτες είναι υποχρεωμένοι να κατεβάσουν και να χρησιμοποιήσουν τις εφαρμογές ιχνηλάτησης επαφών. Εάν υπάρχουν περιορισμοί ως προς τον τρόπο χρήσης των δεδομένων (limited), αφού τα δεδομένα μπορούν να χρησιμοποιηθούν και για σκοπούς που δεν αφορούν την δημόσια υγεία, όπως για παράδειγμα, για την επιβολή του νόμου.

Επίσης, υπάρχει κατηγορία σχετικά με το εάν τα δεδομένα θα καταστραφούν μετά από κάποιο χρονικό διάστημα (Data destruction), αφού τα δεδομένα που συλλέγονται από τις εφαρμογές δεν πρέπει να είναι για πάντα διαθέσιμα. Στις εφαρμογές που υπάρχει τικ στην συγκεκριμένη κατηγορία, τα δεδομένα είτε έχουν διαγραφεί αυτόματα σε εύλογο χρονικό διάστημα (συνήθως το πολύ περίπου 30 ημέρες), είτε η εφαρμογή επιτρέπει στους χρήστες να διαγράψουν με μη αυτόματο τρόπο τα δικά τους δεδομένα (O'Neill, et al., 2020).

Το Minimized αναφέρεται στο εάν η εφαρμογή συλλέγει μόνο τις απαραίτητες πληροφορίες για να λειτουργήσει ορθά και το Transparent αναφέρεται στο εάν υπάρχει διαφάνεια στη χρήση της εφαρμογής. Η διαφάνεια μπορεί να έχει τη μορφή σαφών, διαθέσιμων στο κοινό πολιτικών και σχεδιασμού, για παράδειγμα να είναι διαθέσιμος στους πολίτες, ο κώδικας για την υλοποίηση της κάθε εφαρμογής.

Ενδεικτικά θα γίνει σχολιασμός σε ορισμένες από τις παραπάνω εφαρμογές, οι οποίες βασίζονται στην τεχνολογία BLE. Οι περισσότερες χώρες ανταποκρίνονται και στις πέντε κατηγορίες που αναφέρονται στον παραπάνω πίνακα. Ωστόσο χώρες όπως οι Φιλιππίνες, η Β. Ιρλανδία, η Εσθονία, το Μεξικό, η Μαλαισία, η Ινδονησία και το Μπαχρέιν περιορίζονται είτε μόνο στην εθελοντική χρήση των εφαρμογών είτε και στην συλλογή μόνο των απαραίτητων πληροφοριών. Επίσης, σε χώρες όπως το Κατάρ και την Ταϊλάνδη, η εγκατάσταση και η χρήση των εφαρμογών είναι υποχρεωτική, δεν υπάρχει περιορισμός ως προς τον τρόπο χρήσης των δεδομένων, δεν υπάρχει κάποια εγγύηση ότι τα δεδομένα θα διαγραφούν μετά από ορισμένο χρονικό διάστημα, η εφαρμογή μπορεί να συλλέγει και μη απαραίτητες πληροφορίες και υπάρχει και έλλειψη διαφάνειας.

Η πρώτη μεγάλη εφαρμογή παρακολούθησης επαφών με βάση την τεχνολογία Bluetooth, είναι το TraceTogether της Σιγκαπούρης. Ωστόσο, η κυβέρνηση των Φίτζι ξεκίνησε την εφαρμογή παρακολούθησης επαφών της χώρας, η οποία βασίζεται στο πρωτόκολλο BlueTrace που αναπτύχθηκε από την κυβέρνηση της Σιγκαπούρης (apps, 2020).

Ένα βασικό αρνητικό που υπάρχει στην εφαρμογή BlueZone του Βιετνάμ, είναι ότι απαιτείται πρόσβαση σε επαφές και σε άλλα μέσα των κινητών συσκευών, όπως είναι οι φωτογραφίες. Το ίδιο συμβαίνει και στην εφαρμογή του Κατάρ, που απαιτείται πρόσβαση στις φωτογραφίες της συσκευής, όμως στην συγκεκριμένη εφαρμογή η λήψη είναι υποχρεωτική για όλους τους πολίτες.

Όσον αφορά το COVIDSafe, application το οποίο χρησιμοποιείται στην Αυστραλία, ειδικοί έχουν επικρίνει την κυβέρνηση για έλλειψη διαφάνειας και μη ανταπόκρισης σε θέματα απορρήτου. Επίσης, η μόνη δημοκρατική χώρα η οποία καθιστά υποχρεωτική την εγκατάσταση και χρήση της εφαρμογής της είναι η Ινδία. Τέλος, η Τουρκία, έδωσε διαταγή στα άτομα τα οποία είναι θετικά στον ιό, να εγκαταστήσουν την εφαρμογή στις συσκευές τους και να μπορούν να μοιράζονται τα δεδομένα τους με την αστυνομία (Patrick Howell O'Neill , et al., 2020).

5.6.6 Αρνητικά που προκύπτουν από την χρήση της τεχνολογία Bluetooth LE

Τα συστήματα εντοπισμού που βασίζονται στην τεχνολογία Bluetooth χαμηλής ενέργειας, έχουν χαμηλό κόστος, χαμηλή κατανάλωση ενέργειας και αναπτύσσονται εύκολα. Επίσης το συγκεκριμένο σύστημα είναι ισχυρό ενάντια σε τρίτους που παρακολουθούν υποκλοπές, στους οποίους τα αναγνωριστικά εμφανίζονται ως τυχαίος «θόρυβος». Ένα τέτοιο σύστημα, είναι το TraceTogether, που έχει αναπτυχθεί στη Σιγκαπούρη (Hart, et al., 2020)

Οι εφαρμογές που βασίζονται στην εγγύτητα μπορούν να δημιουργήσουν πολλά ψευδώς θετικά δεδομένα. Η απόσταση υπολογίζεται με βάση την εξασθένηση του ασύρματου σήματος στον ελεύθερο χώρο. Ωστόσο, το σήμα μπορεί επίσης να εξασθενεί σε μεγάλο βαθμό από τα ανθρώπινα σώματα. Εάν δύο άτομα στέκονται με την πλάτη τους το ένα προς το άλλο, το σήμα μπορεί να γίνει αδύναμο και η απόσταση μεταξύ τους μπορεί να παρερμηνευθεί, με αποτέλεσμα να προκύψει ψευδώς αρνητικό αποτέλεσμα. Η ακρίβεια της εφαρμογής εξαρτάται από τη θέση των smartphone που αλληλοεπικαλύπτονται. Για παράδειγμα, ένας λεπτός τοίχος σε δύο διαμερίσματα ενδέχεται να μην εξασθενήσει αρκετά το σήμα και θα μπορούσε να οδηγήσει σε ένα συμβάν εγγύτητας, ακόμη και όταν δεν είναι. Τα ψευδώς θετικά, μπορούν να οδηγήσουν στην απομόνωση των ατόμων που δεν είναι θετικοί στον ιό και τα ψευδώς αρνητικά να εμποδίσουν τον κύριο στόχο της εφαρμογής (RAJAN GUPTA, et al., 2020).

Επίσης επειδή τα άτομα αναφέρουν αυτοπροσώπως τη διάγνωσή τους, με τρόπο που δεν μπορεί να επαληθευτεί, μπορεί να διατρέχουν μεγαλύτερο κίνδυνο κατάχρησης και εκμετάλλευσης. Αυτή η αρχιτεκτονική δεν βασίζεται σε μια κεντρική αρχή και επομένως δεν είναι ευάλωτη σε μαζική παρακολούθηση ή παραβίαση δεδομένων. Ωστόσο, ενδέχεται να είναι ευάλωτο σε επιθέσεις τρίτων, παρόμοια με τις επιθέσεις DDoS, όπου πολλά μηνύματα αποστέλλονται για να κατακλύσουν το σύστημα, καθιστώντας το μη λειτουργικό (Vi Hart, et al., 2020).

5.7 Ανίχνευση τοποθεσίας μέσω GPS, QR Code και CSLI

Η παρακολούθηση τοποθεσίας είναι μια προσέγγιση που χρησιμοποιεί τεχνολογίες που εντοπίζουν και παρακολουθούν φυσικά, την κίνηση των ανθρώπων. Ορισμένες εφαρμογές παρακολούθησης επαφών, χρησιμοποιούν κωδικούς GPS, CSLI ή QR για παρακολούθηση τοποθεσίας.

5.8 GPS Location Data – Δεδομένα Θέσης GPS

Το GPS αναφέρεται συνήθως σε συστήματα πλοήγησης, τα οποία χρησιμοποιούν δορυφόρους για την παροχή γεωχωρικών δεδομένων θέσης. Το GPS ενός smartphone, ή οποιασδήποτε άλλης έξυπνης συσκευής, επιτρέπει την παρακολούθηση της θέσης του ατόμου, σε απόσταση από 1.5 έως και 3 μέτρα. Το GPS ως επί το πλείστων περιορίζεται σε εξωτερική τοποθέτηση, αφού το σήμα GPS είναι πολύ αδύναμο για να δώσει αξιόπιστα (εάν υπάρχουν) αποτελέσματα τοποθέτησης σε εσωτερικούς χώρους (Tobias Weitze & Henrique Barros, 2020).

Ωστόσο, πολλές εφαρμογές που χρησιμοποιούν δεδομένα θέσης, ζητούν από τους χρήστες να μοιράζονται τον αριθμό του τηλεφώνου, ή τις πληροφορίες διαβατηρίου πριν την χρήση της εφαρμογής. Ορισμένες από αυτές τις εφαρμογές, κρυπτογραφούν δεδομένα τοποθεσίας, όμως υπάρχουν κι άλλες που διατηρούν τα δεδομένα σε μια απλή βάση δεδομένων, με αποτέλεσμα η κρυπτογράφηση να μην αποφέρει κάποιο αποτέλεσμα.

Οι εφαρμογές ανίχνευσης που βασίζονται στη γεωγραφική τοποθεσία, συλλέγουν δεδομένα σε πραγματικό χρόνο που σχετίζονται με την ακριβή τοποθεσία και τις κινήσεις των ατόμων. Επίσης συλλέγουν πληροφορίες σχετικές με την υγεία των ατόμων, οι οποίες θέτουν υψηλότερο κίνδυνο στην προστασία της ιδιωτικής ζωής και θέτουν ερωτήματα σχετικά με την αναλογικότητα (Parliament, 2020).

Το πλεονέκτημα των εφαρμογών ιχνηλάτησης επαφών με βάση το GPS είναι ότι ήδη το μεγαλύτερο ποσοστό χρηστών που έχουν στην κατοχή τους smartphone, καταγράφουν δεδομένα τοποθεσίας είτε στο Google Maps Timeline, είτε σε κρυπτογραφημένο τοπικό χώρο αποθήκευσης

σε συσκευές iOS ή και στα δύο. Αυτό επιτρέπει στους χρήστες να εγκαταστήσουν μια τέτοια εφαρμογή, αλλά να μπορούν να λάβουν ειδοποιήσεις σχετικά με την έκθεση τους σε πιθανό κρούσμα, που ενδέχεται να έχει συμβεί, μία ή δύο εβδομάδες πριν την εγκατάσταση της εφαρμογής. Επίσης ένα άλλο πλεονέκτημα του GPS, είναι ότι μπορεί να προειδοποιήσει τους χρήστες να αποφύγουν συγκεκριμένες περιοχές λόγω κρουσμάτων.

5.8.1 Χώρες που χρησιμοποιούν εφαρμογές που βασίζονται σε δεδομένα θέσης

Στον παρακάτω πίνακα, παρουσιάζεται μια λίστα με αναγνωρισμένες εφαρμογές παρακολούθησης επαφών:

Country	System	Voluntary	Limited	Data destruction	Minimized	Transparent	Tech
Βουλγαρία	ViruSafe	✓	✓	✓		✓	Location
Κίνα	Chinese health code system						Location, Data mining
Κύπρος	CovTracer	✓		✓	✓	✓	Location
Ιράν	AC-19	✓					Location
Ισραήλ	HaMagen		✓	✓	✓	✓	Location
Κουβέιτ	Shlonik	✓					Location
Σαουδική Αραβία	Tawakkalna						Location
Μπαχρέιν	BeAware	✓	✓				Bluetooth, Location
Ινδία	Aaraqya Setu		✓	✓			Bluetooth, Location
Νορβηγία	Smittestopp	✓	✓	✓			Bluetooth, Location
Κατάρ	Ehteraz						Bluetooth, Location
Ταϊλάνδη	MorChana						Bluetooth, Location
Τουρκία	Hayat Eve Sigar				✓		Bluetooth, Location
Ινδονησία	PEduliniLindungi	✓					Bluetooth, Location
Γκανά	GH COVID-19 Tracker	✓					Bluetooth, Location
Ισλανδία	Ranking C-19	✓	✓	✓	✓	✓	Bluetooth, Location

Πίνακας 2 Εφαρμογές Ιχνηλάτησης που βασίζονται στην Τοποθεσία *(Patrick Howell O'Neill , et al., 2020)*

Οι εφαρμογές ανίχνευσης επαφών στο Μπαχρέιν, το Κουβέιτ και την Νορβηγία, ακολουθούν μια επεμβατική συγκεντρωτική προσέγγιση, θέτοντας μια μεγάλη απειλή για την ιδιωτική ζωή. Αυτά

τα συστήματα καταγράφουν δεδομένα τοποθεσίας μέσω GPS και τα ανεβάζουν σε μια κεντρική βάση δεδομένων, παρακολουθώντας τις κινήσεις των χρηστών σε πραγματικό χρόνο.

Οι αρχές στο Μπαχρέιν, το Κουβέιτ, τη Νορβηγία και το Κατάρ μπορούν να συνδέσουν τα ευαίσθητα προσωπικά δεδομένα με ένα άτομο, αφού απαιτούν από τους χρήστες να εγγραφούν με τον εθνικό αριθμό ταυτότητας. Στην Νορβηγία απαιτείται εγγραφή με έναν έγκυρο αριθμό τηλεφώνου. Ωστόσο, στις 16 Ιουνίου 2020, η Νορβηγία έθεσε μια παύση στην εφαρμογή και διέγραψε όλα τα δεδομένα των χρηστών λόγω ανησυχιών και θεμάτων ασφαλείας.

Η εφαρμογή Ehteraz του Κατάρ μπορεί να ενεργοποιήσει προαιρετικά την παρακολούθηση ζωντανής τοποθεσίας όλων των χρηστών ή συγκεκριμένων ατόμων. Η Ehteraz ακολουθεί ένα συγκεντρωτικό μοντέλο, όπου αντί να καταγράφονται συντεταγμένες GPS, γίνεται σάρωση για την εγγύτητα μέσω της τεχνολογίας Bluetooth. Η εφαρμογή αυτή εξέθεσε ευαίσθητα προσωπικά στοιχεία περισσότερων από ενός εκατομμυρίου ανθρώπων, αυτό ήταν ιδιαίτερα ανησυχητικό καθώς η εφαρμογή έγινε υποχρεωτική για χρήση στις 22 Μαΐου. Η ευπάθεια διορθώθηκε αφού η Αμνηστία ειδοποίησε τις αρχές για την ανακάλυψη στα τέλη Μαΐου. Το ελάττωμα ασφαλείας θα επέτρεπε στους επιτιθέμενους στον κυβερνοχώρο να έχουν πρόσβαση σε πολύ ευαίσθητες προσωπικές πληροφορίες, συμπεριλαμβανομένου του ονόματος, της εθνικής ταυτότητας, της κατάστασης υγείας και της καθορισμένης τοποθεσίας περιορισμού των χρηστών (Bahrain, 2020).

Στην Ισλανδία, η μεταφόρτωση των πληροφοριών γίνεται μόνο όταν οι χρήστες αποφασίζουν οικειοθελώς να αναφέρουν τον εαυτό τους ως συμπτωματικό ή κατόπιν αιτήματος των υγειονομικών αρχών. Τέτοιες εθελοντικές και συναινετικές μεταφορτώσεις μειώνουν τον κίνδυνο μαζικής παρακολούθησης, καθώς τα δεδομένα δεν μεταφορτώνονται αυτόματα.

5.9 Σύγκριση Bluetooth με GPS

Τα συστήματα που βασίζονται σε Bluetooth είναι συνήθως πιο ακριβή από τις μεθόδους που βασίζονται στο GPS. Οι εφαρμογές παρακολούθησης που βασίζονται σε Bluetooth έχουν χαμηλότερο ψευδώς θετικό ρυθμό και καταναλώνουν λιγότερη ισχύ από τις εφαρμογές παρακολούθησης που βασίζονται σε GPS. Εκτός από τις ανησυχίες περί απορρήτου σχετικά με την παρακολούθηση GPS, τα δεδομένα GPS είναι πολύ ανακριβή ή εντελώς μη διαθέσιμα εντός κτιρίων και συνεπώς περιορισμένης χρήσης (Philipp H. Kindt, et al., 2020).

Το πλεονέκτημα του GPS έναντι του Bluetooth, είναι ότι στο πρώτο η επιτυχή ανίχνευση επαφών είναι ευκολότερη. Με το GPS, δεν χρειάζεται να έχουν ήδη κατεβάσει την εφαρμογή για να είναι αποτελεσματική. Ένα άτομο που έχει θετικά αποτελέσματα για τον ιό μπορεί να χρησιμοποιήσει

το εργαλείο Web Safe Place για να δημιουργήσει χειροκίνητα ίχνη GPS και να βοηθήσει υγιείς ανθρώπους (Luccio, 2020). Αυτό είναι ένα από τα μεγαλύτερα πλεονεκτήματα του GPS σε σύγκριση με το Bluetooth, επειδή το τελευταίο απαιτεί ανταλλαγή πληροφοριών απευθείας, μέσω του υλικού, το οποίο δεν μπορεί να γίνει μετά το γεγονός.

Έχει μελετηθεί ότι μέσω των σημάτων του GPS είναι σχεδόν απίθανο να παρέχονται εκτιμήσεις τοποθεσίας με μεγάλη ακρίβεια, που είναι απαραίτητες, για την ουσιαστική πρόβλεψη του κινδύνου μετάδοσης COVID-19. Σε αντίθεση με τις τεχνολογίες παρακολούθησης Bluetooth που έχουν πολύ πιο ακριβείς μετρήσεις, μέσω σημάτων GPS, η ακρίβεια μπορεί να υποβαθμιστεί παρουσία άλλων συσκευών μετάδοσης σήματος και σε περιοχές με υψηλά επίπεδα παρεμβολών, όπως κτίρια υψηλής πυκνότητας και κυρίως σε πόλεις (Q&A, 2020).

Οι εφαρμογές που βασίζονται στο GPS δημιουργούν ένα «ίχνος τοποθεσίας» για κάθε χρήστη, καταγράφοντας τη θέση τους με τη «σφραγίδα» του χρόνου (timestamps). Ενώ οι εφαρμογές που βασίζονται στο Bluetooth, δημιουργούν ένα μοναδικό αναγνωριστικό, έναν αριθμό ή ένα διακριτικό, το οποίο μεταδίδει η εφαρμογή. Ανίχνευση Τοποθεσίας μέσω QR Code

Ο κωδικός QR είναι ένας ραβδοκώδικας (barcode) δύο διαστάσεων σε τετράγωνο μοτίβο και περιέχει πληροφορίες σχετικά με το αντικείμενο στο οποίο επισυνάπτεται. Ο κωδικός QR σχεδιάστηκε έτσι ώστε να επιτρέπει την αποκωδικοποίηση του περιεχομένου του σε υψηλή ταχύτητα (Tawari, 2020). Οι κωδικοί γρήγορης απόκρισης (quick response code), μπορούν να διαβαστούν από την κάμερα ενός smartphone ή ενός tablet, για άμεση σύνδεση σε websites.

Οι κωδικοί QR είναι πιο χρήσιμοι γιατί επιτρέπουν στον χρήστη να τους χρησιμοποιήσει χωρίς να είναι απαραίτητο να κατεβάσει κάποια συγκεκριμένη εφαρμογή σάρωσης. Κατά τη διάρκεια της πανδημίας COVID – 19, είναι πιθανόν οι έρευνες με βάση το QR code να είναι ιδιαίτερα χρήσιμες. Σε σύγκριση με την ανίχνευση της τοποθεσίας με βάση το GPS, η παρακολούθηση των συμπτώματα των επαφών με το QR code, δεν προσδιορίζει τις λεπτομέρειες τοποθεσίας των χρηστών. Με αυτόν τον τρόπο, μπορεί να αρθεί η ευπάθεια που υπάρχει στις εφαρμογές που βασίζονται στο GPS και να ενισχυθεί η αξιοπιστία και η ιχνηλασιμότητα σε σχέση με τον μηχανισμό self-report, που χρησιμοποιείται στις εφαρμογές που χρησιμοποιούν το Bluetooth (Ichiro Nakamoto , et al., 2020).

5.9.1 Εφαρμογές που χρησιμοποιούν QR Code

Εφαρμογή εργαλείου QR Code στην Κίνα

Το εργαλείο QR έχει αναπτυχθεί επίσημα στο Fujian, μια επαρχία που βρίσκεται στη νοτιοανατολική Κίνα και έχει πληθυσμό σχεδόν 40 εκατομμύρια. Σε όλα τα άτομα ηλικίας τριών

ετών και άνω, ζητήθηκε επίσημα να παρουσιάσουν τον ραβδοκώδικα τους κατά τη διάρκεια καθημερινών δημόσιων δραστηριοτήτων, όπως για παράδειγμα, όταν χρησιμοποιούν συστήματα δημόσιας μεταφοράς, εργάζονται σε ιδρύματα και εισέρχονται ή εξέρχονται από σχολεία (Ichiro Nakamoto , et al., 2020).

Στην Κίνα, η κυβέρνηση βασίζεται στον Κώδικα Υγείας, που αναπτύχθηκε από την Alipay και την WeChat, για τον εντοπισμό ατόμων που πιθανόν να έχουν εκτεθεί στο COVID-19. Ο κωδικός βάσει χρώματος μπορεί να καθορίσει τους κινδύνους έκθεσης των ανθρώπων και την ελευθερία κινήσεων με βάση παράγοντες όπως το ιστορικό ταξιδιού, τη διάρκεια του χρόνου που αφιερώνεται σε επικίνδυνες περιοχές και τις σχέσεις με πιθανούς φορείς (Liang, 2020). Ο Κώδικας Υγείας συγκεντρώνει τρείς τύπους δεδομένων, για την μετατροπή του κινδύνου από την έκθεση του κάθε χρήστη, σε κωδικούς βάσει χρώματος (Mozur, et al., 2020).

Κάθε χρήστης είναι απαραίτητο να δώσει τα προσωπικά του στοιχεία, όπως είναι το όνομα, ο εθνικός αριθμός ταυτότητας και η τρέχουσα κατάσταση της υγείας του. Εν συνεχεία, είναι απαραίτητο να γίνει εγγραφή με αναγνώριση προσώπου και να γίνεται συνεχής ενημέρωση για την κατάσταση της υγείας των ατόμων. Η δεύτερη πηγή δεδομένων σχετίζεται με χωρικά – χρονικά δεδομένα, τα οποία καταγράφονται από το Alipay, το WeChat και άλλες εφαρμογές. Τα χωρικά δεδομένα βασίζονται στο GPS των έξυπνων συσκευών και μπορούν να καθορίσουν, εάν οι χρήστες επισκέφθηκαν περιοχές με εκτεταμένη ή συνεχή εξάπλωση, ενώ τα χρονικά δεδομένα μπορούν να εξετάσουν τη διάρκεια του χρόνου που έμεινε κάποιος χρήστης, σε κάποια επικίνδυνη περιοχή. Τέλος, ο Κώδικας Υγείας αναλύει τα δίκτυα χρηστών και τις διαδικτυακές συναλλαγές για να αξιολογήσει εάν οι χρήστες είχαν επικοινωνήσει με πιθανούς φορείς του ιού (Liang, 2020).

Έπειτα οι χρήστες λαμβάνουν ένα QR Code στο smartphone, υποδεικνύοντας τους κινδύνους έκθεσης και την κινητικότητά τους. Οι χρήστες ταξινομούνται σε τρείς χρωματικές κατηγορίες, ανάλογα με τα δεδομένα τους, σε πράσινο, κίτρινο και κόκκινο. Όπως φαίνεται στην παρακάτω εικόνα:

Εικόνα 4 Health QR Code

Ένα πράσινο QR Code υποδηλώνει ότι το άτομο είναι υγιές και μπορεί να μετακινηθεί ελεύθερα στην πόλη. Ενώ ένα κίτρινο ή ένα κόκκινο QR Code, δεν σημαίνει απαραίτητα ότι το άτομο έχει τον ιό, αλλά υποδηλώνει ότι το άτομο έχει μεγαλύτερο κίνδυνο μόλυνσης.

NZ COVID Tracer

Μία ακόμα εφαρμογή που χρησιμοποιεί QR Code είναι αυτή της Νέας Ζηλανδίας, η NZ COVID Tracer, δεν χρησιμοποιεί ούτε Bluetooth, ούτε κοντινή επικοινωνία πεδίου (NFC) ούτε διεπαφές προγραμματισμού εφαρμογών (API), αλλά λειτουργεί μέσω κωδικών QR, οι οποίοι δημιουργούνται για επιχειρήσεις και οργανισμούς όταν εγγράφονται στην εφαρμογή. Οι επίσημοι κωδικοί QR του Υπουργείου Υγείας τοποθετούνται στις εγκαταστάσεις για να «σαρώσουν» οι άνθρωποι όταν φτάνουν και να προσθέσουν τη θέση στο «ψηφιακό ημερολόγιο» των κινήσεών τους, παρέχοντας μια προσωπική ιστορική πορεία σημείων επαφής (Fan Yang, et al., 2020).

Σε αντίθεση με την Κίνα, η διαδικασία στη Νέα Ζηλανδία δεν είναι ούτε αυτοματοποιημένη, ούτε υποχρεωτική, αλλά σύμφωνα με το Google Play υπάρχουν χρήστες με προβλήματα στη σάρωση. Σε περίπτωση οποιουδήποτε είδους μόλυνσης, η εφαρμογή NZ COVID Tracer επιτρέπει στους χρήστες να μοιράζονται με ασφάλεια το ιστορικό check-in τους με ένα εγγεγραμμένο «Contact Tracer».

5.10 Ανίχνευση της τοποθεσίας μέσω CSLI (Cell Site Location Information)

Εκτός από τον καθορισμό της τοποθεσίας μέσω GPS, υπάρχει και το CLSI, όπου είναι αρχεία που αποθηκεύονται από τηλεπικοινωνιακούς φορείς και συλλέγονται κάθε φορά που ένα τηλέφωνο συνδέεται με έναν από τους πύργους κυψέλης τους (cell tower). Καταγράφουν τον ακριβή χρόνο

και τη διάρκεια κάθε σύνδεσης. Η θέση ενός τηλεφώνου μπορεί να περιοριστεί κάπου στη ζώνη λήψης του αντίστοιχου πύργου κυψελών (Julian Sanchez & Matthew Feeney, 2020). Για αστικές περιοχές με υψηλή ένταση κυψελών, μπορεί να χρησιμοποιηθεί μια τεχνική που ονομάζεται «triangulation» για την ακριβή εκτίμηση της τοποθεσίας. Οι αγροτικές περιοχές μπορεί να βλέπουν αρκετά χιλιόμετρα μεταξύ cell towers και επομένως ο καθορισμός των τοποθεσιών είναι λιγότερο ακριβής. Η χρήση τους στις εφαρμογές ανίχνευσης επαφών είναι περιορισμένη.

5.11 Σύνοψη τεχνολογιών GPS – CSLI – Bluetooth

Το CSLI αλλά και το GPS, δεν είναι αρκετά ακριβή για να προσδιορίσουν με αξιοπιστία εάν οι άνθρωποι βρίσκονται εντός της κρίσιμης εμβέλειας των δύο έως τριών μέτρων μεταξύ τους που παρουσιάζει τον μεγαλύτερο κίνδυνο μετάδοσης. Υπό ιδανικές συνθήκες, το GPS μπορεί να εντοπίσει την οριζόντια θέση σε απόσταση περίπου πέντε μέτρων, ενώ οι μετρήσεις κάθετης θέσης είναι συνήθως λιγότερο ακριβείς και εάν οι συνθήκες δεν είναι ιδανικές, όπως συμβαίνει στις περιπτώσεις που ο δέκτης GPS είναι σε εσωτερικούς χώρους, όπου ο κίνδυνος μετάδοσης είναι πολύ υψηλότερος, η ακρίβεια μειώνεται περισσότερο (Julian Sanchez & Matthew Feeney, 2020).

Το GPS μπορεί να έχει ανάλυση 1 μέτρου, αλλά συνηθέστερα είναι 5 έως 20 μέτρα και η τεχνολογία δεν λειτουργεί σε εσωτερικούς χώρους, λειτουργεί άσχημα στη σκιά μεγάλων κτιρίων και κατά τη διάρκεια κάποιας καταιγίδας και χιονοθύελλας (Kitchin, 2020).

Το CSLI είναι λιγότερο αξιόπιστο, τοποθετώντας συνήθως μόνο ένα τηλέφωνο στην ακτίνα ενός μπλοκ της πόλης, ενώ όπως αναφέρθηκε και παραπάνω, είναι ακόμα πιο αναξιόπιστο στις αγροτικές περιοχές και επομένως δεν θα μπορούσε να γίνει διάκριση μεταξύ ατόμων που βρίσκονται σε στενή επαφή και σε άτομα που μοιράζονται για παράδειγμα διαφορετικά δωμάτια ενός ξενοδοχείου.

Ενώ σε ορισμένα μέρη η παρακολούθηση βάσει τοποθεσίας δεν είναι καθόλου λειτουργική, αφού τόσο η παρακολούθηση θέσης CSLI, όσο και το GPS απαιτούν από τις συσκευές να μπορούν να συνδεθούν σε εξωτερικά δίκτυα. Επομένως, δεν θα λειτουργούν σε περιβάλλοντα όπου δεν είναι δυνατή η πρόσβαση σε αυτά (τα δίκτυα), όπως συστήματα υπόγειων δημόσιων συγκοινωνιών και γκαράζ στάθμευσης (Julian Sanchez & Matthew Feeney, 2020).

Η σηματοδότηση (signaling) με Bluetooth, μερικές φορές αντιμετωπίζει παρόμοια σφάλματα με τις παραπάνω τεχνολογίες, ωστόσο είναι σε πολύ μικρότερο βαθμό. Στο Bluetooth, χωρίς να ανιχνεύεται η θέση του χρήστη, το τηλέφωνό χρησιμοποιεί ραδιοκύματα για να διαπιστώσει ποιες άλλες συσκευές βρίσκονται κοντά (Ingram, 2020).

5.12 Blockchain

Εκτός όμως από τις σύγχρονες πλατφόρμες που χρησιμοποιούν ως επί το πλείστων, τεχνολογίες όπως το Bluetooth και το Global Positioning System (GPS). Ορισμένες εφαρμογές έχουν υιοθετήσει επίσης, την χρήση του Blockchain, μιας αναδυόμενης τεχνολογίας που βοηθά στην αποθήκευση δεδομένων με τη μορφή αμετάβλητων μπλοκ. Οι εφαρμογές που χρησιμοποιούν την συγκεκριμένη τεχνολογία, έχουν ένα βασικό πλεονέκτημα, έχουν την ικανότητα μέσω του Blockchain να επικυρώνουν συνεχώς μεταβαλλόμενα δεδομένα και παρέχουν κοινή χρήση πληροφοριών, διατηρώντας παράλληλα το απόρρητο των χρηστών. Επίσης, η τεχνολογία Blockchain επιτρέπει σε άτομα και οργανισμούς από οποιαδήποτε γωνιά του κόσμου να γίνουν μέρος ενός ενιαίου διασυνδεδεμένου δικτύου που διευκολύνει την ασφαλή κοινή χρήση δεδομένων (Vinay Chamola, et al., 2020).

Το απόρρητο που παρέχεται στον χρήστη και η απόδοση της εφαρμογής όσον αφορά τον αποτελεσματικό εντοπισμό των επαφών, θα πρέπει να αποτελούν το κύριο επίκεντρο των εφαρμογών. Οι εφαρμογές δεν έχουν τη δυνατότητα να παρέχουν το απόρρητο στους χρήστες, το κύριο μέλημα σήμερα είναι η αποτελεσματική ανίχνευση χωρίς να διακυβεύεται η ταυτότητα και το απόρρητο των χρηστών (Sheikh Mohammad Idrees, et al., 2020). Αυτό θα μπορούσε να αντιμετωπιστεί σε συστήματα που βασίζονται σε blockchain, καθώς το δίκτυο είναι πλήρως διανεμημένο και οι ταυτότητες των χρηστών γίνονται ανώνυμες στην αρχή. Εκτός από τη διατήρηση του απορρήτου των χρηστών, η εφαρμογή θα πρέπει επίσης να αποδίδει αποτελεσματικά όσον αφορά τον εντοπισμό των πιθανών επαφών, την κάλυψη δικτύου, την πρόληψη λοιμώξεων κ.λπ. Επομένως, το αποκεντρωμένο δίκτυο που βασίζεται σε blockchain θα παρέχει στο δίκτυο προσβασιμότητα και ιχνηλασιμότητα σε παγκόσμιο επίπεδο και θα συνδέει τον μεγαλύτερο αριθμό χρηστών από διαφορετικές γεωγραφικές τοποθεσίες χωρίς να διακυβεύεται το απόρρητό τους. Επιπλέον, οι πληροφορίες που κοινοποιούνται στο blockchain θα μπορούσαν να συλλεχθούν από οποιοδήποτε μέσο τεχνολογίας (Bluetooth, GPS κ.λπ.) (Sheikh Mohammad Idrees, et al., 2020).

Η χρήση των εφαρμογών που βασίζονται στην συγκεκριμένη τεχνολογία είναι εντελώς εθελοντική. Οι χρήστες της εφαρμογής, ακόμα και οι μολυσμένοι, είναι απαραίτητο να ανεβάσουν τα δεδομένα τους, δηλαδή το μοναδικό αναγνωριστικό χρήστη και τις γεωγραφικές πληροφορίες, μετά την εφαρμογή κρυπτογράφησης στο δίκτυο blockchain. Όταν ένας χρήστης πηγαίνει στο διαγνωστικό κέντρο για τη διεξαγωγή του τεστ, τα αποτελέσματα θα μεταφορτώνονται στην εφαρμογή εντοπισμού επαφών blockchain, η οποία θα χαρτογραφήσει το μολυσμένο άτομο έτσι ώστε να πάρει τις λεπτομέρειες των επαφών με τη βοήθεια του διακομιστή. Τα γεωγραφικά

δεδομένα που παρέχονται στους διακομιστές συλλέγονται χρησιμοποιώντας τις ασύρματες τεχνολογίες όπως Wi-Fi, Bluetooth ή GPS κ.λπ. που καταγράφει τις λεπτομέρειες τοποθεσίας των χρηστών (Vinay Chamola, et al., 2020).

Είναι γνωστό ότι υπάρχουν περιπτώσεις διάδοσης ψευδών πληροφοριών, οι οποίες οδηγούν τους ανθρώπους σε πανικό, λόγω των ψευδών πληροφοριών ή των ανακριβών λεπτομερειών που παρέχονται. Η επιλογή ενός δικτύου Blockchain είναι μια πολύ καλή επιλογή, καθώς παρέχει «διαφανή» ανίχνευση επαφών, διατηρώντας ταυτόχρονα το απόρρητο. Η τεχνολογία blockchain παρέχει στους χρήστες τον πλήρη έλεγχο της διαχείρισης των δεδομένων τους καθ' όλη τη διάρκεια του κύκλου ζωής (συνήθως 14 ημέρες) και τους επιτρέπει να τα μοιράζονται και να τα αποσύρουν όποτε θέλουν. Παρόλο που η χρήση συναίνεσης αλγορίθμων θα διασφαλίσει ότι δεν θα προκύψει καμία παραπληροφόρηση, ακόμα κι αν γίνει, οι αρχές μπορούν να καθορίσουν γρήγορα τον εκκινητή μηνυμάτων με βάση την ψηφιακή του υπογραφή. Μια τέτοια πλατφόρμα θα αποτρέψει τους ανθρώπους από το να πέφτουν θύματα ψεύτικων πληροφοριών (Vinay Chamola, et al., 2020) (Sheikh Mohammad Idrees, et al., 2020).

Παρά τα όσα θετικά αναφέρθηκαν παραπάνω, η εφαρμογή blockchain δεν είναι ακόμα αρκετά γνωστή και υπάρχει εκτεταμένη έλλειψη ενημέρωσης σχετικά με την χρήση της και τις δυνατότητες που προσφέρει. Το blockchain, έχει λανθασμένα συνδεθεί μόνο με κρυπτονομίσματα και «δόλιες» δραστηριότητες. Επίσης, οι πλατφόρμες που βασίζονται στην τεχνολογία αυτή, υποφέρουν από έλλειψη επεκτασιμότητας και μέχρι στιγμής, είναι ελάχιστες οι πλατφόρμες που βασίζονται σε blockchain και σχεδόν όλες έχουν εγγενείς περιορισμούς κλιμάκωσης. Τέλος, δεδομένου ότι η τεχνολογία blockchain είναι σχετικά νέα και «ανώριμη», καθίσταται δύσκολη η ενσωμάτωση εφαρμογών blockchain με παλαιά συστήματα (Sheikh Mohammad Idrees, et al., 2020).

Υπάρχουν δύο εφαρμογές που βασίζονται στο blockchain, με στόχο την καταπολέμηση της πανδημίας του COVID-19, η Civitas και η MiPasa. Η Civitas, είναι μια εφαρμογή που μπορεί να βοηθήσει τις τοπικές αρχές σε διάφορα έθνη του κόσμου να ελέγξουν τον COVID-19, συσχετίζει τα επίσημα αναγνωριστικά ατόμων με αρχεία blockchain για να επαληθεύσει εάν το άτομο έχει άδεια να εγκαταλείψει το σπίτι του ή όχι. Επίσης, η εφαρμογή μπορεί να καθορίσει την ιδανική ώρα και μέρα, ελαχιστοποιώντας τον κίνδυνο μόλυνσης. Επιπλέον, η Civitas προσφέρει μια ενσωματωμένη λειτουργικότητα τηλεϊατρικής που επιτρέπει στους γιατρούς να παρακολουθούν τα συμπτώματα των ασθενών τους και να τους στέλνουν σημειώσεις σχετικά με τα φάρμακα που πρέπει να χρησιμοποιηθούν και τις στρατηγικές υγειονομικής περίθαλψης που πρέπει να ακολουθούνται. Σύμφωνα με τους ισχυρισμούς της εταιρείας, η εφαρμογή διασφαλίζει ότι τα

δεδομένα των ατόμων παραμένουν ιδιωτικά και ασφαλή (T. Wright, 2020) (Sheikh Mohammad Idrees, et al., 2020).

Το MiPasa από την άλλη, είναι μια πλατφόρμα ροής δεδομένων, αυτή η πλατφόρμα βασίζεται επίσης στις υπηρεσίες που παρέχονται από το IBM blockchain & τις πλατφόρμες cloud της IBM, για να διευκολύνει την ανταλλαγή επαληθευμένων πληροφοριών σχετικά με την υγεία και την τοποθεσία μεταξύ ατόμων, αρχών και νοσοκομείων. Αυτή η εφαρμογή λειτουργεί συλλέγοντας τις πληροφορίες που παρέχονται από διάφορους ιατρικούς οργανισμούς, υπαλλήλους δημόσιας υγείας και άλλα άτομα (Sheikh Mohammad Idrees, et al., 2020). Ο ΠΟΥ πρόσφατα αναγνώρισε αυτήν την εφαρμογή ως μια αποτελεσματική πλατφόρμα για να βοηθήσει τους γιατρούς να αποκτήσουν πρόσβαση σε επαληθεύσιμες πληροφορίες. Τα διαθέσιμα δεδομένα σε αυτήν την πλατφόρμα μπορούν να βοηθήσουν τα νοσοκομεία να καθορίσουν τα μελλοντικά τους σχέδια δράσης και να διαθέσουν αποτελεσματικά τους πόρους τους (Gari Singh & Jonathan Levi, 2020).

6

Αρχιτεκτονικές Συστημάτων

Υπάρχουν κάποιες αρχιτεκτονικές συστήματος που χρησιμοποιούνται συνήθως ή προτείνονται για την ανάπτυξη εφαρμογών ανίχνευσης COVID-19. Οι δύο βασικές μορφές ψηφιακού εντοπισμού είναι: η κεντρική προσέγγιση (centralized approach), που συχνά χρησιμοποιεί δεδομένα τοποθεσίας κινητού τηλεφώνου και η αποκεντρωμένη προσέγγιση (decentralized approach) που συχνά χρησιμοποιεί ένα πρότυπο Bluetooth μικρής εμβέλειας.

6.1 Κεντρική Προσέγγιση (Centralized Approach)

Στην κεντρική προσέγγιση, οι δημόσιες αρχές συλλέγουν δεδομένα σε έναν κεντρικό διακομιστή όπου γίνεται η αντιστοίχιση μεταξύ δεδομένων. Η ανίχνευση επαφών γίνεται σε κεντρικούς διακομιστές που ζητούν από τους χρήστες που είναι θετικοί στον ιό, να ανεβάσουν όλα τα αναγνωριστικά (πρόσφατα συμβάντα επαφής (contact events) τους). Εν συνεχεία, ο διακομιστής θα αναλύσει αυτά τα συμβάντα για να εντοπίσει όλους τους χρήστες που έχουν βρεθεί στον ίδιο χώρο με αυτό το άτομο (Qingchuan Zhao, et al., 2020). Σε ένα κεντρικό σύστημα, όπου τα μόνιμα αναγνωριστικά των χρηστών μπορούν να συσχετιστούν μεταξύ τους. Ο διακομιστής μπορεί να παρακολουθεί εάν μια θετική αναφορά ακολουθείται από περαιτέρω θετικές αναφορές από τα άτομα με τα οποία έχει έρθει σε επαφή. Όταν μια αρχική θετική αναφορά δεν ακολουθείται από περαιτέρω θετικές αναφορές, η περίπτωση θα μπορούσε να αναγνωριστεί από τον διακομιστή ως πιθανό ψευδώς θετικό και όλες οι επαφές του θα μπορούσαν να απελευθερωθούν γρήγορα από την καραντίνα που πιθανώς, να τους είχε επιβληθεί.

Μπορούν να αποκωδικοποιήσουν τις ταυτότητες των εκτιθέμενων χρηστών, κάτι που επιτρέπει στις υγειονομικές αρχές να ειδοποιούν τους χρήστες αυτούς, σύμφωνα πάντα με τα στοιχεία επικοινωνίας του κάθε χρήστη, συνήθως τον αριθμό κινητού τηλεφώνου που συλλέγεται κατά την εγγραφή του. Οι χρήστες θα γνωρίζουν μόνο ένα «κομμάτι» πληροφοριών: είτε εκτέθηκαν πρόσφατα σε έναν μολυσμένο χρήστη είτε όχι.

Υπάρχουν πολλά πρωτόκολλα διατήρησης απορρήτου που χρησιμοποιούν τον συγκεκριμένο τύπο αρχιτεκτονικής και αναλύονται παρακάτω, όπως είναι το BlueTrace και το ROBERT, αλλά και εφαρμογές όπως η TraceTogether της Σιγκαπούρης και το COVIDSafe της Αυστραλίας. Επομένως, στις κεντρικές εφαρμογές εντοπισμού επαφών, οι πληροφορίες ταυτότητας των χρηστών των εκάστοτε εφαρμογών και η κατάσταση τους (μολυσμένοι, εκτεθειμένοι), ενδέχεται να είναι προσβάσιμες, από τους εργαζομένους στον τομέα της υγείας, τους προγραμματιστές εφαρμογών και τις αρχές υγείας σε πολιτειακό / ομοσπονδιακό επίπεδο (ανάλογα με το επίπεδο που η εφαρμογή έχει αναπτυχθεί) (Tianshi Li, et al., 2020).

Υπάρχουν δύο τρόποι διασφάλισης ότι οι θετικές αναφορές των χρηστών είναι ακριβείς. Στην πρώτη, είναι να απαιτήσουν να γίνει ένα τέστ, ώστε να είναι βέβαιοι για το αποτέλεσμα και στην συνέχεια να αναφερθούν ως θετικοί στην εκάστοτε εφαρμογή. Όμως, ενώ είναι ένας αρκετά καλός τρόπος, αφού διασφαλίζεται η ακρίβεια, υπάρχει πρόβλημα σχετικά με την καθυστέρηση των αποτελεσμάτων. Η δεύτερη επιλογή είναι να επιτραπεί στους χρήστες, να αναφέρουν ότι είναι θετικοί, μόλις εμφανίσουν συμπτώματα. Αυτή η επιλογή, επιταχύνει την διαδικασία, ωστόσο υπάρχει κίνδυνος το σύστημα να γεμίσει με ψευδώς θετικές αναφορές. Επιπλέον, μπορεί να υπάρξουν πολλοί κακόβουλοι χρήστες, οι οποίοι μπορούν να ανοίξουν πολλούς λογαριασμούς σε μια εφαρμογή, με στόχο να μειώσουν τον επαναπροσδιορισμό των ατόμων και τον περιορισμό των ταυτοτήτων των μολυσμένων ατόμων, με αποτέλεσμα να αναιρούνται τα οφέλη της κεντρικής αρχιτεκτονικής.

Όσον αφορά την κεντρική προσέγγιση είναι απαραίτητο να σημειωθούν κάποια συγκεκριμένα πράγματα. Αρχικά, θα πρέπει να διευκρινιστεί ότι μέχρι στιγμής η παρούσα προσέγγιση δεν έχει εφαρμοστεί στην πραγματική ζωή. Τα κεντρικά συστήματα που δοκιμάστηκαν στο Ηνωμένο Βασίλειο και την Αυστραλία εγκαταλείφθηκαν, αφού δεν μπορούσαν να εντοπίσουν με αρκετή ακρίβεια επαφές, όχι λόγω εγγενούς προβλήματος με το σύστημα, αλλά ως αποτέλεσμα της δυσκολίας σχεδιασμού μιας λειτουργικής εφαρμογής σε Android και iPhone χωρίς την υποστήριξη της Apple και της Google, που υποστηρίζουν μόνο αποκεντρωμένες αρχιτεκτονικές εφαρμογών.

Συνοψίζοντας, τα οφέλη στην περίπτωση επιλογής μιας κεντρικής αρχιτεκτονικής, είναι ότι οι επαγγελματίες υγείας μπορούν να επικοινωνήσουν με τους χρήστες που έχουν εκτεθεί στον ιό και να τους καθοδηγήσουν. Όπως επίσης, κανένας χρήστης δεν είναι άμεσα αναγνωρίσιμος στον κεντρικό διακομιστή, αφού ταυτίζεται με το ψευδώνυμο του. Επίσης, υπάρχουν κίνδυνοι απορρήτου, αφού οι εργαζόμενοι στον τομέα της υγείας, οι αρχές της υγείας και οι προγραμματιστές εφαρμογών είναι πιθανόν να γνωρίζουν ποιος εγκατέστησε την εφαρμογή, ποιοι έχουν μολυνθεί και ποιοι έχουν εκτεθεί στον ιό (Tianshi Li, et al., 2020). Οι υποστηρικτές των αποκεντρωμένων συστημάτων επισημαίνουν ότι η αποθήκευση δεδομένων χρήστη σε έναν κεντρικό διακομιστή συνεπάγεται με κινδύνους παραβίασης. Κανένας χρήστης δεν είναι άμεσα αναγνωρίσιμος στον κεντρικό διακομιστή, επειδή ταυτίζεται με το ψευδώνυμο, αλλά, είναι αρκετά εύκολο για τις κυβερνήσεις να λάβουν τις πληροφορίες αυτές, επιτρέποντας τους να παρακολουθούν τους πολίτες και να υπάρξει η πιθανότητα διαβίβασης τους για την επιβολή του νόμου ή για κάποιον άλλο σκοπό.

Τέλος, μπορούμε να αντιληφθούμε ότι παρά τις απόψεις των υποστηρικτών των αποκεντρωμένων συστημάτων, τα κεντρικά συστήματα εάν είναι εξοπλισμένα με κατάλληλη δευτερογενή πρόληψη θα μπορούσαν να ελαχιστοποιήσουν τον συνολικό ηθικό κίνδυνο. Ένας κεντρικός σχεδιασμός αυξάνει την πιθανότητα αποτελεσματικής ανίχνευσης επαφών και, συνεπώς, ενδέχεται να είμαστε σε μια κατάσταση όπου είναι προτιμότερο ένα κεντρικό σχέδιο, μόνο όμως εάν οι σχετικοί κίνδυνοι παραβίασης μπορούν να ελαχιστοποιηθούν επαρκώς μέσω δευτερογενών προληπτικών μέτρων, όπως αναφέρθηκαν και παραπάνω.

6.2 Αποκεντρωμένη Προσέγγιση (Decentralized Approach)

Στην αποκεντρωμένη αρχιτεκτονική, οι κεντρικοί διακομιστές συλλέγουν αναγνωριστικά αναγνωρισμένων χρηστών και τα «ωθούν» σε κάθε εγγεγραμμένο χρήστη. Οι μοναδικοί κωδικοί που δημιουργούνται μέσω ενός συμβάντος επαφής καταγράφονται στη συσκευή κάθε ατόμου και δεν μεταδίδονται σε κεντρικό διακομιστή. Η επεξεργασία των δεδομένων γίνεται μόνο όταν ένας από τους χρήστες έχει μολυνθεί από τον ιό. Το περιεχόμενό του περιορίζεται σε άτομα με τα οποία ο ασθενής έχει στενή επαφή. Με τη δημιουργία μικρότερων ομάδων δεδομένων, το αποκεντρωμένο μοντέλο προσφέρει καλύτερη προστασία από κακόβουλες δραστηριότητες μεγάλης κλίμακας ή κυβερνητικές «καταχρήσεις», όπως για παράδειγμα η δημιουργία κοινωνικών γραφημάτων (Emre Kursat Kaya, 2020). Υπάρχουν πολλά πρωτόκολλα ανίχνευσης επαφών που διατηρούν το απόρρητο, όπως το DP-3T, (East) PACT, (West) Pact και το Notification Exposure, τα οποία χρησιμοποιούν μια τέτοια αποκεντρωμένη αρχιτεκτονική (Qingchuan Zhao, et al., 2020).

Οι κρυπτογράφοι υποστηρίζουν ότι τόσο τα κεντρικά όσο και τα αποκεντρωμένα συστήματα είναι ευάλωτα σε επιθέσεις hacking, αλλά τα τρωτά τους σημεία διαφέρουν. Στα αποκεντρωμένα συστήματα είναι πιθανές οι επιθέσεις που μπορούν να εκθέσουν τις ταυτότητες των μολυσμένων χρηστών, αφού όπως αναφέρθηκε και παραπάνω, όταν ένας χρήστης αποκεντρωμένου συστήματος αναφέρει ότι έχει μολυνθεί από τον ιό, όλα τα προσωπικά του στοιχεία μεταφορτώνονται στον κεντρικό διακομιστή, όπου είναι προσβάσιμα σε όλους. Αυτό καθιστά δυνατή την εγγραφή των προσωρινών αναγνωριστικών που μεταδίδονται από συγκεκριμένους χρήστες και στην συνέχεια τον μετέπειτα έλεγχο έναντι των αναγνωριστικών που είναι αποθηκευμένα στον διακομιστή. Τέτοιες επιθέσεις, υποστηρίζει ο Vaudenay, «θα μπορούσαν να διεξαχθούν από οποιονδήποτε χρήστη με γνώση της τεχνολογίας» (Serge Vaudenay, 2020).

Από την άλλη, τα κεντρικά συστήματα είναι πολύ ευάλωτα σε επιθέσεις hacking, ένας hacker μπορεί να είναι θέση να αναγνωρίσει τους χρήστες των εφαρμογών μέσω των κεντρικά αποθηκευμένων μόνιμων ψευδώνυμων αναγνωριστικών τους, καθώς και τις ταυτότητες των ατόμων με τα οποία έχουν έρθει σε επαφή. Ο Serge Vaudenay υποστηρίζει ότι μια τέτοια επίθεση θα ήταν δύσκολο να επιτευχθεί και πιθανότατα θα απαιτούσε από μια κακόβουλη κυβερνητική αρχή να αποθηκεύει πρόσθετες πληροφορίες, καθώς εγγράφεται ένας χρήστης της εφαρμογής (Serge Vaudenay, 2020).

Οι χρήστες που έχουν επίγνωση της ιδιωτικής ζωής, είναι λιγότερο πιθανό να αναφέρουν ότι έχουν μολυνθεί σε ένα αποκεντρωμένο σύστημα, σε σχέση με ένα κεντρικό. Οι πληροφορίες που αποθηκεύονται με αποκεντρωμένο τρόπο θα μπορούσαν να χρησιμοποιηθούν από την επιβολή του νόμου, για παράδειγμα, μετά από μια διάρρηξη κατά τη διάρκεια της οποίας ένας αισθητήρας Bluetooth κατέλαβε ένα εφήμερο αναγνωριστικό, οι ύποπτοι θα μπορούσαν να έχουν τα τηλέφωνά τους «ανοιχτά» για ανακάλυψη πληροφοριών για 2 εβδομάδες και να βρεθούν αποδεικτικά στοιχεία. Τα δικά του εφήμερα αναγνωριστικά αποθηκεύονται στο τηλέφωνο κάποιου άλλου σε ένα αποκεντρωμένο σύστημα, η πρόσβαση στο τηλέφωνο κάποιου θα απέδιδε περισσότερες πληροφορίες από ότι σε ένα κεντρικό σύστημα.

Η παραπάνω αρχιτεκτονική προσφέρει καλύτερη επιδημιολογική χρήση των δεδομένων και τα οφέλη που προκύπτουν σχετίζονται με το γεγονός ότι η εφαρμογή ανίχνευσης επαφών, μπορεί να ενημερώσει τους εκτεθειμένους χρήστες και να παρέχει οδηγίες. Υπάρχει όμως μεγάλος κίνδυνος όσον αφορά τους χρήστες που γνωρίζουν την τεχνολογία, επειδή ενδέχεται να μπορούν να συμπεράνουν τις ταυτότητες ορισμένων μολυσμένων χρηστών με τους οποίους έχουν επικοινωνήσει. Καταγρά,φοντας με αυτόν τον τρόπο, πρόσθετες πληροφορίες τοποθεσίας ή ανοίγοντας πολλούς λογαριασμούς.(Qingchuan Zhao, et al., 2020)Επίσης, θεωρούνται ότι

διαφυλάσσουν την προστασία της ιδιωτικής ζωής, ωστόσο ενέχουν σημαντικούς ηθικούς κινδύνους, καθώς είναι λιγότερο πιθανό να είναι αποτελεσματικοί στην συγκράτηση της πανδημίας και η ενδεχόμενη αποτυχία τους θα συνεπάγεται με πιθανή βλάβη (πχ οικονομική).

Σύμφωνα με τους Lucie και τον Philippe van Basshuysen, μπορούμε να αναμένουμε ότι οι παραβιάσεις θα είναι πιο πιθανές σε διεσπαρμένα αποκεντρωμένα συστήματα, αλλά λιγότερο πιθανές και πιο σοβαρές, σε πιο ολοκληρωμένα κεντρικά συστήματα. Στα αποκεντρωμένα συστήματα, είναι αρκετά ανησυχητικές οι επιθέσεις οι οποίες μπορούν να εκθέσουν τις ταυτότητες των μολυσμένων χρηστών

Όπως υποστηρίξαμε στην προηγούμενη ενότητα, οι κεντρικές εφαρμογές είναι πιο πιθανό να διαθέτουν αποτελεσματικά μέσα για την καταπολέμηση της πανδημίας. Λαμβάνοντας υπόψη τους πιθανούς κινδύνους και τα οφέλη κάθε επιλογής, πρέπει να επανεξετάσουμε την υπόθεση ότι οι αποκεντρωμένες εφαρμογές είναι σαφώς ηθικά ανώτερες.

6.3 Εφαρμογές – Πρωτόκολλα που βασίζονται στην Κεντρική Αρχιτεκτονική

Τα κύρια πρωτόκολλα που χρησιμοποιούνται και βασίζονται στην Κεντρική Αρχιτεκτονική (Centralized Architecture) είναι τα: Bluetrace, ROBERT και το Aarogya Setu, τα οποία αναλύονται παρακάτω.

Bluetrace

Το πρωτόκολλο Bluetrace, χρησιμοποιείται από την εφαρμογή TraceTogether, η οποία χρησιμοποιείται στην Σιγκαπούρη και ακολουθεί μια κεντρική προσέγγιση. Οι χρήστες καταγράφουν τους αριθμούς τηλεφώνου τους στην υπηρεσία backend, η οποία παρέχει τυχαία αναγνωριστικά που σχετίζονται με αυτούς τους αριθμούς και χρησιμοποιούνται όταν δύο έξυπνες συσκευές «συναντώνται» (BlueTrace, 2020). Όμως, σε περίπτωση που κάποιος χρήστη βρεθεί θετικός στον ιό, θα πρέπει να κοινοποιηθεί το ιστορικό συνάντησης του με την υγειονομική αρχή, η οποία μπορεί να λάβει τον αριθμό τηλεφώνου του μολυσμένου ατόμου, καθώς και τον αριθμό των ατόμων που ήρθαν σε επαφή με το μολυσμένο άτομο. Γίνεται αντιληπτό ότι με βάση τον σχεδιασμό του BlueTrace, η υπηρεσία backend μπορεί να έχει πρόσβαση στις προσωπικές πληροφορίες των χρηστών (Tania Martin, et al., 2020) (NADEEM AHMED, et al., 2020).

Άλλη μια εφαρμογή που ακολουθεί το συγκεκριμένο πρωτόκολλο είναι το CovidSafe, το οποίο κυκλοφόρησε η Αυστραλιανή Κυβέρνηση και διαθέτει πολλά παρόμοια χαρακτηριστικά με την εφαρμογή TraceTogether της Σιγκαπούρης. Οι εφαρμογές διαφέρουν ως προς την διάρκεια των

tempIDs. Το TraceTogether χρησιμοποιεί την τιμή των 15 λεπτών, η οποία συνίσταται και από τις προδιαγραφές του πρωτοκόλλου BlueTrace, ενώ το CovidSafe έχει διάρκεια 2 ώρες. Το γεγονός αυτό, καθιστά την εφαρμογή CovidSafe πιο ευάλωτη σε επαναλαμβανόμενες επιθέσεις (CovidSafe, 2020). Ενώ, ο διακομιστής στο TraceTogether, εκδίδει tempIDs με ημερομηνία προώθησης σε κάθε συσκευή, αντί για ένα μόνο tempID. Αυτό γίνεται για να διασφαλιστεί ότι κάθε συσκευή, διαθέτει παροχή έγκυρων tempID ακόμα και όταν η σύνδεση στο διαδίκτυο είναι ασταθής. Το σχετικό πλεονέκτημα του CovidSafe έναντι του TraceTogether είναι ότι οι συσκευές δεν χρειάζεται να λαμβάνουν συχνά TempIDs. Μια ακόμα διαφορά μεταξύ των δύο εφαρμογών είναι στην υποδομή backend, ενώ η TraceTogether χρησιμοποιεί το Google Cloud για την παροχή υπηρεσιών backend, η CovidSafe κάνει χρήση διακομιστών Amazon AWS που βρίσκονται στην Αυστραλία (NADEEM AHMED, et al., 2020).

ROBERT

Το πρωτόκολλο ανίχνευσης ROBERT (Robust and Privacy-Preserving Proximity Tracing) είναι ένα κεντρικό πρωτόκολλο, το οποίο αναπτύχθηκε από κοινού από ερευνητές της INRIA (Γαλλία) και του Fraunhofer (Γερμανία). Το πρωτόκολλο ROBERT επιτρέπει σε ένα άτομο που είναι θετικός στον Covid-19, να μεταδίδει ψευδώνυμα των αναγνωριστικών των smartphone με τα οποία έχουν έρθει σε επαφή με κεντρικούς διακομιστές. Κάθε smartphone που είναι εξοπλισμένο με την εφαρμογή ελέγχει περιοδικά αυτούς τους κεντρικούς διακομιστές για να επιβεβαιώσει ότι ένα από τα ψευδώνυμα του δεν είναι εκεί, πράγμα που θα σήμαινε ότι ο ιδιοκτήτης του ενδέχεται να έχει μολυνθεί.

AAROGYA SETU

Το Aarogya Setu, είναι μια εφαρμογή που δημιουργήθηκε στην Ινδία βασιζόμενη στην κεντρική προσέγγιση. Η εφαρμογή συλλέγει δεδομένα προσωπικής ταυτοποίησης PII (Gathering of Personally Identifiable Information), όπου σύμφωνα με το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST), το PII ορίζεται ως: «οποιεσδήποτε πληροφορίες μπορούν να χρησιμοποιηθούν για τη διάκριση ή τον εντοπισμό της ταυτότητας ενός ατόμου, όπως όνομα, αριθμός κοινωνικής ασφάλισης, ημερομηνία και τόπο γέννησης, πατρικό όνομα μητέρας ή βιομετρικά αρχεία και οποιαδήποτε άλλη πληροφορία που συνδέεται με ένα άτομο, όπως ιατρικές, εκπαιδευτικές, οικονομικές και εργασιακές πληροφορίες» (Wikipedia, n.d.). Η συλλογή PII είναι οποιαδήποτε δραστηριότητα που συλλέγει, οργανώνει, χειρίζεται, αναλύει, ανταλλάσσει ή κοινοποιεί αυτά τα δεδομένα. Επίσης, η εφαρμογή συλλέγει δεδομένα τοποθεσίας και δεδομένα

αυτό-αξιολόγησης (απαντήσεις που παρέχονται από ένα άτομο στη δοκιμή αυτό-αξιολόγησης) (NADEEM AHMED, et al., 2020).

Η εφαρμογή εκτελεί αναλύσεις δεδομένων στις πληροφορίες που έχουν συγκεντρωθεί, για να δείξει πόσες θετικές περιπτώσεις υπάρχουν σε απόσταση μεταξύ 500 μέτρων με 10 χιλιομέτρων, από την τρέχουσα τοποθεσία του χρήστη (NADEEM AHMED, et al., 2020) (A Review of India's Contact-tracing App, 2020). Οι χρήστες μπορούν να ανεβάσουν τα δεδομένα παρακολούθησης, εάν είναι θετικοί στον ιό, ή απέτυχαν στην αυτό–αξιολόγηση. Στην συγκεκριμένη εφαρμογή, όπως έχει αναφερθεί και σε προηγούμενη ενότητα, η κυβέρνηση της Ινδίας έχει καταστήσει υποχρεωτική την εγκατάσταση της για όλους τους κυβερνητικούς υπαλλήλους.

6.4 Εφαρμογές – Πρωτόκολλα που βασίζονται στην Αποκεντρωμένη Αρχιτεκτονική

Google Apple Exposure Notification (GAEN)

Η Google και η Apple συνέβαλαν στην καταπολέμηση του COVID-19 χρησιμοποιώντας την τεχνολογία Bluetooth, για να βοηθήσουν τις κυβερνήσεις και τους οργανισμούς υγειονομικής περίθαλψης στον περιορισμό της εξάπλωση του ιού. Το συγκεκριμένο σύστημα έχει σχεδιαστεί, λαμβάνοντας υπόψη τη σημασία του απορρήτου και της ασφάλειας των χρηστών.

Το Google / Apple ENS επιτρέπει σε συσκευές iPhone ή Android να εντοπίζουν άλλες συσκευές που βρίσκονται σε μια συγκεκριμένη απόσταση για σημαντική διάρκεια. Η «χειραψία» (handshake) θα προκαλέσει την αποθήκευση μοναδικών κωδικών αναγνώρισης, σε κρυπτογραφημένη μορφή, και στις δύο συσκευές (Laura Bradford, et al., 2020). Όπως συμβαίνει και στις άλλες εφαρμογές που χρησιμοποιούν το πρωτόκολλο Bluetooth, έτσι και σε αυτή, κάθε 10-20 λεπτά δημιουργούνται νέα τυχαία αναγνωριστικά, έτσι ώστε να διατηρηθεί το απόρρητο του χρήστη και να μην είναι δυνατή η ανίχνευση της ταυτότητας του ή της γεωγραφικής του θέσης.

Η συσκευή του χρήστη θα συνεχίζει να ανταλλάσσει τα τυχαία αναγνωριστικά μέσω Bluetooth, με άλλες συσκευές που βρίσκονται σε κοντινή απόσταση. Τα δεδομένα συλλέγονται, αποθηκεύονται και υποβάλλονται σε επεξεργασία μόνο στη συσκευή του χρήστη. Εάν, ανά πάσα στιγμή, ένας χρήστης διαγνωστεί θετικός, ενημερώνει την εφαρμογή για την κατάστασή της υγείας του. Οι συσκευές άλλων χρηστών ταυτίζουν όλα τα τυχαία αναγνωριστικά με θετικές περιπτώσεις COVID-19. Καθ' όλη τη διάρκεια της διαδικασίας, η ταυτότητα του χρήστη δεν

κοινοποιείται σε κανέναν, ούτε καν με την Google και την Apple (Sheikh Mohammad Idrees, et al., 2021)

PACT

Υπάρχουν δύο διαφορετικά πρωτόκολλα με αυτό το όνομα. Το Private Automated Contact Tracing (PACT), είναι το πρωτόκολλο που αναπτύχθηκε κυρίως από ερευνητές του Ινστιτούτου Τεχνολογίας της Μασαχουσέτης (MIT) και φέρει ομοιότητες με άλλες σχετικές αποκεντρωμένες λύσεις όπως TCN, DP-3T και PACT Westcoast. Το άλλο είναι το Privacy sensitive protocols And mechanisms for mobile Contact Tracing (PACT - Westcoast), το οποίο αναπτύχθηκε από μία ομάδα του πανεπιστημίου της Ουάσιγκτον. Για τον ορθό διαχωρισμό αυτών των δύο πρωτοκόλλων, το πρωτόκολλο που αναπτύχθηκε στο MIT ονομάζεται «PACT East Coast», ενώ το άλλο, «PACT Westcoast» (NADEEM AHMED, et al., 2020).

PACT East Coast

Στο συγκεκριμένο πρωτόκολλο, η εφαρμογή του χρήστη δημιουργεί ψευδοτυχαία αναγνωριστικά, τα οποία ονομάζονται chirps και αλλάζουν κάθε μερικά λεπτά. Τα chirps μεταδίδονται με την χρήση της τεχνολογίας BLE και αποθηκεύονται τοπικά στο τηλέφωνο του χρήστης, έως και 3 μήνες. Οι εφαρμογές που λαμβάνουν, μπορούν να αποθηκεύσουν προαιρετικά τα chirps μέχρι 3 μήνες, αλλά και να αποθηκεύσουν την τοποθεσία συνάντησης (Tania Martin, et al., 2020).

Για την καλύτερη κατανόηση θα πάρουμε ως παράδειγμα τον Bob και την Alice, είναι απαραίτητο να υπάρχει δυνατότητα η Alice να μπορεί να προσδιορίσει τον κίνδυνο για το αν θα προσβληθεί από την ασθένεια και σε ποιον βαθμό, εάν έχει έρθει σε επαφή με κάποιο μολυσμένο άτομο. Για τον λόγο αυτό, η Alice αλληλεπιδρά με μια βάση δεδομένων που θα την βοηθήσει να καθορίσει το επίπεδο έκθεσης της. Στο υψηλό επίπεδο, αντιστοιχεί μια καταχώρηση στη βάση δεδομένων από τον Bob, ο οποίος είναι θετικός. Τα chirps που αντιστοιχούν στη συσκευή του Bob, είναι απλοί τυχαίοι αριθμοί, οι οποίοι δεν μπορούν να συνδεθούν με πληροφορίες που αναγνωρίζουν τον Bob. Εάν όμως ο Bob δεν είχε έρθει σε επαφή με κανέναν, τα chirps δεν θα αποκαλύψουν τίποτα για τον αυτόν. Για την Alice που ήρθε σε επαφή με τον Bob, θα γίνει σύγκριση των chirps που βρίσκονται στην βάση δεδομένων, με αυτά που αποθηκεύονται στο ημερολόγιο επαφών της, έτσι ώστε να μπορεί να δει ότι ήρθε σε επαφή με μολυσμένο άτομο. Η εφαρμογή μπορεί να σχεδιαστεί για να εμφανίζει άμεσα όλα τα μεταδεδομένα στην Alice ή απλά να λέει στην Alice μόνο τον βαθμό έκθεσης της (Ronald L. Rivest, et al., 2020).

Οι επαγγελματίες υγείας λαμβάνουν τα chirps από τα άτομα που έχουν μολυνθεί από τον ιό μέσα από μια κεντρική βάση δεδομένων, στην οποία έχουν πρόσβαση μέσω one-time κωδικών. Ανά τακτά χρονικά διαστήματα, οι εφαρμογές κάνουν download την βάση δεδομένων και ελέγχουν εάν τα chirps που περιέχονται στη βάση δεδομένων, υπάρχουν και στη λίστα των τοπικών επαφών τους.

PACT West Coast

Το πρωτόκολλο αυτό, αναπτύχθηκε κυρίως από ερευνητές από το Πανεπιστήμιο της Ουάσιγκτον και βασίζεται στον ορισμό ενός δωρεάν πλαισίου τρίτου μέρους για την ανίχνευση επαφών μέσω κινητού. Οι ερευνητές-συγγραφείς ορίζουν ένα σύνολο πρωτοκόλλων για την ενίσχυση πτυχών απορρήτου διατηρώντας τα δεδομένα των χρηστών στα smartphone τους (Tania Martin, et al., 2020). Αυτή η προσέγγιση σχετίζεται με το σύστημα DP-3T, καθώς μόνο τα μολυσμένα άτομα θα μπορούν να μοιράζονται τα δεδομένα τους σε εθελοντική βάση (NADEEM AHMED, et al., 2020).

Temporary Contact Number (TCN)

Το πρωτόκολλο προσωρινού αριθμού επαφής, είναι ένα αποκεντρωμένο πρωτόκολλο παρακολούθησης επαφών που βασίζεται στην ανταλλαγή προσωρινών αναγνωριστικών 128-bit μεταξύ των κοντινών smartphone που χρησιμοποιούν BLE. Αυτά τα αναγνωριστικά είναι ψευδοτυχαία και δημιουργούνται τοπικά στο smartphone. Όταν ο χρήστης βρεθεί θετικός στον ιό δημιουργείται μια αναφορά, η οποία αποστέλλεται σε έναν κεντρικό διακομιστή με εκτεθειμένη τη λίστα TCN. Οι συσκευές χρηστών «τραβούν» αυτήν την αναφορά και προσδιορίζουν το αντίστοιχο TCN για να δουν εάν ο χρήστης έχει εκτεθεί (Vikram Sharma Mailthody, et al., 2021). Ένα από τα χαρακτηριστικά του TCN είναι ότι η συμμετοχή των υγειονομικών αρχών είναι προαιρετική. Εάν εμπλέκεται κάποια υγειονομική αρχή, τα αποτελέσματα των δοκιμών επαληθεύονται με υπογραφή από την υγειονομική αρχή για να εγγυηθεί την ακεραιότητα της έκθεσης. Εάν όχι, ο χρήστης δημιουργεί μια αυτό-αναφορά για τα συμπτώματά του, για να ενημερώσει άλλους χρήστες που βρίσκονται κοντά (Tania Martin, et al., 2020).

Decentralised Privacy-Preserving Proximity Tracing (DP-3T)

Το πρωτόκολλο του Αποκεντρωμένου Εντοπισμού Εγγύτητας Διατήρησης Απορρήτου, βασίζεται στη μετάδοση αναγνωριστικών (ID) μέσω Bluetooth Low Energy (BLE) από το smartphone του χρήστη. Σε περίπτωση που εντοπιστεί ένα μολυσμένο άτομο, το smartphone του, εξουσιοδοτείται να στείλει τα αναγνωριστικά του στο backend, το οποίο με τη σειρά του μεταδίδει τα

αναγνωριστικά στους χρήστες του συστήματος. Με αυτόν τον τρόπο, κάθε χρήστης που λαμβάνει συγκρίνει τα λαμβανόμενα αναγνωριστικά με τη λίστα των αποθηκευμένων αναγνωριστικών και σε περίπτωση αντιστοίχισης ταυτότητας, η εφαρμογή ειδοποιεί το χρήστη ότι έχει έρθει σε επαφή με ένα μολυσμένο άτομο (Tania Martin, et al., 2020).

Στο DP-3T ο κεντρικός διακομιστής αναφοράς δεν έχει ποτέ πρόσβαση σε αρχεία καταγραφής επαφών και επειδή τα αρχεία αυτά, δεν διαβιβάζονται ποτέ σε τρίτα μέρη, έχει σημαντικά οφέλη απορρήτου έναντι της προσέγγισης PEPP-PT, που αναλύεται παρακάτω. Ωστόσο αυτό επιβαρύνεται με την ανάγκη περισσότερης υπολογιστικής ισχύος από την πλευρά του client για την επεξεργασία αναφορών μόλυνσης (Wikipedia, 2020).

Το πρωτόκολλο λειτουργεί μέσω της μετάδοσης μεταβαλλόμενων εφήμερων αναγνωριστικών Ephemenal IDs (EphIDs), τα οποία αποστέλλονται μέσω BLE beacons. Το DP-3T χρησιμοποιεί 16 byte Ephemeral IDs (EphID) για τον μοναδικό εντοπισμό συσκευών κοντά στον client, αυτά τα EphID καταγράφονται τοπικά στη συσκευή ενός πελάτη που λαμβάνει και δεν μεταδίδονται ποτέ σε τρίτους. Τα αναγνωριστικά αυτά δημιουργούνται από ένα secret key (SK_t), που αντιπροσωπεύει την τρέχουσα ημέρα. Το κλειδί ανανεώνεται καθημερινά χρησιμοποιώντας μια λειτουργία κατακερματισμού, για την οποία ισχύει:

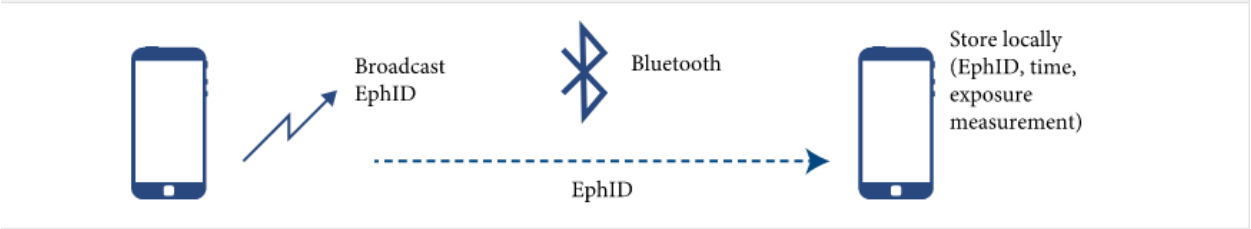
$$\mathrm{SK}_t t \;\; H\,\mathrm{SK}_t = H(\mathrm{SK}_{t-1})$$

όπου το H() είναι μια κρυπτογραφική συνάρτηση κατακερματισμού, το SK0 υπολογίζεται από έναν τυπικό αλγόριθμο secret key ED25519. Είναι ένα σύστημα αλυσίδας κατακερματισμού, όπου εάν τεθεί σε κίνδυνο ένα κλειδί, τότε αποκαλύπτονται όλα τα επόμενα SK, άλλα όχι τα SK που βρίσκονται πριν από αυτό (Tania Martin, et al., 2020) (Wikipedia, 2020).

Στη συνέχεια, χρησιμοποιείται για την παραγωγή ενός συνόλου EphIDs χρησιμοποιώντας μια ψευδοτυχαία συνάρτηση (PRF), (ας πούμε, HMAC-SHA-256) και μια ψευδοτυχαία γεννήτρια (PRG), (ας πούμε, AES) σε λειτουργία μετρητή: SKt

$$\mathrm{EphID}_1 \| \cdots \| \mathrm{EphID}_n = \mathrm{PRG}\left(\mathrm{PRF}\left(\mathrm{SK}_t, \text{"broadcast key"}\right)\right).$$

Για να αποφευχθεί η παρακολούθηση τοποθεσίας, κάθε EphID έχει περίοδο ισχύος μερικών λεπτών, τα EphID λαμβάνονται από κοντινούς χρήστες μέσω διαφημίσεων BLE (advertisements). Στη συνέχεια, κάθε EphID αποθηκεύεται από αυτούς τους χρήστες μαζί με μια μέτρηση έκθεσης, π.χ. εξασθένηση σήματος και την ημέρα λήψης του σήματος. Στο παρακάτω σχήμα παρατηρούμε την παραπάνω διαδικασία:



Εικόνα 5 DP-3T processing and storing of observed EphIDs

Επιπλέον, η εφαρμογή κάθε χρήστη αποθηκεύει τοπικά τα κλειδιά της που δημιουργήθηκαν τις τελευταίες 14 ημέρες. Εάν ένας χρήστης διαγνωστεί θετικός από την υγειονομική αρχή (η αρχή είναι υπεύθυνη για την κοινοποίηση των αποτελεσμάτων των δοκιμών), τότε ενεργοποιείται η διαδικασία εντοπισμού εγγύτητας. Τότε το άτομο που έχει επιβεβαιωθεί ότι είναι θετικό, μέσω κωδικού εξουσιοδότησης, ανεβάζει το κλειδί SKt, την πρώτη ημερά που θεωρήθηκε θετικό (Carmela Troncoso, et al., 2020). Το backend συλλέγει τα ζεύγη (SKt, t) θετικών χρηστών COVID-19 και τα τηλέφωνα κατεβάζουν περιοδικά αυτά τα ζεύγη. Με αυτές τις πληροφορίες, οι χρήστες έχουν τη δυνατότητα να υπολογίζουν τη λίστα των EphID που σχετίζονται με ένα συγκεκριμένο ζεύγος. Σε περίπτωση που ένα τέτοιο EphID περιλαμβάνεται στον αποθηκευμένο κατάλογό του χρήστη, συμπεραίνουμε ότι ο χρήστης ήρθε σε επαφή με κάποιο μολυσμένο άτομο.

Η παραπάνω προσέγγιση ονομάζεται Αποκεντρωμένη ανίχνευση εγγύτητας χαμηλού κόστους (Low-cost decentralized proximity tracing), ωστόσο υπάρχουν άλλες δύο προσεγγίσεις. Η μία είναι η «unlinkable decentralised proximity tracing», η οποία αποσκοπεί στην παροχή καλύτερων ιδιοτήτων απορρήτου. Σε αυτήν την περίπτωση, όταν ένας χρήστης διαγνωστεί ως μολυσμένος, μπορεί να αποφασίσει ποια αναγνωριστικά κοινοποιούνται για να αποφευχθεί η πιθανή σύνδεση των EphID. Και η τρίτη προσέγγιση ονομάζεται υβριδική αποκεντρωμένη ανίχνευση εγγύτητας (hybrid decentralised proximity tracing), στην οποία τα seeds δημιουργούνται και χρησιμοποιούνται για τη δημιουργία εφήμερων αναγνωριστικών σύμφωνα με τον πρώτο σχεδιασμό, αλλά τα seeds ανεβαίνουν μόνο σε περίπτωση που σχετίζονται με την εκτίμηση έκθεσης για άλλους χρήστες. Με αυτόν τον τρόπο, η προστασία από τη σύνδεση εφήμερων αναγνωριστικών ενισχύεται σε σύγκριση με τη σχεδίαση χαμηλού κόστους, αλλά η προστασία παρακολούθησης είναι ασθενέστερη από ό, τι για τον unlinkable decentralized (Tania Martin, et al., 2020).

Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT)

Το πρωτόκολλο PEPP-PT είναι κατασκευασμένο για την διευκόλυνση του εντοπισμού επαφών οι οποίοι είναι θετικοί στον ιό. Το πρωτόκολλο αυτό, είναι το ανταγωνιστικό πρωτόκολλο του DP-3T και χρησιμοποιεί την τεχνολογία Bluetooth Low Energy. Οι σχετικές εφαρμογές θα ενημερώνουν τους χρήστες, με βάση τα σήματα Bluetooth του τηλεφώνου, εάν ήταν κοντά σε ένα άτομο που είχε δοκιμαστεί θετικά για το COVID-19 (Dan Cooper, et al., 2020). Σε αντίθεη με το DP-3T, το πρωτόκολλο PEPP-PT, χρησιμοποιεί έναν κεντρικό διακομιστή για να επεξεργάζεται αρχεία καταγραφής επαφών και να ενημερώνει μεμονωμένα τα άτομα για πιθανή επαφή με έναν μολυσμένο ασθενή. Υποστηρίζεται ωστόσο, ότι η παραπάνω προσέγγιση θέτει σε κίνδυνο την ιδιωτική ζωή (Wikipedia, 2020).

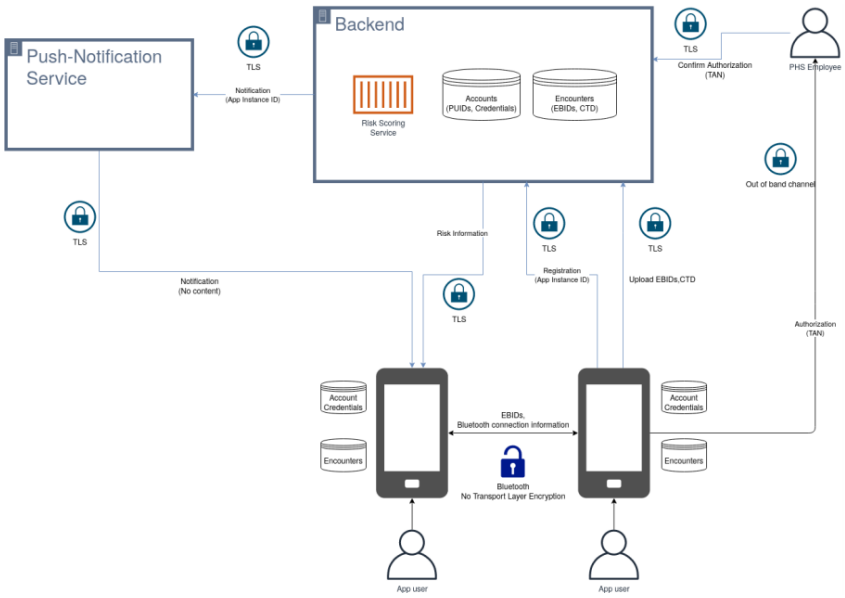
Κατά την εγγραφή απαιτείται έλεγχος ταυτότητας για την αποτροπή κακόβουλων παραγόντων, όπως τη δημιουργία πολλαπλών ψεύτικων λογαριασμών, οι οποίοι χρησιμοποιούνται ως παρέμβαση στο σύστημα. Για να διατηρηθεί η ανωνυμία των χρηστών, το πρωτόκολλο χρησιμοποιεί έναν συνδυασμό proof-of-work challenge (PoW) και CAPTCHA. Το πρώτο καθιστά τις μαζικές καταχωρίσεις ακριβείς και αποτρέπει τις επιθέσεις DoS με εξειδικευμένα αλλά μη εξουσιοδοτημένα αιτήματα και το δεύτερο απαιτεί ανθρώπινη αλληλεπίδραση. Μετά το πρωτόκολλο εγγραφής, το backend διαθέτει ένα μοναδικό τυχαίο ψευδώνυμο 128-bit του χρήστη, που ονομάζεται PUID (PEPP-PT, 2020).

Όταν δύο άτομα συναντηθούν, ανταλλάσσονται και καταγράφονται τα στοιχεία αναγνώρισης, για να μην γίνεται όμως παρακολούθηση των χρηστών, γίνεται ανταλλαγή προσωρινών αναγνωριστικών από τον κεντρικό διακομιστή. Για να δημιουργηθούν αυτά τα προσωρινά αναγνωριστικά, ο κεντρικός διακομιστής δημιουργεί ένα καθολικό μυστικό κλειδί, το οποίο χρησιμοποιείται για τον υπολογισμό όλων των προσωρινών αναγνωριστικών για ένα σύντομο χρονικό διάστημα t (Wikipedia, 2020). Από το παραπάνω υπολογίζεται ένα Ephemeral Bluetooth ID (EBID), για κάθε χρήστη, τα οποία χρησιμοποιούνται από τους χρήστες ως προσωρινά αναγνωριστικά για ανταλλαγή. Στην συνέχεια, οι χρήστες μεταδίδουν τα EBIDs κάτω από το αναγνωριστικό PEPP-PT Bluetooth, ενώ ταυτόχρονα πραγματοποιείται και σάρωση για άλλους χρήστες.

Εάν ένας χρήστης επιβεβαιωθεί ότι είναι θετικός στον ιό, ζητείται από τον ασθενή να «ανεβάσει» τα αρχεία καταγραφής επαφών του στον κεντρικό διακομιστή. Εάν ο χρήστης συναινεσει με το παραπάνω, η αρχή υγείας εκδίδει ένα κλειδί που του επιτρέπει την μεταφόρτωση. Στη συνέχεια, ο χρήστης μεταδίδει το αρχείο καταγραφής επαφών μέσω HTTPS στον διακομιστή αναφοράς για επεξεργασία. Μόλις ληφθεί το αρχείο από τον διακομιστή, κάθε καταχώρηση εκτελείται μέσω

ενός αλγορίθμου ελέγχου εγγύτητας για την μείωση της πιθανότητας ψευδών θετικών. Η λίστα που προκύπτει, επιβεβαιώνεται χειροκίνητα και μαζί με ένα τυχαίο δείγμα άλλων χρηστών, αποστέλλεται ένα μήνυμα που περιέχει έναν τυχαίο αριθμό και ένα κατακερματισμένο μήνυμα. Το μήνυμα αυτό χρησιμοποιείται για την «αφύπνιση» του πελάτη, ώστε να ελέγξει τον διακομιστή για νέες αναφορές (Wikipedia, 2020). Εάν ο χρήστης βρίσκεται στο τυχαίο δείγμα, θα λάβει μία απάντηση χωρίς νόημα. Ο λόγος για τον οποίο σε ένα τυχαίο δείγμα χρηστών αποστέλλεται ένα μήνυμα για κάθε αναφορά, είναι ότι οι υποκλοπείς δεν μπορούν να προσδιορίσουν ποιος κινδυνεύει από μόλυνση «ακούγοντας» την επικοινωνία μεταξύ του πελάτη και του διακομιστή (PEPP-PT, 2020).

Το παρακάτω σχήμα απεικονίζει τα στοιχεία και τα δεδομένα που αποθηκεύονται, καθώς και τις αλληλεπιδράσεις μεταξύ στοιχείων και χρηστών.



6.5 *Άλλα πλαίσια*

OpenCovidTrace

Η συγκεκριμένη πλατφόρμα είναι ανοιχτού κώδικα και ακολουθεί μια αποκεντρωμένη προσέγγιση. Ενσωματώνει όλα τα πρωτόκολλα παρακολούθησης επαφών BLE, DP-3T, Google & Apple Exposure Notification και Bluetrace, με ένα επιπλέον σύνολο λειτουργειών για πλατφόρμες iOS και Android. Αυτή η ενσωμάτωση προβλέπεται να διευκολύνει τη διαλειτουργικότητα μεταξύ ανοιχτού κώδικα, όπως στην περίπτωση του DP-3T και ιδιόκτητων πλατφορμών, συμπεριλαμβανομένων των Google / Apple Exposure Notification και BlueTrace. (Anon.,

2020)Το OpenCovidTrace ακολουθεί τις αρχικές προδιαγραφές DP-3T, όταν χρησιμοποιείται το πλαίσιο Google /Apple Exposure Notification, τα ψευδοτυχαία προσωρινά αναγνωριστικά δημιουργούνται τοπικά στο smartphone του χρήστη, ακολουθώντας την προσέγγιση DP-3T. Εάν ο χρήστης αναφέρει ότι έχει συμπτώματα, η εφαρμογή στέλνει στον κεντρικό διακομιστή τα IDs που χρησιμοποιήθηκαν για τη δημιουργία των προσωρινών αναγνωριστικών και την τοποθεσία του χρήστη, τις τελευταίες 14 ημέρες. Περιοδικά, η εφαρμογή κατεβάζει τα κλειδιά των χρηστών από τον διακομιστή, που αναφέρουν συμπτώματα και πληροφορίες σχετικά με το ποιος ήταν στην ίδια περιοχή με τον αιτούντα χρήστη. Εάν υπάρξει κάποιος που βρέθηκε στην ίδια τοποθεσία και είναι τελικά θετικός, ο χρήστης ειδοποιείται ότι ίσως να κινδυνεύει (Tania Martin, et al., 2020).

DESIRE

Το συγκεκριμένο σύστημα ενσωματώνει διαφορετικές πτυχές κεντρικών και αποκεντρωμένων μοντέλων και ακολουθεί την αρχιτεκτονική ROBERT. Στην αρχιτεκτονική αυτή, ο διακομιστής διαχειρίζεται risk scores και ειδοποιήσεις, ωστόσο, η προσέγγιση βασίζεται στην έννοια του Private Encounter Tokens (PET), τα οποία δημιουργούνται ιδιωτικά από τους χρήστες και συνεπώς είναι αποσυνδεδεμένα. Ο διακομιστής προορίζεται να κάνει το ταίριασμα μεταξύ των PET που παρέχονται από τους χρήστες που είναι θετικοί στον ιό, με τα PET των αιτούντων. Τέλος, οι πληροφορίες που φιλοξενούνται από τον διακομιστή κρυπτογραφούνται με κρυπτογραφικά κλειδιά, τα οποία ωστόσο αποθηκεύονται τοπικά στα smartphone των χρηστών.

7

Παροχή υγειονομικής περίθαλψης μέσω νέων τεχνολογιών

7.1 Τεχνητή Νοημοσύνη

Υπάρχουν αρκετές εφαρμοσμένες στρατηγικές που βασίζονται σε Artificial Intelligence (AI) και μπορούν να υποστηρίξουν τις υπάρχουσες τυπικές μεθόδους αντιμετώπισης του COVID-19 σε συστήματα υγειονομικής περίθαλψης σε όλο τον κόσμο. Ο κίνδυνος μόλυνσης είναι συνάρτηση πολλών παραγόντων, που σχετίζονται με την ηλικία, το ιστορικό ταξιδιού, την τρέχουσα κατάσταση υγείας και το ιατρικό οικογενειακό ιστορικό. Η ολοκληρωμένη ανάλυση αυτών των παραγόντων που ενσωματώνεται στις τεχνικές AI, μπορεί να προσφέρει μια πιο ακριβή και αξιόπιστη πρόβλεψη μεμονωμένων προφίλ κινδύνου.

Οι τεχνικές AI και κυρίως οι αλγόριθμοι μηχανικής μάθησης, μπορούν να χρησιμοποιηθούν για να συσχετιστούν οι παράμετροι δεδομένων του ασθενούς με τη χρήση ενός συγκεκριμένου φαρμάκου. Αυτοί οι συσχετισμοί είναι χρήσιμοι γιατί μπορούν να χρησιμοποιηθούν για την πρόβλεψη της επίδρασης του φαρμάκου σε μια συγκεκριμένη ομάδα ασθενών. Η προληπτική γνώση των παραπάνω, είναι πιθανό να επιτρέψει στα μέλη της ιατρικής κοινότητας να προετοιμαστούν καλύτερα για τις ενδεχόμενες συνέπειες. Από τα παραδείγματα χρήσης της τεχνολογίας AI που παρουσιάζονται παρακάτω, είναι σημαντικό να σημειωθεί ότι η AI είναι πιο κατάλληλη, για να βοηθήσει στον έλεγχο των ασθενών με COVID-19 παρά να διαγνώσει τις περιπτώσεις τελείως. Για να είναι σε θέση να διαγνώσει με ακρίβεια κάθε ασθενής που είναι

θετικός στον COVID-19, οι συσκευές AI, οι πλατφόρμες και οι αλγόριθμοι πρέπει να είναι αρκετά ισχυρές ώστε να ανιχνεύουν όλες τις πιθανές μεταλλάξεις του ιού.

Ιατρική διάγνωση και έλεγχος - Medical Diagnosis and Screening

Σαρωτές Προσώπου (Face Scanners)

Όπως είναι ήδη γνωστό, μετά το ξέσπασμα του COVID-19, οι αρχές διαφόρων χωρών χρησιμοποίησαν σαρωτές θερμοκρασίας υπέρυθρων, σε διάφορους δημόσιους χώρους για τη θερμομέτρηση του πληθυσμού. Το αρνητικό όμως σε αυτή την τεχνολογία, ήταν η υποχρεωτική παρουσία προσωπικού για την διεξαγωγή της σάρωσης, για τον λόγο αυτό, αρκετά νοσοκομεία, αεροδρόμια και ιατρικά κέντρα, υιοθέτησαν τη χρήση φωτογραφικών μηχανών με τεχνολογία πολλαπλών αισθητήρων που βασίζονται σε AI. Οι κάμερες αυτές επιτρέπουν στις αρχές να παρακολουθούν τον πληθυσμό, να αναγνωρίζουν τα άτομα με υψηλές θερμοκρασίες σώματος, αλλά και να αναγνωρίζουν τα πρόσωπα τους και να μελετούν τις κινήσεις τους. Ένα από τα πρώτα νοσοκομεία που έκανε χρήση της συγκεκριμένης τεχνολογίας ήταν το νοσοκομείο ampa General Hospital στη Φλόριντα των ΗΠΑ, το οποίο εγκατέστησε μια κάμερα με δυνατότητα τεχνητής νοημοσύνης στην είσοδό του για να ελέγξει όλους τους εισερχόμενους ασθενείς για αυξημένες θερμοκρασίες σώματος δίνοντάς τους θερμική σάρωση προσώπου.

Ιατρική Απεικόνιση (Medical Imaging)

Η χρήση εργαλείων με δυνατότητα AI, μπορεί να αποβεί σωτήρια, αφού είναι δυνατή η ανάλυση των αξονικών τομογραφιών (CT) και των ακτίνων X, με αποτέλεσμα να μπορεί να εξοικονομήσει χρόνο από τους ακτινολόγους, προσφέροντας πιο έγκαιρη ιατρική διάγνωση από τις τρέχουσες δοκιμές για το COVID-19. Για το σκοπό αυτό, έχουν ήδη καταβληθεί πολλές προσπάθειες για τη χρήση ιατρικής απεικόνισης με δυνατότητα AI για τη διάγνωση του COVID-19.

Μια start up εταιρεία που βρίσκεται στο Πεκίνο και ειδικεύεται στη δημιουργία πλατφόρμας ογκολογικών δεδομένων πραγματοποιεί ανάλυση ιατρικών δεδομένων. Το LinkingMed, έχει παρουσιάσει ένα μοντέλο που βασίζεται σε AI για τον έλεγχο της πνευμονίας μέσω ανάλυσης αξονικής τομογραφίας. Η πνευμονία ως γνωστόν, είναι ένα από τα κοινά κλινικά χαρακτηριστικά του COVID-19 και η αναγνώριση της παρουσίας πνευμονίας μπορεί να βοηθήσει στον εντοπισμό μολυσμένων ατόμων.

Παρόλο που η χρήση τεχνικών ιατρικής απεικόνισης με AI, θεωρείται ότι έχει μεγάλες δυνατότητες στη διάγνωση του ιού , αρκετοί ακτινολόγοι έχουν εκφράσει ορισμένα ζητήματα σχετικά με αυτές τις τεχνικές. Πρώτον, η έλλειψη αμερόληπτων δεδομένων εμποδίζει την

απόδοση των μοντέλων AI. Δεύτερον, η χρήση τεχνικών ιατρικής απεικόνισης μπορεί δυνητικά να μολύνει τον εξοπλισμό που χρησιμοποιείται και μπορεί να προκαλέσει περαιτέρω εξάπλωση της νόσου.

Σύστημα Ανίχνευσης Φωνής COVID-19 (COVID-19 Voice Detection Systems)

Η απλούστερη τεχνολογία η οποία μπορεί να χρησιμοποιηθεί για τον εντοπισμό πιθανών κρουσμάτων COVID-19, είναι η ανίχνευση φωνής. Οι εφαρμογές ανίχνευσης φωνής απαιτούν από τους χρήστες να παρέχουν εθελοντικά ένα δείγμα της φωνής τους, βάσει του οποίου η εφαρμογή αποφασίζει εάν ένα άτομο έχει συμπτώματα του COVID-19 ή όχι. Παράδειγμα τέτοιας εφαρμογής για κινητές συσκευές, έχει αναπτυχθεί από τους φοιτητές του Ινστιτούτου Βιο-Τεχνολογίας και Βιομηχανικής στην Ινδία. Για την χρήση της εφαρμογής, είναι απαραίτητο ο χρήστης να μιλήσει στο μικρόφωνο της συσκευής του. Στη συνέχεια η εφαρμογή διασπά τον ήχο σε πολλές παραμέτρους συμπεριλαμβανομένης της συχνότητας και της παραμόρφωσης του θορύβου. Τέλος, οι τιμές αυτών των παραμέτρων συγκρίνονται με τις τιμές παραμέτρων ενός μέσου ατόμου για να προσδιοριστεί εάν ένα άτομο ενδέχεται να μολυνθεί από τον COVID-19.

Θεραπευτική έρευνα και Τεχνητή Νοημοσύνη

Η τεχνολογία AI μπορεί να αποδειχθεί ιδιαίτερα ωφέλιμη για την επιτάχυνση της διαδικασίας ανάπτυξης φαρμάκων. Αρκετά εργαστήρια έχουν υιοθετήσει την χρήση AI για τον εντοπισμό πιθανών θεραπειών για τον COVID-19. Το AI μπορεί να επισπεύσει τη διαδικασία ανάπτυξης φαρμάκων, αλλά και να βοηθήσει στη διαδικασία ανακάλυψης υπαρχόντων φαρμάκων.

Αρχικά, η μηχανική μάθηση (machine learning – ML), η οποία αποτελεί ένα υποσύνολο της AI, έχει αποδείξει την αποτελεσματικότητα της, στην ανάπτυξη φαρμάκων. Χαρακτηριστικό παράδειγμα αποτελεί χρήση των μοντέλων Bayesian ML, τα οποία επιτάχυναν τη διαδικασία ανακάλυψης μοριακών αναστολέων κατά τη διάρκεια της επιδημίας του Έμπολα. Με την ίδια λογική, τα μοντέλα ML, μπορούν να βοηθήσουν και στην παρούσα πανδημία, επιταχύνοντας τη διαδικασία ανάπτυξης φαρμάκων που μπορούν ενδεχομένως να χρησιμοποιηθούν για τη θεραπεία του COVID-19.

Όσον αφορά τη διαδικασία ανακάλυψης υπαρχόντων φαρμάκων, μια νεοσύστατη εταιρεία με έδρα τη Γερμανία με την επωνυμία Innoplexus AG έχει ασκήσει τη χρήση της πλατφόρμας ανακάλυψης φαρμάκων με τεχνολογία AI για να προσδιορίσει έναν συνδυασμό υπαρχόντων φαρμάκων που μπορεί να αποδειχθούν χρήσιμα στη θεραπεία του COVID-19 (Vinay Chamola, et al., 2020). Μετά από εκτενή ανάλυση των υπαρχόντων δεδομένων που σχετίζονται με το COVID-19, η πλατφόρμα τους αποκάλυψε ότι το Chroloquine, ένα φάρμακο κατά της ελονοσίας, μπορεί να λειτουργήσει καλύτερα σε συνδυασμό με το Remdesivir (ένα πειραματικό αντιικό που

αναπτύχθηκε αρχικά για τη θεραπεία του Ebola) ή το Tocilizumab (ένα ανοσοκατασταλτικό φάρμακο) ή Pegasys (χρησιμοποιείται για τη θεραπεία της ηπατίτιδας B & C) ή Clarithromycin (ένα αντιβιοτικό) (Mamumi Das, 2020). Παρόλη την προσπάθεια που καταβάλλεται για την ανακάλυψη θεραπειών, όπως την παραπάνω, είναι πολύ απίθανο κάποια από αυτές να είναι διαθέσιμη σύντομα.

Επαλήθευση Πληροφοριών AI

Κατά τη διάρκεια του ξεσπάσματος του ιού, ξεκίνησαν αρκετές θεωρίες συνωμοσίας, καθώς και η παραπληροφόρηση των πολιτών, σε πλατφόρμες κοινωνικής δικτύωσης. Για τον περιορισμό των ψεύτικων αυτών ειδήσεων και για την παροχή ειδήσεων, οι οποίες είναι επαληθευμένες, εταιρείες τεχνολογίας όπως η Google, το Youtube και το Facebook, προσπάθησαν να καταπολεμήσουν τα κύματα των θεωριών συνωμοσίας, της παραπληροφόρησης και του κακόβουλου λογισμικού, χρησιμοποιώντας AI (Mamumi Das, 2020).

Μια αναζήτηση για coronavirus ή COVID-19, δίνει ένα σήμα προειδοποίησης σε συνδυασμό με συνδέσμους προς επαληθευμένες πηγές πληροφοριών. Συγκεκριμένα το Youtube, έχει θέσει αυστηρά μέτρα για την κατάργηση οποιωνδήποτε βίντεο που διαδίδουν ψεύτικες ειδήσεις, αφού συνδέει απευθείας τους χρήστες με τον ΠΟΥ και παρόμοιους αξιόπιστους οργανισμούς για πληροφορίες. Τα βίντεο για εσφαλμένη πληροφόρηση καθαρίζονται και καταργούνται αμέσως μόλις μεταφορτωθούν (Samer Obeidat, 2020) .

Εν κατακλείδι, η Τεχνητή Νοημοσύνη μπορεί να διαδραματίσει σημαντικό ρόλο στον περιορισμό των επιπτώσεων της πανδημίας, όμως, προς το παρόν τα συστήματα Τεχνητής Νοημοσύνης βρίσκονται ακόμα στα προκαταρκτικά στάδια. Οι διάφορες προκλήσεις και οι περιορισμοί που εμποδίζουν την εφαρμογή της AI στη διαχείριση των επιπτώσεων του COVID-19 περιγράφονται παρακάτω.

Τα μοντέλα AI απαιτούν σημαντική ποσότητα εκπαιδευτικών δεδομένων, ώστε να είναι αξιόπιστα και να δώσουν ακριβή αποτελέσματα. Ωστόσο, λόγω της άνευ προηγουμένου φύσης της πανδημίας, υπάρχει έλλειψη δεδομένων ώστε τα μοντέλα τεχνητής νοημοσύνης να είναι «εκπαιδευμένα». Η χρήση τεχνικών AI για την παρακολούθηση του πλήθους θεωρείται από πολλούς ως παραβίαση της ιδιωτικής ζωής. Αν και οι άνθρωποι έχουν αντιληφθεί το γεγονός ότι οι ανησυχίες για τη δημόσια υγεία είναι πιο σημαντικές από τις ανησυχίες περί απορρήτου δεδομένων. Οι παγίδες απορρήτου που σχετίζονται με τη χρήση της τεχνητής νοημοσύνης έχουν ενσταλάξει το αίσθημα φόβου στο κοινό, αν και οι κυβερνήσεις ενδέχεται να συνεχίσουν να παρακολουθούν ακόμη και μετά την πανδημία.

7.2 IoT & IoMT

Το «Διαδίκτυο των Ιατρικών Πραγμάτων» (Internet of Medical Things – IoMT), είναι συγχώνευση ιατρικών συσκευών και εφαρμογών λογισμικού, που προσφέρουν εκτεταμένες υπηρεσίες υγειονομικής περίθαλψης και συνδέονται με τα συστήματα υγειονομικής περίθαλψης IT.

Τα τελευταία χρόνια λόγω της ραγδαίας ανάπτυξης των κινητών συσκευών, οι οποίες πλέον είναι εξοπλισμένες με αναγνώστες NFC (Near Field Communication), αυξήθηκε ο ρυθμός εγκατάστασης εφαρμογών IoMT. Οι εφαρμογές αυτές περιλαμβάνουν την παρακολούθηση των ασθενών από απομακρυσμένη τοποθεσία, την παρακολούθηση παραγγελιών φαρμάκων και την χρήση wearables, για τη μετάδοση πληροφοριών για την υγεία, στους ενδιαφερόμενους επαγγελματίες υγείας. Οι εφαρμογές έχουν την ικανότητα να συλλέγουν, να αναλύουν και να διαβιβάζουν δεδομένα για την υγεία.

Λόγω του Covid-19, αρκετοί οργανισμοί και κυβερνητικοί φορείς προσπαθούν να αξιοποιήσουν τα εργαλεία IoMT, ώστε να αποδεσμεύσουν και να μειώσουν το «βάρος» στα συστήματα υγειονομικής περίθαλψης. Υπάρχουν λοιπόν διάφορες τεχνολογίες IOT και IOMT, οι οποίες έχουν συμβάλει στην παρακολούθηση, αλλά και στην διαχείριση των επιπτώσεων της πανδημίας, τέτοιες είναι: Smart Thermometers, IoT Buttons καιTelemedicine.

Smart Thermometers – Έξυπνα Θερμόμετρα

Τα θερμόμετρα αυτά δημιουργήθηκαν πριν οκτώ χρόνια από την αμερικανική εταιρεία Kinsa. Αναπτύχθηκαν για να ελέγξουν άτομα με πολύ υψηλό πυρετό και να παρακολουθήσουν την κοινή γρίπη. Μετά το ξέσπασμα του COVID-19, η εταιρεία δημιούργησε περισσότερα από ένα εκατομμύρια Smart Thermometers, αφού θεωρήθηκαν εξαιρετικά χρήσιμα στον εντοπισμό πιθανών κρουσμάτων σε όλες τις ΗΠΑ. Τα θερμόμετρα συνδέονται με μία εφαρμογή για κινητά, η οποία τους επιτρέπει να διαβιβάζουν αμέσως τις μετρήσεις στην εταιρεία. Μόλις λάβει η εταιρεία τα αποτελέσματα, δημιουργούνται ημερήσιοι χάρτες, οι οποίοι δείχνουν ποιες περιοχές των ΗΠΑ έχουν αύξηση των πυρετών, προκειμένου οι αρχές να εντοπίσουν πιθανά σημεία (Vinay Chamola, et al., 2020).

IoT Buttons

Τα IoT Buttons, είναι ηλεκτρονικά κουμπιά, ονομάζονται Wanda QuickTouch και λειτουργούν με μπαταρία. Έχουν διαμορφωθεί για χρήση σε οποιαδήποτε επιφάνεια ανεξάρτητα από το μέγεθος τους, προκειμένου να εκδώσουν άμεσες ειδοποιήσεις στη διοίκηση, προειδοποιώντας τους για τυχόν προβλήματα υγιεινής ή συντήρησης που ενδέχεται να θέσουν σε κίνδυνο τη δημόσια

ασφάλεια (M S Abubakari & Mashoedah, 2021). Ένα αξιοσημείωτο χαρακτηριστικό αυτών των κουμπιών είναι η ανεξαρτησία τους σε εξωτερικές υποδομές, αφού έχουν την ικανότητά να κολλάνε σε οποιαδήποτε διαθέσιμη επιφάνεια. Αρκετά νοσοκομεία στο Βανκούβερ έχουν εγκαταστήσει τέτοια κουμπιά, προκειμένου να διατηρηθούν οι υψηλές προδιαγραφές καθαρισμού και να περιοριστούν οι νοσοκομειακές λοιμώξεις (Vinay Chamola, et al., 2020).

Τηλεϊατρική – Telemedicine

Η χρήση τεχνολογιών IoMT για τη διευκόλυνση της παρακολούθησης απομακρυσμένων ασθενών ονομάζεται τηλεϊατρική. Η πρακτική αυτή επιτρέπει στους γιατρούς να αξιολογούν την κατάσταση της υγείας των ασθενών, χωρίς να χρειάζεται φυσική τους παρουσία. Μετά την εμφάνιση του COVID-19, αρκετές πλατφόρμες τηλεϊατρικής IoMT, είχαν μεγάλη αύξηση «επισκέψεων». Τα οφέλη από την υιοθέτηση τεχνικών τηλεθεραπείας είναι διπλά, γιατί μειώνεται και το υπερβολικό προσωπικό του νοσοκομείου που θα απαιτούνταν σε κανονικές συνθήκες, αλλά και ο κίνδυνος εκπομπής του ιού, από τα μολυσμένα άτομα σε άλλους ασθενείς ή στο προσωπικό του νοσοκομείου (Vinay Chamola, et al., 2020).

Χαρακτηριστικό παράδειγμα χρήσης τέτοιων μεθόδων είναι η Ινδία, όπου οι κρατικές κυβερνήσεις της Άντρα Πράντες και της Ασσάμ, έχουν αναπτύξει εγκαταστάσεις τηλεϊατρικής για να επιτρέψουν την απομακρυσμένη αλληλεπίδραση δυνητικών ασθενών με COVID-19 (Covid-19: AP Launches Telemedicine Facility., 2020).

Παρά την ύπαρξη πολλών εργαλείων τηλεϊατρικής, μπορεί να χρησιμοποιηθεί μόνο όταν οι υπάρχουσες πλατφόρμες τηλεϊατρικής χρησιμοποιούνται σε συνδυασμό με άλλες τεχνολογίες, όπως drones, ρομπότ, 5G δίκτυα και wearable συσκευές. Στις παρακάτω ενότητες, παρουσιάζονται οι τέσσερις αυτές τεχνολογίες που συνδέονται με IoT και έχουν μεγάλο αντίκτυπο στη μάχη ενάντια στο COVID-19.

7.3 Drones

Τα Μη Στελεχωμένα Αεροσκάφη (drones) στην πανδημία του COVID-19 μπορούν να προσφέρουν πολλά πλεονεκτήματα. Μπορούν να διασφαλίσουν την ελαχιστοποιημένη ανθρώπινη αλληλεπίδραση, αλλά και να χρησιμοποιηθούν για να φθάσουν σε δυσπρόσιτες περιοχές. Πολλές χώρες σε όλο τον κόσμο, έχουν υιοθετήσει την τεχνολογία drone. Τα οφέλη που μπορούν να προκύψουν από την χρήση των drones, αναλύονται παρακάτω.

Στην Ινδία η εταιρεία Cyinet έχει παραχωρήσει στην αστυνομία της Τελανγκάνα τεχνολογία μην επανδρωμένης παρακολούθησης για την διαχείριση της πανδημίας. Τα drones, είναι εξοπλισμένα με κάμερες παρακολούθησης, οι οποίες μπορούν να παρακολουθούν αποτελεσματικά περιοχές

που παρουσιάζουν «ευαισθησία» και επιτρέπουν στην αστυνομία να χειρίζεται τις καταστάσεις που μπορεί να προκύψουν. Στο Νέο Δελχί οι αρχές χρησιμοποιούν drones για να περιορίσουν την εξάπλωση του ιού, ονομάζονται drone «corona battle» και μπορούν να μετρήσουν την θερμοκρασία πολλαπλών ατόμων. Τα drones αυτά είναι εξοπλισμένα με θερμική κάμερα για τον έλεγχο των ατόμων, με κάμερα νυχτερινής όρασης για την παρακολούθηση του πλήθους, ένα φορητό ιατρικό κουτί για τη μεταφορά βασικών ιατρικών προμηθειών, ένα μεγάφωνο για την πραγματοποίηση ανακοινώσεων και μια δεξαμενή απολυμαντικών με χωρητικότητα 10 λίτρων για την απολύμανση δημόσιων χώρων.

Στην Ελλάδα οι συζητήσεις για την χρήση των drones από τις αρχές επιβολής του νόμου, ξεκίνησαν από το Μάρτιο του 2020. Στόχος της ΕΛ.ΑΣ, ο έλεγχος των μετακινήσεων των πολιτών εν όψει των περιοριστικών μέτρων λόγω COVID-19, ώστε να είναι βέβαιοι ότι τα μέτρα τηρούνται. Αλλά και να γίνονται περιπολίες σε καταστήματα και επιχειρήσεις, προκειμένου αυτές να προστατευθούν από πιθανές εγκληματικές ενέργειες. Εξαιτίας των δύο παραπάνω παραγόντων οι κάμερες των drones, θα πρέπει να περιλαμβάνουν στο καρέ τους ανθρώπους, δηλαδή την λήψη και την επεξεργασία της εικόνας που θα λαμβάνουν κάθε φορά. Η εικόνα όμως των ατόμων είναι αναγκαίο να μπορεί να εξακριβωθεί, με αποτέλεσμα αυτό να αποτελεί πράξη επεξεργασίας προσωπικών δεδομένων. Το γεγονός ότι τα drones της ΕΛ.ΑΣ. είναι εξοπλισμένα με κάμερα υψηλής ανάλυσης ημέρας, θα μπορούσε να οδηγήσει στην υπόθεση ότι η επεξεργασία εικόνας ενδέχεται να αποτελέσει και επεξεργασία βιομετρικών δεδομένων, ήτοι ειδικής κατηγορίας προσωπικών δεδομένων.(Αντιγόνη Λογοθέτη, et al., 2020)Βιομετρικά, είναι τα δεδομένα προσωπικού χαρακτήρα, τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου, τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα (Άρθρο 44 παρ.1 ιβ)) του Ν. 4624/2019).

Σύμφωνα με την Ομάδα Εργασίας, η χρήση drones από αρχές επιβολής του νόμου, όπως είναι η ΕΛ.ΑΣ., συνιστά άμεση επέμβαση στα δικαιώματα του σεβασμού, της ιδιωτικής ζωής και της προστασίας των προσωπικών δεδομένων, όπως αυτά προστατεύονται στο άρθρο 8 της Ευρωπαϊκής Σύμβασης για τα Δικαιώματα του Ανθρώπου και στα άρθρα 7 και 8 του Ευρωπαϊκού Χάρτη Θεμελιωδών Δικαιωμάτων. Σε σχετικό προεδρικό διάταγμα 98/2019, δεν περιλαμβάνονται οι αναγκαίες διασφαλίσεις για αποφυγή καταχρήσεων εξουσίας από την ΕΛ.ΑΣ. και τα drones αυτής, ούτε παραπέμπει με σαφή τρόπο στις κείμενες γενικές διατάξεις προστασίας προσωπικών δεδομένων. Δεν ορίζεται πουθενά στο εθνικό νομικό πλαίσιο η διαδικασία και οι προϋποθέσεις για την χρήση των drones, Τα κριτήρια για την τήρηση της αναλογικότητας μεταξύ των

χρησιμοποιούμενων μέσων και του επιδιωκόμενου σκοπού, το είδος των προσωπικών δεδομένων που τυγχάνουν επεξεργασίας, τη συλλογή, αποθήκευση, και διαβίβαση των δεδομένων, τους αποδέκτες των δεδομένων, τη διάρκεια διατήρησης και τη διαδικασία διαγραφής, τα οργανωτικά και τεχνικά μέτρα για την ασφάλεια της επεξεργασίας των δεδομένων, την περιοδική αξιολόγηση της αποτελεσματικότητας του μέτρου αυτού, καθώς επίσης και τα δικαιώματα των υποκειμένων των δεδομένων και τον τρόπο άσκησής τους. Επομένως, δεν είναι δυνατή η χρήση των drones από την ΕΛ.ΑΣ, αφού δεν πληρούνται οι αρχές της νομιμότητας, της αναγκαιότητας και της αναλογικότητας.

Εκτός όμως από την παρακολούθηση των πολιτών, τα drones μπορούν να χρησιμοποιηθούν για την μετάδοση σημαντικών μηνυμάτων. Χαρακτηριστικό παράδειγμα αποτελεί η Μαδρίτη, όπου οι αστυνομικές αρχές χρησιμοποίησαν drone, που ήταν εξοπλισμένο με μεγάφωνο για να ενημερώσει τους ανθρώπους για τις οδηγίες που έχουν τεθεί σχετικά με την κατάσταση έκτακτης ανάγκης που επιβλήθηκε.

Παρά το οφέλη που μπορούν να προκύψουν από την χρήση των drones για την καταπολέμηση της πανδημίας, υπάρχουν και κάποιοι περιορισμοί. Τα ευάλωτα σημεία στις λειτουργίες drone, όπως το GPS-jamming και το hacking, καθιστούν τα drone μια ελκυστική προοπτική για κακόβουλους χρήστες να διεξάγουν κυβερνοτρομοκρατία και άλλες παράνομες δραστηριότητες. Τα τελευταία χρόνια, πολλές υπηρεσίες επιβολής του νόμου έχουν εκφράσει τις ανησυχίες τους σχετικά με τους κινδύνους ασφαλείας που θέτουν τα drones.

7.4 Robots

Τα ρομπότ και τα AVs, έχουν παρόμοια λειτουργία με τα drones και στόχο έχουν να βοηθήσουν στον περιορισμό της εξάπλωσης του COVID-19. Η χρήση των ρομπότ έχει πολλαπλά οφέλη για τον άνθρωπο. Αρχικά, μπορούν να διαδραματίσουν σημαντικό ρόλο στην απολύμανση χώρων, χρησιμοποιώντας μεθόδους UV ελεγχόμενης απολύμανσης, για τον περιορισμό της μεταφοράς και κατά συνέπεια της εξάπλωσης της νόσου. Το παραπάνω είναι πιο πρακτικό, σε σχέση με την χειροκίνητη απολύμανση από ένα για παράδειγμα συνεργείο καθαρισμού, που με αυτόν τον τρόπο βάζουν σε κίνδυνο την προσωπική τους υγεία.

Τέτοια ρομπότ χρησιμοποιούνται σε αρκετές χώρες ανά τον κόσμο, με χαρακτηριστικό παράδειγμα το τρίτροχο ρομπότ που κατασκευάστηκε στην Ινδία. Το συγκεκριμένο ρομπότ, μπορεί να χρησιμοποιηθεί για να βοηθήσει τους ασθενείς που διαμένουν σε απομόνωση. Είναι ικανό να κάνει εργασίες, όπως να σερβίρει φαγητό στους ασθενείς και να τους δίνει φάρμακα,

μειώνοντας με αυτόν τον τρόπο τις υποχρεώσεις των εργαζομένων στον τομέα της υγείας, ενώ παράλληλα τους «απελευθερώνουν» από τον κίνδυνο να προσβληθούν και αυτοί από τον ιό.

Wearable Συσκευές

Λόγω της τρέχουσας κατάστασης, διάφοροι οργανισμοί τροποποίησαν τις ήδη υπάρχουσες wearables συσκευές, για να βοηθήσουν στην διαχείριση των επιπτώσεων του COVID-19. Προς υπενθύμιση, wearable συσκευές είναι αυτές που φοριούνται στο σώμα και συνδέονται με το διαδίκτυο, με κύριο σκοπό την παρακολούθηση της σωματικής υγείας του ατόμου. Χαρακτηριστικό παράδειγμα αποτελεί μια καινοτόμα ιδέα που σχεδιάζεται από μια νεοσύστατη εταιρεία Silicon Valley, για να κυκλοφορήσει ένα νέο αδιάβροχο έμπλαστρο με βιοαισθητήρα, τον Biosensor Patch1AX. Το έμπλαστρο αυτό, αξιοποιεί την τεχνική καρδιαγγειακής παρακολούθησης και σκοπό έχει να βοηθήσει στην έγκαιρη ανίχνευση του COVID-19 σε ένα άτομο. Τοποθετείται στην περιοχή του θώρακα και μπορεί να καταγράψει τη θερμοκρασία του ατόμου, τον ρυθμό αναπνοής του, το ηλεκτροκαρδιογράφημα και τον καρδιακό ρυθμό του σε πραγματικό χρόνο. Αυτά τα δεδομένα αποστέλλονται αυτόματα, σε μια εφαρμογή στο smartphone του χρήστη, επιτρέποντάς του να βλέπει τα δεδομένα του σε πραγματικό χρόνο.

Σε περίπτωση χρήσης του Biosensor Patch1AX από άτομο το οποίο στην πορεία εμφανίσει συμπτώματα COVID-19, τα δεδομένα του μπορούν επίσης να σταλούν σε μια κεντρική και ασφαλή πλατφόρμα cloud, προειδοποιώντας τους εργαζόμενους στον τομέα της υγείας για έναν πιθανό ασθενή με COVID-19. Τα Biosensors Patch1AX έχουν σχεδιαστεί με τέτοιο τρόπο, ώστε να μπορεί να φορεθεί από ένα άτομο για πέντε ημέρες (με μία κίνηση), μετά την οποία μπορούν να απορριφθούν με ασφάλεια για να διασφαλιστεί ότι η ασθένεια δεν εξαπλώνεται από το έμπλαστρο.

Ωστόσο παρά τα θετικά στοιχεία που απορρέουν από την χρήση των wearable συσκευών, υπάρχουν ορισμένοι περιορισμοί, που εμποδίζουν την χρήση τους την περίοδο αυτή. Η διάρκεια ζωής της μπαταρίας των έξυπνων φορητών συσκευών είναι συνήθως υπό αμφισβήτηση. Η κουραστική εργασία της φόρτισης φορητών συσκευών ξανά και ξανά, συχνά αποτρέπει τους χρήστες να αγοράσουν αυτές τις συσκευές. Επίσης, δεν υπάρχουν οδηγίες σχετικά με τη χρήση των ιδιωτικών δεδομένων που συσσωρεύονται με τη χρήση αυτών των συσκευών, με αποτέλεσμα να δημιουργούνται προβλήματα ασφάλειας και απορρήτου. Είναι απαραίτητο να διασφαλιστεί ότι η ανάπτυξη τέτοιων φορητών συσκευών γίνεται με γνώμονα την προστασία της ιδιωτικής ζωής των χρηστών.

8

Εφαρμογές υγειονομικής περίθαλψης 5G στην πρόληψη και τον έλεγχο του COVID-19

Ένα δίκτυο 5G έχει υψηλή ταχύτητα και αξιοπιστία, χαμηλότερη καθυστέρηση και υψηλή απόδοση. Τα παραπάνω πλεονεκτήματα, καθιστούν τα δίκτυα 5G, ικανά στο να συμβάλουν στην πρόληψη και στον έλεγχο του Covid-19. Από μόνα τους δεν μπορούν να φέρουν την επανάσταση, όμως σε συνδυασμό με άλλες τεχνολογίες όπως το IoT και το AI, το 5G έχει τη δυνατότητα να φέρει επανάσταση στον τομέα της υγειονομικής περίθαλψης και να δημιουργήσει ένα αποτελεσματικό σύστημα για την «παρακολούθηση» του πλήθους, τον εντοπισμό μολυσμένων ατόμων και να παράσχει θεραπεία σε αυτούς, χωρίς την ανάγκη φυσικής ανθρώπινης επαφής (Haiying Ren, et al., 2020).

5G+ Τηλεϊατρική (Telemedicine)

Η χρήση νέων τεχνολογιών έχει βοηθήσει αποτελεσματικά στην πανδημία του COVID-19, η χρήση των drones, των wearables συσκευών, των εφαρμογών για smartphones, μπορούν να βοηθήσουν αποτελεσματικά, ωστόσο για όλες αυτές τις λειτουργίες είναι απαραίτητη η χρήση δικτύου.

Λόγω του περιορισμένου εύρους ζώνης και ταχύτητας μεταφοράς δεδομένων, τα υπάρχοντα δίκτυα 4G δεν μπορούν να υποστηρίξουν τηλεδιάσκεψη υψηλής ποιότητας σε πραγματικό χρόνο. Επιπλέον, τα δίκτυα 4G LTE συχνά εμποδίζουν τη σύνδεση συσκευών IoMT σε πλατφόρμες cloud, καθιστώντας τις αναποτελεσματικές. Για το σκοπό αυτό, το 5G με τις δυνατότητές που προσφέρει, όπως τον εξαιρετικά χαμηλό λανθάνων χρόνο και τη μεταφορά δεδομένων υψηλής

ταχύτητας, μπορεί να επιτρέψει στα δίκτυα κινητής τηλεφωνίας να αντιμετωπίσουν αυτά τα ζητήματα.

Η Κίνα ήδη χρησιμοποιεί ορισμένα από τα χαρακτηριστικά που δίνουν τα δίκτυα 5G στην τηλεϊατρική. Όπως για παράδειγμα το νοσοκομείο West China το οποίο ξεκίνησε μια πλατφόρμα τηλεδιάσκεψης, COVID-19 5G + με τη βοήθεια της China Telecom.

5G+ και Ιατρική Απεικόνιση (Medical Imaging)

Οι ιατρικές τεχνικές απεικονίσεις, όπως η αρχειοθέτηση εικόνων και τα συστήματα επικοινωνίας (Picture Archiving and Communication Systems – PACS), αποτελούν αναπόσπαστο κομμάτι της διάγνωσης και της θεραπείας, Σε συνδυασμό με τα δίκτυα και τις τεχνολογίες κινητής τηλεφωνίας επόμενης γενιάς, όπως AI και Big Data, το PACS μπορεί να προσφέρει βελτιωμένη ανάλυση και διαχείριση δεδομένων, ενώ απαιτεί ελάχιστη ανθρώπινη προσπάθεια.

5G+ και Θερμική Απεικόνιση (Thermal Imaging)

Ένα σύστημα θερμικής απεικόνισης 5G+ IR μπορεί να διακρίνει την θερμοκρασία κινούμενων σωμάτων σε πραγματικό χρόνο, με υψηλή ακρίβεια. Τα δεδομένα που συγκεντρώνονται, μπορούν να διατίθενται στο κεντρικό σύστημα παρακολούθησης με πολύ χαμηλή καθυστέρηση, με τη χρήση 5G δικτύου. Λόγω της πανδημίας, η παρακολούθηση της θερμοκρασίας των πολιτών μπορεί να τεθεί σε εικοσιτετράωρη βάση. Στην Κίνα αρκετά συστήματα θερμικής απεικόνισης 5G+ έχουν ήδη ενοποιηθεί σε ρομπότ και UAV, τα οποία έχουν αναπτυχθεί σε δημόσιους χώρους αρκετών πόλεων για τη μείωση της εξάπλωσης του COVID-19.

5G+ και Ρομπότ

Στην Ταϊλάνδη αναπτύχθηκαν ρομπότ από την Advanced Info Services (AIS), η οποία είναι η μεγαλύτερη εταιρεία τηλεφωνίας της χώρας. Η AIS, εγκατέστησε σε 20 νοσοκομεία δίκτυα 5G και έχει κατασκευάσει αρκετά ρομπότ 5G, για να βοηθήσει τα νοσοκομεία να αυξήσουν τις εγκαταστάσεις τηλεϊατρικής. Τα ρομπότ έχουν την δυνατότητα να εκτελούν θερμικές σαρώσεις και χρησιμοποιούνται ως μέσο στην επικοινωνία γιατρού και ασθενή.

Το ίδιο συμβαίνει και στην Κίνα, όπου σε πολλές πόλεις χρησιμοποιούνται ρομπότ περιπολίας. Τα ρομπότ αυτά συνδυάζουν αρκετές τεχνολογίες, AI, IoT, 5G και cloud computing. Είναι εξοπλισμένα με πέντε θερμόμετρα υπερύθρων και κάμερες υψηλές ανάλυσης, οι οποίες επιτρέπουν την ταυτόχρονη θερμομέτρηση έως και 10 ατόμων. Επίσης, τα ρομπότ αυτά, μπορούν να προσδιορίσουν εάν ένα άτομο φοράει μάσκα και σε περίπτωση που δεν φοράει, ή έχει υψηλή θερμοκρασία, στέλνει αμέσως ειδοποίηση στις τοπικές αρχές. Τα ρομπότ αυτά πλέον

χρησιμοποιούνται σε δημόσιους χώρους πολλών πόλεων όπως στην Κίνα, την Σαγκάη, το Γκουάνγκτζου και τη Γκουιγιάνγκ.

9

Εφαρμογές ιχνηλάτησης επαφών σε κράτη μέλη της ΕΕ

Εφαρμογές Ιχνηλάτησης Επαφών

Οι εφαρμογές ιχνηλάτησης επαφών παρέχουν έξι βασικές λειτουργίες: διαχείριση πληροφοριών για τη διαχείριση κρίσεων, δημοσίευση δημόσιων πληροφοριών για πολίτες, παροχή ψηφιακών υπηρεσιών σε πολίτες, παρακολούθηση πολιτών σε δημόσιους χώρους, διευκόλυνση της ανταλλαγής πληροφοριών μεταξύ πολιτών και ανάπτυξης καινοτόμων απαντήσεων στο COVID-19 (Meijer & Webster, 2020: σελ.267).

Η παρακολούθηση, η συλλογή και η διαχείριση πληροφοριών προέκυψαν, ακριβώς επειδή σύμφωνα με την κατάσταση εξαίρεσης που δηλώθηκε, οι κυβερνήσεις εισέβαλαν στην ιδιωτική σφαίρα με ψηφιακά μέσα. Σε ορισμένα κράτη μέλη κρίθηκε υποχρεωτική η παροχή δεδομένων τοποθεσίας, ως μέσο για τη διασφάλιση της συμμόρφωσης των πολιτών. Σύμφωνα με την Ευρωπαϊκή Επιτροπή, από τα 27 κράτη μέλη στην ΕΕ, υπάρχουν τρείς κατηγορίες ανάλογα με την εθνική στάση, έναντι των εφαρμογών παρακολούθησης. Η ταξινόμηση έγινε τον Ιούνιο του 2020 και η κατηγοριοποίηση φαίνεται στον παρακάτω πίνακα:

Δεν προβλέπεται ανάπτυξη εφαρμογής	Βουλγαρία, Λουξεμβούργο, Σουηδία.
Προετοιμασία για την εκκίνηση εφαρμογής	Ελλάδα, Ρουμανία, Σλοβακία.
Υπάρχει εφαρμογή	Αυστρία, Βέλγιο, Κροατία, Κύπρος, Τσεχία, Δανία, Εσθονία, Φινλανδία, Γαλλία, Γερμανία, Ουγγαρία, Ιρλανδία, Ιταλία, Λετονία, Λιθουανία, Μάλτα, Ολλανδία,

	Νορβηγία, Πολωνία, Πορτογαλία, Σλοβενία, Ισπανία.

Στην Σουηδία υπήρχαν ηθικοί και πολιτικοί λόγοι, για τους οποίους απορρίφθηκε η υιοθέτηση μιας εφαρμογής. Ο πρώτος αφορούσε τη συμμόρφωση με τον GDPR και ο δεύτερος επειδή η κυβέρνηση περίμενε μια εφαρμογή της ΕΕ, και δεν ήθελε να επενδύσει σε ένα εργαλείο που θα ήταν ξεπερασμένο. Στη Βουλγαρία ενώ αρχικά διατέθηκε προς χρήση η εφαρμογή ViruSafe, πλέον δεν συμμετέχει στο πανευρωπαϊκό πρόγραμμα παρακολούθησης εγγύτητας. Τέλος, ούτε το Λουξεμβούργο προβλέπει την ανάπτυξη κάποιας εφαρμογής σχετικά με τον COVID-19.

Από την άλλη, χώρες όπως η Ελλάδα, η Ρουμανία και η Σλοβακία προετοιμάζονται για την εκκίνηση εφαρμογής. Πιο συγκεκριμένα, η Ελλάδα μετά την απόσυρση της εφαρμογής COVTracer, ύστερα από σύντομο χρονικό διάστημα, αποφάσισε να αποκτήσει ξανά νέα εφαρμογή ιχνηλάτησης επαφών.

Εφαρμογές ιχνηλάτησης επαφών σε χώρες εντός ΕΕ

Stopp Corona App - Αυστρία

Η εφαρμογή για κινητές συσκευές Stopp Corona κυκλοφόρησε στις 25 Μαρτίου 2020. Αναπτύχθηκε από την Αυστρία και είναι μια από τις πρώτες ευρωπαϊκές χώρες που έχει αναπτύξει τη δική της εφαρμογή και συμβάλλει στον περιορισμό της εξάπλωσης του ιού. Είναι δωρεάν εφαρμογή και χρησιμοποιεί την τεχνολογία Bluetooth LE για την μέτρηση της απόστασης και της διάρκειας της επαφής των χρηστών που έχουν εγκαταστήσει στα smartphones τους την εφαρμογή.

Η εφαρμογή έχει δύο επίπεδα ειδοποίησης. Μια κίτρινη ειδοποίηση, η οποία δείχνει ότι κάποιος που ήρθε ο χρήστης σε επαφή έχει εμφανίσει συμπτώματα COVID-19. Η κόκκινη ειδοποίηση δείχνει ότι κάποιος με τον οποίο ήρθε ο χρήστης σε στενή επαφή σε απόσταση μικρότερη των δύο μέτρων και για περισσότερο από 15 λεπτά έχει διαγνωστεί ως θετικός. Έχοντας ο χρήστης λάβει μια κίτρινη ειδοποίηση, συνιστάται να σταματήσει την επαφή με άλλα άτομα όπου είναι δυνατόν και να παρακολουθεί την υγεία του. Εάν εμφανιστεί κόκκινη ειδοποίηση, τότε απαιτείται αυτοαπομόνωση. Ωστόσο η εφαρμογή δεν αποφασίζει εάν πρέπει να υποβληθεί ο χρήστης σε δοκιμή, επομένως, συνιστάται να καλέσει την τηλεφωνική γραμμή παροχής συμβουλών για την υγεία (Stopp Corona App, 2020).

Τα δεδομένα κρυπτογραφούνται πριν από την ανταλλαγή, εμποδίζοντας τόσο τους προγραμματιστές εφαρμογών όσο και άλλους χρήστες να έχουν πρόσβαση στα προσωπικά σας στοιχεία. (Stopp Corona App, 2020). Η εφαρμογή Stopp Corona, διαθέτει ψηφιακή χειραψία και

αυτο-παρακολούθηση (Digital Handshake and Self-Monitoring). Οι χρήστες της εφαρμογής μέσω της ψηφιακής χειραψίας της εφαρμογής «χαιρετούν» ο ένας τον άλλον. Οι «χειραψίες» αυτές αποθηκεύονται αυτόματα από την εφαρμογή, έτσι ώστε να μπορεί να στείλει ο χρήστης μια ειδοποίηση εάν ένας χρήστης βρεθεί θετικός.

Σχετικά με την ανάπτυξη της εφαρμογής η Karina Fedorovskaia ανέφερε, «η εφαρμογή, χρησιμοποιώντας DevOps, που περιελάμβανε μια απομακρυσμένη συνεργασία με τον Rotes Kreuz και άλλες ΜΚΟ, αλλά όχι μια διεπιστημονική ομάδα». Χρησιμοποιήθηκε η μεθοδολογία δοκιμών που βασίζεται σε UX. Οι προγραμματιστές χρησιμοποίησαν τις ακόλουθες μεθόδους δοκιμών: γρήγορες δοκιμές πρωτοτύπων (rapid prototyping tests), κλασικές δοκιμές χρηστών (classic user tests) και think aloud tests, προκειμένου να δοκιμάσουν τα wireframes της εφαρμογής (Csilla Herendy, 2020).

Coronalert – Βέλγιο

Η εφαρμογή Coronalert είναι η κύρια εφαρμογή που χρησιμοποιείται στο Βέλγιο. Η εφαρμογή συνδέεται με το εθνικό σύστημα υγειονομικής περίθαλψης και χρησιμοποιεί τεχνολογία Bluetooth και API ειδοποιήσεων έκθεσης Apple / Google. Ωστόσο, δεν συλλέγει προσωπικά στοιχεία ανά πάσα στιγμή, τα δεδομένα του χρήστη είναι ασφαλή και η χρήση της εφαρμογής είναι εθελοντική. Δεν ζητώνται πληροφορίες που αφορούν το όνομα, την ηλικία ή την διεύθυνση του χρήστη και ο χρήστης παραμένει ανώνυμος. Δεν απαιτείται η εγγραφή του χρήστη στην εφαρμογή. Χρησιμοποιείται αποκεντρωμένη αποθήκευση δεδομένων, τα δεδομένα αποθηκεύονται μόνο στο ίδιο smartphone και διαγράφονται μετά από 14 ημέρες. Η εφαρμογή προορίζεται για οποιονδήποτε ζει ή εργάζεται στο Βέλγιο, είναι σε διακοπές στη χώρα ή επισκέπτεται το Βέλγιο τακτικά ή για μεγάλο χρονικό διάστημα (Coronalert - Belgium, 2020).

Όταν είναι ενεργοποιημένη η λειτουργία εγγραφής έκθεσης, τα smartphone ανταλλάσσουν κρυπτογραφημένα τυχαία αναγνωριστικά με άλλες συσκευές που χρησιμοποιούν Bluetooth. Τα τυχαία αναγνωριστικά παρέχουν μόνο πληροφορίες σχετικά με τη διάρκεια και την απόσταση μιας συνάντησης. Κανείς δεν μπορεί να αναγνωρίσει το άτομο πίσω από τα τυχαία αναγνωριστικά (Coronalert, 2020).

Stop COVID-19 – Κροατία

Η Stop COVID-19 είναι η εφαρμογή της Κροατίας, η οποία προειδοποιεί τους χρήστες ότι ενδέχεται να βρεθούν σε επιδημιολογικά επικίνδυνη ζώνη. Η εφαρμογή είναι εθελοντική σε όλα τα στάδια της χρήσης της και η αποθήκευση των δεδομένων είναι προσωρινή. Αξίζει να σημειωθεί ότι χρησιμοποιεί μόνο προσωρινά και ψευδο-ανώνυμα δεδομένα και είναι κυβερνητικά

ασφαλής. Η εφαρμογή βασίζεται στο Google-Apple Exposure Notification (GAEN) και απαιτεί ρητή συγκατάθεση του χρήστη.

Σχετικά με την λειτουργία της εφαρμογής, η εφαρμογή εκχωρεί τυχαία κλειδιά σε όλα τα smartphone που έχουν εγκαταστήσει την εφαρμογή, τα οποία εναλλάσσονται πολλές φορές κάθε ώρα, για να διατηρούν το απόρρητο προστατευμένο. Τα smartphone ανταλλάσσουν αυτά τα κλειδιά μέσω Bluetooth. Με αυτόν τον τρόπο, η εφαρμογή μπορεί να παρακολουθεί τις επαφές που πραγματοποιούνται, χωρίς να προσδιορίζει τον χρήστη ή το άτομο που ήρθε σε επαφή. Η εφαρμογή ελέγχει περιοδικά τα κοινόχρηστα κλειδιά με τον διακομιστή και τα συγκρίνει με τα κλειδιά που είναι αποθηκευμένα στο κινητό, έτσι, η εφαρμογή μπορεί να προσδιορίσει την πιθανή έκθεση του χρήστη. Τέλος, εάν βρεθεί ένα κοινόχρηστο κλειδί, ο χρήστης λαμβάνει ειδοποίηση, ότι ήρθε σε επαφή με ένα άτομο με το οποίο έχει μοιραστεί τα κλειδιά και επομένως ίσως και ο ίδιος να είναι θετικός (Stop COVID-19, 2020).

Στα μέσα Νοεμβρίου, η διασυνοριακή ανταλλαγή δεδομένων μεταξύ της εφαρμογής Κροατίας Stop COVID-19 και επίσημων εφαρμογών από άλλα κράτη μέλη της ΕΕ καθιερώθηκε ως αποτέλεσμα των αποφάσεων και των συστάσεων της Ευρωπαϊκής Επιτροπής. Η διασυνοριακή ανταλλαγή δεδομένων μεταξύ των εθνικών εφαρμογών παρακολούθησης επαφών για κινητά καθορίζεται από την εκτελεστική απόφαση (ΕΕ) 2020/1023 της Επιτροπής της 15ης Ιουλίου 2020 (Stop COVID-19, 2020).

CovTracer-EN – Κύπρος

Το CovTracer-EN είναι η επίσημη εφαρμογή της Κυπριακής Κυβέρνησης η οποία δημιουργήθηκε για την ανίχνευση επαφών, η εφαρμογή είναι εθελοντική, με πλήρη σεβασμό στο απόρρητο των χρηστών, αφού δεν αποθηκεύει τις προσωπικές πληροφορίες των χρηστών. Ακόμα, είναι ανοιχτού κώδικα εφαρμογή και λαμβάνει μόνο τις πληροφορίες που της είναι εντελώς απαραίτητες. Βασίζεται στην τεχνολογία Bluetooth και είναι σε θέση να εντοπίσει πιθανή επαφή του χρήστη με επιβεβαιωμένο κρούσμα COVID-19, μετά από αξιολόγηση ημερομηνίας, χρονικού διαστήματος και εγγύτητας της επαφής του χρήστη. Η εφαρμογή χρησιμοποιεί το πρωτόκολλο Bluetooth και το Google-Apple Exposure Notification (GAEN) για να καταγράψει πότε κάποιος βράθηκε κοντά σε άλλους χρήστες της εφαρμογής. Εάν ένας χρήστης της εφαρμογής βρεθεί θετικός στον ιό, τότε έχει την επιλογή να εισάγει έναν κωδικό στην εφαρμογή ώστε να στείλει αυτή την πληροφορία στις εφαρμογές άλλων χρηστών με τους οποίους είχε έρθει σε επαφή (COVTracer-EN, 2020) (Lempers, Timo, 2021).

eRouška – Τσεχία

Η εφαρμογή eRouška της Τσεχίας αναπτύχθηκε από το Υπουργείο Υγείας σε συνεργασία με το NAKIT (Εθνική Υπηρεσία Πληροφορικής και Επικοινωνιών) και είναι ανοιχτού κώδικα. Χρησιμοποιεί την τεχνολογία Bluetooth LE, η οποία έχει σχεδιαστεί για να είναι ιδιαίτερα ενεργειακά αποδοτική και δεν συλλέγει δεδομένα γεωγραφικής τοποθεσίας, συμπεριλαμβανομένων δεδομένων GPS. Η εφαρμογή δεν αποκαλύπτει το άτομο που είναι θετικό στον ιό, απλώς ενημερώνει ότι υπήρξε επαφή με κάποιο ανώνυμο άτομο. Η εφαρμογή αυτή δεν παρακολουθεί τον χρήστη, συλλέγει τις πληροφορίες τοποθεσίας με μοναδικό σκοπό, να γίνει έλεγχος αν ο χρήστης είχε στενή επαφή με κρούσμα (Raymond Johnston, 2020) (eRouška, 2020).

Η εφαρμογή αναπτύχθηκε και κυκλοφόρησε σε πλήρη συμμόρφωση με τις απαιτήσεις Πολιτικής API ειδοποίησης έκθεσης, είναι πλήρως συμβατή με το GDPR και δεν συλλέγει και επεξεργάζεται άμεσα προσωπικά δεδομένα - τυχόν δεδομένα που θα ταυτοποιούν τον χρήστη ή την κινητή συσκευή του, όπως το όνομα, τη διεύθυνση ή αριθμός τηλεφώνου. Το eRouska είναι σε θέση να προσδιορίσει ότι η επαφή πραγματοποιήθηκε μεταξύ δύο χρηστών χωρίς να γνωρίζει ποιοι είναι αυτοί οι χρήστες και πού συνέβη η επαφή. Τέλος, τα δεδομένα του χρήστη διαγράφονται όταν πλέον δεν είναι απαραίτητα (eRouška, 2020).

Smittestop – Δανία

Η εφαρμογή Smittestop της Δανίας, αναπτύχθηκε στις 13 Μαρτίου του 2020 από την κυβερνητική εταιρεία Simula, είναι μια διαλειτουργική εφαρμογή που μπορεί να επικοινωνήσει με άλλες εφαρμογές, Η λήψη και η χρήση της είναι εθελοντική και όσο περισσότερα άτομα την χρησιμοποιούν, τόσο περισσότερες αλυσίδες μολύνσεων μπορεί να επιβραδύνει. Η εφαρμογή συλλέγει τα δεδομένα της τοπικά, μέσω δεδομένων GPS και Bluetooth και χρησιμοποιεί μια κεντρική, μη ανώνυμη αποθήκευση δεδομένων. Τα δεδομένα μεταφέρονται από το smartphone του χρήστη, στον διακομιστή σε ωριαία βάση. Όλα τα δεδομένα παρακολούθησης αποθηκεύονται κεντρικά στην Ιρλανδία, στην πλατφόρμα Azure που ανήκει στη Microsoft Azure και ελέγχεται από τη νορβηγική κυβέρνηση

Σε περίπτωση που διαπιστωθεί «επαφή» με μολυσμένο άτομο, ο χρήστης θα λάβει μήνυμα κειμένου, που θα εξηγεί τι πρέπει να κάνει, ώστε να μην κολλήσει κάποιον άλλον, καθώς και οδηγίες για την προσωπική του υγεία. Η εφαρμογή δεν θα αναφέρει ποιος ήταν ο ασθενής που μετέφερε τον ιό, αλλά θα δώσει την ημερομηνία κατά την οποία βρέθηκαν σε στενή επαφή. Το κατώτατο όριο για την ενεργοποίηση της λειτουργίας SMS είναι 15 λεπτά εγγύτητας, ορίζεται ως επαφή πιο κοντά από ένα εύρος 2 μέτρων για περισσότερο από 15 λεπτά σε μια περίοδο 24 ωρών. Ενώ για να χρησιμοποιήσει κάποιος την παρούσα εφαρμογή, είναι απαραίτητο να έχει συμπληρώσει το δέκατο έκτο έτος της ηλικίας του. Τα δεδομένα αποθηκεύονται σε cloud για 30

ημέρες, αλλά μπορεί ο χρήστης να διαγράψει και τα δεδομένα του και την εφαρμογή ανά πάσα στιγμή (smitte|stop, 2020).

Οι κανονισμοί δίνουν μια λεπτομερή λίστα με τα δεδομένα που καταχωρούνται στο σύστημα της εφαρμογής, τα δεδομένα αυτά είναι, ο αριθμός κινητού τηλεφώνου, η ηλικία, τα δεδομένα τοποθεσίας και η εγγύτητα/ επαφή με κάποιο μολυσμένο άτομο. Τα προσωπικά δεδομένα από αυτό το σύστημα ενδέχεται να συνδέονται με μια σειρά κυβερνητικών βάσεων δεδομένων. Οι κανονισμοί περιλαμβάνουν επίσης μέτρα σχετικά με τον περιορισμό του σκοπού και την αποστολή και λειτουργία, καθώς και περιορισμούς στην εμπορική χρήση δεδομένων και την κοινοποίησή τους στην αστυνομία ή στο δικαστικό σύστημα (Kristin B Sandvik, 2020).

Η εφαρμογή κυκλοφόρησε σε ελάχιστο χρόνο από την ανάπτυξη της και προκάλεσε σωρεία αρνητικών σχολίων. Υπήρξαν πολλά προβλήματα σχετικά με την φιλικότητα της προς τον χρήστη, την λειτουργικότητα, τις αποτυχίες λήψης και την υψηλή χρήση της μπαταρίας. Ο συνδυασμός GPS / Bluetooth είναι επίσης αμφιλεγόμενος. Όπως γνωρίζουμε από άλλες χώρες, η νορβηγική κυβέρνηση δεν έπρεπε να επιλέξει αυτήν τη λύση. Επίσης, υπάρχουν προβλήματα σχετικά με την αποτελεσματικότητα της εφαρμογής, την δημιουργία ψευδών θετικών αποτελεσμάτων, καθώς και το φαινόμενο της παρεμβατικότητας. Τέλος, έχει εκφραστεί ανησυχία σχετικά με την ασφάλεια που υπάρχει στην αποστολή γραπτών μηνυμάτων, στα άτομα που πιθανώς να νοσήσουν από COVID-19, καθώς υπάρχει σοβαρός κίνδυνος για εξαπάτηση των παραληπτών, για παροχή ευαίσθητων προσωπικών δεδομένων, συμπεριλαμβανομένων και οικονομικών δεδομένων (Kristin B Sandvik, 2020).

HOIA – Εσθονία

Η εφαρμογή HOIA της Εσθονίας, κυκλοφόρησε στις 20 Αυγούστου του 2020 και έχει ληφθεί περισσότερο από 115.000 φορές. Η εφαρμογή βασίζεται στην τεχνολογία BLE, όπου από κοντινά σε απόσταση τηλέφωνα που έχουν εγκατεστημένη την εφαρμογή, θα συλλέγονται και θα αποθηκεύονται ανώνυμοι κωδικοί στο τηλέφωνο που αναφέρεται στο άτομο αυτό. Σε περίπτωση που ένα άτομο με την εγκατεστημένη εφαρμογή HOIA έχει μολυνθεί, μπορεί να ειδοποιήσει την εφαρμογή και επομένως αυτοί που θεωρούνται ότι έχουν στενή επαφή με το άτομο αυτό, θα ειδοποιηθούν αμέσως. Η ταυτότητα του μολυσμένου ατόμου, επομένως, παραμένει ανώνυμη καθ' όλη τη διάρκεια της διαδικασίας (Justin Petrone, 2020).

Η εφαρμογή δημιουργήθηκε χρησιμοποιώντας την αρχή μιας αποκεντρωμένης προσέγγισης, έτσι ώστε να εξασφαλίζεται το επιθυμητό επίπεδο απορρήτου και εν συνεχεία οι εκθέσεις των χρηστών να υπολογίζονται μόνο από τις δικές τους συσκευές. Επίσης, εισήγαγε DP-3T, ως ένα ανοιχτό πρωτόκολλο που επιτρέπει την παρακολούθηση ψηφιακών επαφών μολυσμένων

συμμετεχόντων που χρησιμοποιούν τεχνολογία BLE και χρήση του API ειδοποίησης έκθεσης που παρέχεται από την Google και την Apple.

Koronavilkku – Φινλανδία

Η εφαρμογή Koronavilkku της Φινλανδίας, αναπτύχθηκε από το Εθνικό Ινστιτούτο Υγείας και Πρόνοιας και επιτρέπει στους χρήστες να λαμβάνουν πληροφορίες, για το εάν έχουν εκτεθεί στον ιό, με βάση τις πληροφορίες που λαμβάνει. Η χρήση της εφαρμογής είναι ανώνυμη, εθελοντική και δωρεάν και υπάρχει έντονη προστασία απορρήτου (HannaTiirinki, et al., 2020). Η εφαρμογή βοηθά στο να μάθει ο χρήστης, εάν υπάρχει πιθανότητα να έχει εκτεθεί στον ιό. Εάν ο χρήστης έχει κάνει τεστ κορωνοϊού και βγει θετικός, μπορεί να χρησιμοποιήσει την εφαρμογή, για να κοινοποιήσει αυτές τις πληροφορίες ανώνυμα, ώστε να είναι ενήμερα τα άτομα με τα οποία ήρθε σε επαφή (Helsinki, 2020).

TousAntiCovid - Γαλλία

Η εφαρμογή TousAntiCovid αναπτύχθηκε στην Γαλλία και είναι μια ενημέρωση της εφαρμογής StopCovid, εμπλουτισμένη με πρόσβαση σε υγειονομικές πληροφορίες σχετικά με τον COVID-19. Είναι μια εφαρμογή που χρησιμοποιεί την τεχνολογία BLE για να εντοπίσει ένα κοντινό smartphone και να αποδείξει με ανώνυμο τρόπο τις πιθανές συναντήσεις των ατόμων. Η εφαρμογή εξετάζει επαφές εντός του ενός μέτρου για τουλάχιστον 5 λεπτά, καθώς και για επαφές 2 μέτρων για τουλάχιστον 15 λεπτά. Η περίοδος μετάδοσης ξεκινά από τις 48 ώρες που προηγούνται της ημερομηνίας έναρξης των συμπτωμάτων ή επτά ημέρες πριν από τη θετική εξέταση εάν το άτομο είναι ασυμπτωματικό (Application TousAntiCovid, 2020).

Η χρήση της εφαρμογής βασίζεται σε εθελοντική υπηρεσία και κάθε χρήστης είναι ελεύθερος να την ενεργοποιήσει και να την απενεργοποιήσει ανάλογα με την κατάσταση. Είναι ένα βασικό συμπληρωματικό εργαλείο για την καταπολέμηση του COVID-19. Όσο περισσότερο χρησιμοποιείται η εφαρμογή, τόσο πιο γρήγορα θα ειδοποιηθούν τα περιστατικά επαφής και τόσο πιο συλλογικό θα είναι το αντίκτυπο στον έλεγχο και την εξέλιξη της πανδημίας.

Το έργο συγκεντρώνει την εμπειρογνωμοσύνη των εθνικών δημόσιων και ιδιωτικών φορέων (Inria, ANSSI, Orange και Dassault ειδικότερα) οι οποίοι δεσμεύονται να διατηρήσουν την ασφάλεια και την ιδιωτικότητα των Γάλλων σε όλα τα επίπεδα ανάπτυξης του συστήματος.

Όλα τα AntiCovid αποθηκεύουν μόνο το ιστορικό εγγύτητας ενός κινητού τηλεφώνου. Δεν είναι δυνατόν να γνωρίζουμε την ταυτότητα ενός χρήστη της εφαρμογής, ούτε ποιον συνάντησε, ούτε πού ή πότε. Ο χρήστης μπορεί επίσης να επιλέξει να διαγράψει το ιστορικό του από καιρό σε καιρό αν το επιθυμεί (Application TousAntiCovid, 2020).

Corona-Warn App - Γερμανία

Η εφαρμογή Corona-Warn App αναπτύχθηκε στην Γερμανία στις 16 Ιουνίου 2020 και χρησιμοποιείται για την αποτελεσματική διάσπαση αλυσίδων λοίμωξης. Είναι μια δωρεάν εφαρμογή που χρησιμοποιεί την τεχνολογία BLE για την μέτρηση της απόστασης και της διάρκειας επαφής μεταξύ smartphone που έχουν εγκαταστήσει την εφαρμογή (Bettina Maria Zimmermann, et al., 2021).

Τα άτομα που είναι θετικά και έχουν εγκαταστημένη την εφαρμογή, μπορούν να ενημερώσουν εθελοντικά κι άλλους χρήστες. Οι συσκευές ανταλλάσσουν τυχαία κλειδιά, τα κλειδιά των μολυσμένων ατόμων διατίθενται σε όλους εκείνους που χρησιμοποιούν ενεργά την εφαρμογή. Μόλις εγκατασταθεί, ελέγχει εάν ο χρήστης έχει συναντήσει άτομα θετικά στον ιό. Σε αυτήν την περίπτωση, η εφαρμογή υποδεικνύει μια προειδοποίηση (Open Gonernment Deutshland, 2020). Πληρείται η ελαχιστοποίηση των δεδομένων, οι χρήστες της εφαρμογής παραμένουν ανώνυμοι και δεν χρειάζεται να δώσουν στοιχεία, όπως διεύθυνση email και όνομα κατά την εγγραφή στην εφαρμογή. Η εφαρμογή καταγράφει μόνο συναντήσεις με άλλες εφαρμογές και αναλύει στατιστικά για το εάν εάν υπάρχει πιθανός κίνδυνος μόλυνσης για τον χρήστη. Η εφαρμογή είναι διαλειτουργική και μπορεί να επικοινωνήσει με άλλες εφαρμογές. Έχει αναπτυχθεί με προσιτό τρόπο και υποστηρίζει τις κοινές βελτιώσεις προσβασιμότητας του λειτουργικού συστήματος smartphone. Πρόσθετες εκδόσεις της εφαρμογής κυκλοφόρησαν σταδιακά: σε επιπλέον γλώσσες (π.χ. από τις αρχές Ιουλίου στα τουρκικά) και για ξένα καταστήματα εφαρμογών (π.χ. από τα τέλη Ιουνίου στην Αυστρία), έτσι ώστε η εφαρμογή να έχει μεγαλύτερη αξία, όταν πρόκειται για ταξίδια στην Ευρώπη.

Οι αναφορές στην εφαρμογή προειδοποίησης Corona αναφέρουν επανειλημμένα ότι το πλήρες αποτέλεσμα επιτυγχάνεται μόνο όταν συμμετέχει το 60% τουλάχιστον του πληθυσμού (Corona-Warn-App, 2021). Είναι ανοιχτού κώδικα εφαρμογή, οπότε η τεκμηρίωση και η υποδομή του κώδικα είναι ελεύθερα διαθέσιμη. Η προσέγγιση ανοιχτού κώδικα επιτρέπει στο κοινό και την κοινότητα προγραμματιστών να συμβάλλουν ενεργά στην επιτυχία της λύσης, π.χ. αναφέροντας σφάλματα ή προτείνοντας βελτιώσεις απευθείας στην πλατφόρμα GitHub.

Η εφαρμογή ακολουθεί την αποκεντρωμένη αποθήκευση δεδομένων και διασφαλίζει ότι πληροί τις υψηλές απαιτήσεις προστασίας δεδομένων στη Γερμανία και την Ευρώπη. Τον Απρίλιο του 2020, ξεκίνησε μια επιστημονική συζήτηση με το σύνθημα «κεντρική έναντι αποκεντρωμένης αποθήκευσης». Η απώλεια της εμπιστοσύνης του κοινού θα έθετε σε κίνδυνο όλες τις προσπάθειες να εντοπιστούν νωρίτερα αλυσίδες λοίμωξης με ψηφιακή υποστήριξη και να τις

διακόψουν πιο γρήγορα. Αυτός είναι ο λόγος για τον οποίο η Ομοσπονδιακή Κυβέρνηση επέλεξε τελικά μια αποκεντρωμένη τεχνική προσέγγιση (Open Gonernment Deutshland, 2020).

COVTRACER – Ελλάδα

Το COVTRACER είναι μια εφαρμογή για παρακολούθηση της τοποθεσίας των χρηστών και χρησιμοποιούσε Bluetooth. Ήταν διαθέσιμη προς εγκατάσταση για μικρό χρονικό διάστημα στην Ελλάδα αλλά αποσύρθηκε γρήγορα και συνεχίζεται μέχρι και σήμερα να χρησιμοποιείται από την Κύπρο. Ωστόσο

Η εφαρμογή χρησιμοποιούσε το πρωτόκολλο Bluetooth και το Google-Apple Exposure Notification (GAEN) για να καταγράψει πότε κάποιος ήταν κοντά σε άλλους χρήστες της εφαρμογής. Στην Κύπρο, το COVTRACER δημιουργεί ένα ημερολόγιο με χρονική σήμανση με βάση την τοποθεσία και την κίνηση του χρήστη, το οποίο αποθηκεύεται ιδιωτικά σε κάθε συσκευή. Ο χρήστης μπορεί να ενεργοποιήσει και να απενεργοποιήσει την καταγραφή της εφαρμογής και η τοποθεσία μπορεί να προσδιοριστεί από: GPS, δεδομένα αισθητήρα συσκευής, σημεία πρόσβασης Wi-Fi διεύθυνσης IP, Bluetooth και cell towers (COVTracer, 2020).

Εάν ένας χρήστης της εφαρμογής μολυνθεί, μπορεί να μοιραστεί οικειοθελώς το αρχείο καταγραφής του, με τις αντίστοιχες υγειονομικές αρχές, προκειμένου να εντοπίσουν τα μέρη που έχει επισκεφθεί κάθε μολυσμένος χρήστης και να ενημερώσουν μέσω της εφαρμογής άλλους χρήστες που βρέθηκαν κοντά τους (Lazaridou, 2020).

Η συγκεκριμένη εφαρμογή, δεν ταυτοποιεί δημόσια οποιοδήποτε χρήστη που προσβλήθηκε από τον ιό, δεν διαθέτει τα προσωπικά δεδομένα στο Υπουργείο Υγείας, χωρίς πρώτα να πάρει τη συγκατάθεση του χρήση και δεν χρησιμοποιεί τα δεδομένα για οποιοδήποτε λόγο εκτός από την ανίχνευση επαφών. Όσον αφορά την αποθήκευση δεδομένων, όλα τα προσωπικά δεδομένα αποθηκεύονται αποκλειστικά στη συσκευή κάθε χρήστη με κρυπτογραφημένο τρόπο, ώστε να προστατεύεται ο χρήστης από πιθανές κακόβουλες εισβολές, Ωστόσο ο χρήστης μπορεί οποιαδήποτε στιγμή θέλει, να τα εξάγει ή να τα «προμηθεύσει» σε τρίτους. Όλα τα δεδομένα αποθηκεύονται μόνο στην συσκευή του χρήστη, όπως αναφέρθηκε και παραπάνω και δεν μεταδίδονται σε οποιαδήποτε άλλη συσκευή ή πλατφόρμα και κανένα τρίτο μέρος δεν μπορεί να έχει πρόσβαση ή δικαίωμα επεξεργασίας των προσωπικών δεδομένων του χρήστη, χωρίς πρώτα εκείνος να έχει δώσει την συγκατάθεση του.

Ο χρήστης έχει τα παρακάτω δικαιώματα, της πρόσβασης, έχει τη δυνατότητα να ζητήσει πρόσβαση και λάβει πληροφορίες για προσωπικά δεδομένα που τον αφορούν και τα διατηρούν. Αίτημα για διόρθωση, το οποίο επιτρέπει στον χρήστη να αιτηθεί την συμπλήρωση ή και την διόρθωση των δεδομένων του που διατηρούνται στην εφαρμογή. Τον περιορισμό της

επεξεργασίας, ώστε τα δεδομένα να χρησιμοποιούνται μόνο για συγκεκριμένους σκοπούς, την ένσταση επεξεργασίας προσωπικών δεδομένων, αυτό επιτρέπει στον χρήστη να αντιταχθεί στην επεξεργασία προσωπικών του δεδομένων. Και την φορητότητα των δεδομένων, για να έχει τη δυνατότητα ο χρήστης να αποκτήσει ένα αντίγραφο των προσωπικών δεδομένων σε δομημένη, ευρέως χρησιμοποιούμενη και μηχανικά αναγνώσιμη μορφή ή και τη διαβίβαση των προσωπικών δεδομένων σε άλλο ελεγκτή (COVTracer, 2020).

VirusRadar – Ουγγαρία

Το VirusRadar μπορεί να βοηθήσει στην ανίχνευση επαφών. Μετά τη λήψη, η εφαρμογή μπορεί να εντοπίσει μέσω Bluetooth εάν είχε έρθει σε επαφή με άλλο τηλέφωνο σε ακτίνα δύο μέτρων για περισσότερο από 15 λεπτά. Η εφαρμογή χρησιμοποιεί Bluetooth για να επικοινωνεί με άλλους χρήστες και να ανταλλάσσει κρυπτογραφημένα, ανώνυμα δεδομένα, σχετικά με την απόσταση του χρήστη από τις γύρω συσκευές και να ελέγχει εάν ήρθε σε επικίνδυνη επαφή τις τελευταίες 14 ημέρες. Εάν ένας χρήστης μολυνθεί, μπορεί να κοινοποιήσει τα δεδομένα σε επιδημιολόγους. Οι επιδημιολόγοι μπορούν να ζητήσουν από ένα μολυσμένο άτομο, να κοινοποιήσει τα δεδομένα που συλλέγονται από την εφαρμογή, βοηθώντας τους να εντοπίσουν πιο εύκολα άλλους χρήστες που έχουν έρθει σε επαφή με αυτόν, ειδοποιώντας με αυτόν τον τρόπο άτομα που είχαν στενή επαφή με αυτό το μολυσμένο άτομο (Védd meg magad a koronavírustól, 2020).

Τα δεδομένα του χρήστη είναι απόλυτα ασφαλή, τα μόνα προσωπικά δεδομένα που συλλέγονται για τον χρήστη είναι ο αριθμός τηλεφώνου, ο οποίος είναι αποθηκευμένος στους διακομιστές υψηλής ασφάλειας του Κυβερνητικού Οργανισμού Πληροφορικής και Ανάπτυξης, ο οποίος λειτουργεί ως ραχοκοκαλιά του Υπουργείου Καινοτομίας και Τεχνολογίας και χρησιμοποιείται μόνο για έρευνα επαφών με τη συγκατάθεση του χρήστη. Κάθε χρήστης συμβάλλει προσωπικά σε μια πιο αποτελεσματική άμυνα κατά της εξάπλωσης του ιού (VirusRadar, 2020).

Κατά την εγγραφή στην εφαρμογή, δημιουργείται ένας μοναδικός τυχαίος κωδικός, που στην συνέχει αντιστοιχεί στον αριθμό του κινητού του χρήστη. Οι αριθμοί και οι κωδικοί του κινητού τηλεφώνου των χρηστών αποθηκεύονται σε ασφαλή διακομιστή και δεν εμφανίζονται ποτέ στο κοινό. (Védd meg magad a koronavírustól, 2020).

COVID Tracker – Ιρλανδία

Το Health Service Executive (HSE) COVID Tracker είναι μια δωρεάν εφαρμογή της Ιρλανδίας, η οποία αναπτύχθηκε από το NearForm, σε όλα τα διαδικτυακά καταστήματα εφαρμογών της Apple και της Google. Αναπτύχθηκε και δοκιμάστηκε μέχρι τα τέλη Ιουνίου 2020, όταν έως και το 80% των ενηλίκων ερωτηθέντων, ανέφεραν την ετοιμότητα τους να την χρησιμοποιήσουν (Wiley Online Library, 2020). Η χρήση της είναι εθελοντική και ανοιχτού κώδικα. Εφαρμόζει το GAEN

και χρησιμοποιεί Bluetooth, με ανώνυμα αναγνωριστικά για την καταγραφή οποιουδήποτε άλλου τηλεφώνου που έχει εγκατεστημένη την εφαρμογή στην συσκευή του και βρίσκεται σε στενή επαφή, παρακολουθώντας την απόσταση και τον χρόνο που πέρασε.

Κάθε 2 ώρες, η εφαρμογή πραγματοποιεί λήψη μιας λίστας ανώνυμων αναγνωριστικών που έχουν κοινοποιηθεί στο HSE από άλλους χρήστες που είναι θετικοί στον ιό. Εάν ένας χρήστης βρίσκεται σε απόσταση μεγαλύτερη των 2 μέτρων για περισσότερα από 15 λεπτά με οποιοδήποτε από αυτά τα τηλέφωνα, θα λάβει μια ειδοποίηση ότι είναι στενή επαφή. Η εφαρμογή εκτελείται στο παρασκήνιο. Δεν συλλέγει το όνομα, την ηλικία ή την διεύθυνση του χρήστη, δεν κρατά κάποιον αριθμό τηλεφώνου, εκτός κι αν ο ίδιος ο χρήστης επιλέξει να το κοινοποιήσει, για να λάβει μια κλήση σε περίπτωση που ήρθε σε στενή επαφή με άτομο θετικό στον ιό. Μπορεί να έχει πρόσβαση μόνο σε πληροφορίες που ο χρήστης επιλέγει να μοιράζεται (Privacy and how we use your data, 2020).

Immuni – Ιταλία

Η συγκεκριμένη εφαρμογή ξεκίνησε από την ιταλική κυβέρνηση τον Ιούνιο του 2020 και προειδοποιεί τους χρήστες που έρχονται σε στενή επαφή. Είναι μια ανοιχτού κώδικα εφαρμογή η οποία χρησιμοποιεί την τεχνολογία BLE, εξασφαλίζοντας χαμηλή κατανάλωση ενέργειας. Όταν δύο χρήστες έρχονται σε στενή επαφή ανταλλάσσουν αυτόματα κωδικούς. Ο κωδικός εισάγεται στο κεντρικό σύστημα από τις υγειονομικές αρχές, με τη συγκατάθεση των ασθενών. Το σύστημα αυτό χρησιμοποιείται για να ειδοποιεί όλους τους άλλους χρήστες που έχουν έρθει σε στενή επαφή (χρησιμοποιώντας τον κωδικό) (Turki Alanzi, 2021) (Immuni, 2020).

Η εφαρμογή δεν συλλέγει προσωπικά στοιχεία, όπως, όνομα, ημερομηνία γέννησης, διεύθυνση κατοικίας, αριθμό τηλεφώνου και διεύθυνση email. Όπως επίσης, δεν παρακολουθεί τις κινήσεις των χρηστών και μοιράζεται μόνο τους κωδικούς για την ανίχνευση επαφών. Τα δεδομένα διαγράφονται όταν δεν είναι πλέον απαραίτητα (Turki Alanzi, 2021).

Apturi Covid – Λετονία

Η επίσημη εφαρμογή παρακολούθησης επαφών για την Λετονία είναι το Apturi Covid, που παρέχεται από το SPKC, το τοπικό Κέντρο Πρόληψης και Ελέγχου Νόσων. Όσοι περισσότεροι χρήστες χρησιμοποιούν την εφαρμογή, τόσο πιο αποτελεσματική θα είναι, για την διακοπή της εξάπλωσης του ιού. Η εφαρμογή δεν λειτουργεί μόνο στη Λετονία, αλλά και σε άλλες ευρωπαϊκές χώρες, αφού είναι διαλειτουργική.

Η εφαρμογή χρησιμοποιεί τεχνολογία Bluetooth και API ειδοποιήσεων έκθεσης της Google για να διασφαλίσει το απόρρητο και την ασφάλεια. Η συγκεκριμένη εφαρμογή σέβεται το απόρρητο

του χρήστη και δεν παρακολουθεί την τοποθεσία του. Αποθηκεύει τα δεδομένα μόνο στη συσκευή και τα διαγράφει αυτόματα μετά από 14 ημέρες (Apturi Covid Latvia - SPKC, 2020).

Korona Stop – Λιθουανία

Το Korona Stop είναι η επίσημη εφαρμογή ειδοποιήσεων έκθεσης για τη Λιθουανία που δημιουργήθηκε από την αρχή του Υπουργείου Υγείας της Δημοκρατίας της Λιθουανίας. Η χρήση της εφαρμογής είναι εθελοντική και προειδοποιεί τους χρήστες ότι μέσα σε διάστημα 14 ημερών ήρθαν σε κοντινή επαφή μεγαλύτερη των 15 λεπτών, με κάποιον άλλο χρήστη της εφαρμογής, ο οποίος έχει ειδοποιήσει για τη μόλυνσή. Για να χρησιμοποιήσει την εφαρμογή ο χρήστης πρέπει να δώσει τη συγκατάθεσή του για χρήση Bluetooth, ώστε να εντοπιστούν κοντινές συσκευές. Η εφαρμογή δημιουργεί προσωρινούς κωδικούς για ανταλλαγή με άλλες συσκευές. Η ταυτότητα, η τοποθεσία και ο ακριβής χρόνος έκθεσης δεν πρέπει σε καμία περίπτωση να αποκαλυφθεί. Οι χρήστες μπορούν να απεγκαταστήσουν την εφαρμογή από τη συσκευή τους ανά πάσα στιγμή (Korona Stop LT, 2020).

COVIDAlert – Μάλτα

Το COVIDAlert είναι μια ανοιχτού κώδικα εφαρμογή, η οποία στοχεύει στο περιορισμό της εξάπλωσης του ιού. Η χρήση της εφαρμογής είναι εθελοντική και χρησιμοποιεί Bluetooth Low Energy για την μετάδοση των αναγνωριστικών. Η αποθήκευση πληροφοριών στο κινητό τηλέφωνο ενός χρήστη θα πραγματοποιηθεί με τη συγκατάθεση του χρήστη. Οι χρήστες μπορούν να αποσύρουν τη συγκατάθεσή τους για χρήση του συστήματος ανά πάσα στιγμή διαγράφοντας την εφαρμογή ή απλώς σταματώντας να τη χρησιμοποιούν, οπότε δεν θα δημιουργηθούν περισσότερα δεδομένα. Τα δεδομένα χρησιμοποιούνται αποκλειστικά για τον επιδιωκόμενο σκοπό και δεν χρησιμοποιούνται για κανέναν άλλο λόγο. Η επεξεργασία προσωπικών δεδομένων περιορίζεται στο ελάχιστο και έχει σχεδιαστεί για να διατηρεί το απόρρητο μέσω ανωνυμοποίησης και ψευδωνυμοποίησης. Τα δεδομένα δεν μπορούν να εντοπιστούν με τεχνικά μέσα σε άτομα, τοποθεσίες ή συσκευές. Αυτό που συλλέγεται δεν είναι δεδομένα τοποθεσίας, αλλά απλώς κρυπτογραφημένα δεδομένα που αφορούν συμβάντα εγγύτητας (Privacy Policy – COVID Alert Malta, 2020).

CoronaMelder – Ολλανδία

Το CoronaMelder είναι μια εφαρμογή που δημιουργήθηκε από το Υπουργείο Υγείας. Χρησιμοποιεί το πλαίσιο ειδοποιήσεων έκθεσης της Google και της Apple (GAEN). Πρόκειται για ένα αποκεντρωμένο πλαίσιο που επιτρέπει στα σύγχρονα smartphone να συλλέγουν ανώνυμα και να καταγράφουν συναντήσεις με άλλα smartphone σε κοντινή απόσταση. Όταν είναι

ενεργοποιημένη η εφαρμογή ειδοποιήσεων παρακολουθεί τις συναντήσεις για 14 ημέρες (Jan-Willem van't Klooste, et al., 2021).

Smittestopp – Νορβηγία

Το Smittestopp είναι μια εφαρμογή από το Νορβηγικό Ινστιτούτο Δημόσιας Υγείας. Η εφαρμογή βασίζεται σε τεχνολογία από την Apple και την Google. Η προστασία της ιδιωτικής ζωής ήταν ένας πολύ σημαντικός παράγοντας κατά την ανάπτυξη της εφαρμογής. Η χρήση της είναι εθελοντική, αλλά δεν είναι ανοιχτού κώδικα εφαρμογή. Χρησιμοποιεί κυρίως την τεχνολογία Bluetooth, για τον προσδιορισμό της, ενώ χρησιμοποιεί και GPS, το οποίο επιτρέπει τον προσδιορισμό της θέσης και την ακριβέστερη αναγνώριση της διάρκειας επαφής (Umaer Naseer, et al., 2020). Κανένας άλλος χρήστης της εφαρμογής ή οι δημόσιες αρχές δεν έχουν πρόσβαση σε πληροφορίες σχετικά με το ποιος είναι ο χρήστης. Ο χρήστης μπορεί να επιλέξει να διαγράψει τα δεδομένα του, να απενεργοποιήσει την εφαρμογή ή να την απεγκατεστήσει από την συσκευή του. Το Smittestopp δεν συλλέγει προσωπικά δεδομένα του χρήστη, ούτε διαθέτει σχετική υπηρεσία πρόσβασης (The Smittestopp app, 2020).

ProteGO Safe – Πολωνία

Το ProteGO Safe είναι μια εφαρμογή της Πολωνίας, η οποία παρακολουθεί το περιβάλλον του χρήστη μέσω αναζήτησης άλλων συσκευών που έχουν εγκατεστημένη την εφαρμογή. Οι περιπτώσεις που αποτελούν κίνδυνο είναι οι συναντήσεις που διήρκησαν περισσότερο από 15 λεπτά και σε απόσταση μικρότερη των 2 μέτρων (STOP COVID ProteGO Safe, 2020). Η εφαρμογή προορίζεται για εθελοντική χρήση και δεν έχει πρόσβαση στην ταυτότητα του. Επίσης, είναι ανοιχτού κώδικα και τα δεδομένα διαγράφονται όταν πλέον δεν είναι απαραίτητα για χρήση (που δεν αφορούν την διασπορά του ιού). Η εφαρμογή χρησιμοποιεί την τεχνολογία Bluetooth για την ανταλλαγή κλειδιών μεταξύ smartphones που ήταν κοντά μεταξύ τους (Tanvir Rahman, et al., 2021).

StayAway COVID – Πορτογαλία

Η εφαρμογή προορίζεται για εθελοντική χρήση και δεν έχει πρόσβαση στην ταυτότητά ή στα προσωπικά δεδομένα του χρήστη. Η εφαρμογή STAYAWAY COVID υιοθετεί το πρωτόκολλο DP3T (το οποίο διαφέρει εννοιολογικά και αρχιτεκτονικά από τα συστήματα που υιοθετούνται εκτός Ευρώπης), προκειμένου να διασφαλιστεί το μέγιστο απόρρητο των χρηστών και να διασφαλιστεί ο έλεγχός τους στα προσωπικά τους στοιχεία. Η υιοθέτηση αυτού του πρωτοκόλλου από διάφορες ευρωπαϊκές χώρες όπως η Γερμανία, η Ελβετία, η Ιταλία, η Ιρλανδία και η Δανία, δείχνει ότι δεν υπάρχουν ενδείξεις σημαντικών κινδύνων μέχρι αυτή τη στιγμή (STAYAWAY COVID app, 2020).

Επιπλέον, η λειτουργία του συστήματος STAYAWAY COVID ακολουθεί τις ορθές πρακτικές που έχουν υιοθετηθεί από τους εταίρους της πρωτοβουλίας DP3T και παρακολουθεί στενά την εξέλιξη των λύσεων που εφαρμόζονται σε άλλες χώρες, με τη διαχείριση πιθανών θεμάτων ασφάλειας και απορρήτου, σύμφωνα με το τι είναι γίνεται διεθνώς (STAYAWAY COVID, 2020).

Η εφαρμογή χρησιμοποιεί GAEN και λειτουργεί με την υπηρεσία BLE. Το STAYAWAY COVID στοχεύει να συνεργαστεί με τον μεγαλύτερο αριθμό πρωτοβουλιών ψηφιακού εντοπισμού COVID-19, τόσο εντός όσο και εκτός Ευρώπης. Θα πρέπει να είναι δυνατή η διασταύρωση των δεδομένων που συλλέγονται από την εφαρμογή με εκείνα που παρέχονται στο διαδίκτυο από οποιαδήποτε από αυτές τις χώρες (STAYAWAY COVID, 2020).

Τα μόνα δεδομένα που διαχειρίζεται το σύστημα είναι τα τυχαία αναγνωριστικά που δημιουργούνται από τα κινητά τηλέφωνα. Αυτά τα δεδομένα αποθηκεύονται σε κινητά τηλέφωνα, για μέγιστο χρονικό διάστημα 14 ημερών. Τα δεδομένα που μεταδίδονται και λαμβάνονται από κινητά τηλέφωνα, καθώς και τα δεδομένα που ενδέχεται να κοινοποιούνται στο διαδίκτυο, είναι τυχαίοι αριθμοί που δημιουργούνται από την εφαρμογή STAYAWAY COVID,

#OStaniZdrav – Σλοβενία

Η εφαρμογή #OstaniZdrav (#StayHealthy), είναι μια εφαρμογή για κινητά για την προστασία της δημόσιας υγείας και η χρήση της είναι εντελώς εθελοντική. Μέσω της εφαρμογής, οι χρήστες προειδοποιούνται με ασφαλή και ανώνυμο τρόπο ότι έχουν εκτεθεί σε επικίνδυνη επαφή. Η εφαρμογή ειδοποιεί τον χρήστη ότι ο κίνδυνος μόλυνσης έχει αυξηθεί και τους ενθαρρύνει να συμπεριφέρονται ακόμη πιο υπεύθυνα (The #OstaniZdrav mobile application, 2020).

Είναι απαραίτητη η ενεργοποίηση του Bluetooth, ώστε το smartphone να καταγράφει τυχαία αναγνωριστικά από άλλα smartphone και να τα αποθηκεύει στο αρχείο καταγραφής έκθεσης της συσκευής. Η εφαρμογή εκτελείται στο παρασκήνιο, προκειμένου να εκτιμάται αυτόματα ο κίνδυνος. Εάν ο χρήστης αρνηθεί να εκτελείται η εφαρμογή στο παρασκήνιο, η εφαρμογή δεν θα λειτουργεί σωστά. Δεν συλλέγονται δεδομένα τοποθεσίας σε αυτήν τη διαδικασία. Όλα τα δεδομένα που είναι αποθηκευμένα στην εφαρμογή διαγράφονται όταν δεν είναι πλέον χρήσιμα για τις λειτουργίες της εφαρμογής (Privacy notice • #OstaniZdrav App, 2020).

Η λειτουργικότητα παρέχεται από την Apple ή την Google. Σε αυτήν την περίπτωση, η διαγραφή εξαρτάται από το τι Apple ή η Google έχει καθορίσει. Επί του παρόντος, τα δεδομένα διαγράφονται αυτόματα μετά από 14 ημέρες. Όμως είναι δυνατόν, λόγω της λειτουργικότητας που παρέχεται από την Apple και την Google, ο χρήστης να διαγράψει τα δεδομένα του με μη αυτόματο τρόπο, από τις ρυθμίσεις συστήματος της συσκευής.

Τα δεδομένα που δημιουργούνται κατά τη χρήση της εφαρμογής υποβάλλονται σε επεξεργασία αποκλειστικά σε διακομιστές στη Δημοκρατία της Σλοβενίας. Το σύστημα back-end της εφαρμογής #OstaniZdrav για κινητές συσκευές συνδέεται με τον Ευρωπαϊκό Κεντρικό Διακομιστή (που διαχειρίζεται η Ευρωπαϊκή Επιτροπή) από όπου θα λάβει προσωρινά κλειδιά έκθεσης χρηστών εφαρμογών σε άλλες χώρες της ΕΕ και θα στείλει προσωρινά κλειδιά έκθεσης σλοβενικών χρηστών στον κεντρικό διακομιστή. Σήμερα, η Αυστρία, το Βέλγιο, η Κροατία, η Δανία, η Φινλανδία, η Γερμανία, η Ιρλανδία, η Ιταλία, η Λετονία, οι Κάτω Χώρες, η Πολωνία και η Ισπανία περιλαμβάνονται στη διασυνοριακή ανταλλαγή (The #OstaniZdrav mobile application, 2020) (Privacy notice • #OstaniZdrav App, 2020).

Radar Covid – Ισπανία

Το Radar Covid είναι μια εφαρμογή για smartphones που αναπτύχθηκε, για να παρακολουθήσει την εξάπλωση του ιού και βοηθήσει στον εντοπισμό πιθανών στενών επαφών, μέσω της τεχνολογίας Bluetooth. Η περίοδος κατά την οποία αναζητούνται στενές επαφές όταν εντοπιστεί επιβεβαιωμένο κρούσμα είναι από 2 ημέρες πριν από την έναρξη των συμπτωμάτων του ατόμου.

Τα δεδομένα που αποθηκεύονται στο smartphone του χρήστη είναι κρυπτογραφημένα. Η εφαρμογή δεν συλλέγει δεδομένα που επιτρέπουν τον εντοπισμό της ταυτότητας του χρήστη, όπως ονοματεπώνυμο, διεύθυνση, αριθμό τηλεφώνου ή διεύθυνση email. Η εφαρμογή δεν συλλέγει δεδομένα γεωγραφικής τοποθεσίας, συμπεριλαμβανομένου του GPS και δεν παρακολουθεί τις κινήσεις του χρήστη (Protégete y protege a los tuyos, 2020).

10

Η χρήση των εφαρμογών ιχνηλάτησης και η αντιμετώπιση τους από τους ανθρώπους

10.1 Παράγοντες που επηρεάζουν την κοινωνική αποδοχή των εφαρμογών ιχνηλάτησης επαφών

Υπάρχουν αρκετοί παράγοντες που μπορούν να επηρεάσουν την κοινωνική αποδοχή της παρακολούθησης. Αρχικά, έχουμε τον παράγοντα των ψηφιακών ανισοτήτων που υπάρχουν στην κοινωνία, αφού η χρήση της τεχνολογίας διαφέρει μεταξύ ατόμων, ανάλογα με την ηλικία τους, τα κοινωνικοοικονομικά τους χαρακτηριστικά, τον τύπο συσκευής που διαθέτουν, καθώς και άλλους σχετικούς παράγοντες. Τα χαμηλά επίπεδα «ψηφιακής παιδείας» είναι πιθανόν να αυξήσουν τις θεωρίες συνωμοσίας και να δημιουργήσουν ψεύτικες ειδήσεις, με αποτέλεσμα να αυξηθεί η αντίσταση στην υιοθέτηση τεχνολογιών παρακολούθησης μεταξύ των ευάλωτων ομάδων του πληθυσμού. Επομένως, η χρήση της παρακολούθησης πρέπει να ενσωματωθεί στο κοινωνικό-τεχνικό πλαίσιο στο οποίο επιθυμεί να τεθεί σε εφαρμογή, πράγμα που σημαίνει ότι μια εφαρμογή παρακολούθησης δεν θα ήταν λειτουργική σε μια περιοχή ή χώρα όπου τα άτομα δεν διαθέτουν smartphone. Το συμπέρασμα το οποίο προκύπτει, είναι ότι τα άτομα που κινδυνεύουν από επιπλοκές μετά από μόλυνση με τον ιό, είναι αυτά, που είτε δεν έχουν πρόσβαση σε smartphone είτε δεν έχουν την δυνατότητα λόγω έλλειψης γνώσεων να εγκαταστήσουν την εφαρμογή στις έξυπνες συσκευές τους, το γεγονός αυτό έχει ως αποτέλεσμα να υπάρχει πιθανότητα να αυξηθεί η πίεση στα ιατρικά συστήματα, επειδή θα χρειάζονται ιατρικές

υπηρεσίες. Για τον λόγο αυτό, τα άτομα που κινδυνεύουν περισσότερο, θα πρέπει να κάνουν καλύτερη χρήση αυτών των εφαρμογών για να αποφύγουν αποτελεσματικά τη μόλυνση.

Επίσης, σχετίζεται με την προσκόλληση του πληθυσμού στην έννοια της «τεχνολογικής παρακολούθησης». Όπως αναφέρθηκε και σε προηγούμενη ενότητα, οι εφαρμογές παρακολούθησης διακρίνονται στις εθελοντικές και στις μη εθελοντικές. Και οι άνθρωποι χωρίζονται σε δύο κατηγορίες, σε αυτούς που είναι έτοιμοι να χρησιμοποιήσουν μια εφαρμογή ιχνηλάτησης επαφών και να δεχτούν την παρακολούθηση και σε αυτούς που είναι εντελώς απρόθυμοι. Η προσφορά κάποιου βαθμού επιλογής, τουλάχιστον στα πρώτα στάδια της περιόδου παρακολούθησης, θα μπορούσε να είναι ένας σημαντικός παράγοντας για την αύξηση της συνολικής αποδοχής.

10.2Κίνδυνοι και Προκλήσεις

Παρά τις σημαντικές προσπάθειες που καταβάλλονται από τις κυβερνήσεις, για την χρήση των εφαρμογών ιχνηλάτησης επαφών, με σκοπό την μείωση των κρουσμάτων. Οι εφαρμογές αποτυγχάνουν σε παγκόσμιο επίπεδο, αφού ο βαθμός εμπιστοσύνης των ατόμων σε αυτά τα εργαλεία, είναι πολύ μικρός, πιστεύοντας ότι οι εφαρμογές θέτουν σε κίνδυνο τις ατομικές τους ελευθερίες.

Η πιθανή αποκάλυψη προσωπικών πληροφοριών των ατόμων, ενδέχεται να αυξήσει τον στιγματισμό. Ο πληθυσμός με χαμηλότερα επίπεδα ψηφιακών δεξιοτήτων, κινδυνεύει περισσότερο από παραβιάσεις εμπιστευτικότητας, ενισχύοντας τον επιβλαβή αντίκτυπο των ψηφιακών ανισοτήτων κατά τη διάρκεια της κρίσης (Beaunoyer & Guitton, 2017). Τα ψηφιακά μέσα κοινωνικής δικτύωσης είναι τέλειοι φορείς για τη διάδοση ψεύτικων ειδήσεων και θεωριών συνωμοσίας και η παρακολούθηση μέσω της τεχνολογίας προσφέρει έναν τέλειο στόχο. Χωρίς να εμπίπτει στην παράνοια, είναι προφανές ότι ορισμένες κυβερνήσεις θα μπορούσαν εύκολα να παρακολουθήσουν τον πληθυσμό για να απομακρύνουν τους πολίτες από ορισμένα από τα δικαιώματά τους.

Σε μετά-πανδημικό πλαίσιο, ο προσδιορισμός των ατόμων ανάλογα με τις συμπεριφορές, τις αντιδράσεις ή την κατάσταση της υγείας τους πριν, κατά τη διάρκεια ή μετά την κρίση μπορεί να έχει μεγάλο ενδιαφέρον για διάφορες εταιρείες, συμπεριλαμβανομένων ενδεικτικά των ασφαλιστικών εταιρειών, ή των κυβερνητικών που δεν σχετίζονται άμεσα με την υγειονομική περίθαλψη, όπως υπηρεσίες επιβολής του νόμου ή μετανάστευσης. Παρόλο που υπάρχουν νόμοι για την προστασία του απορρήτου των πληροφοριών που σχετίζονται με την υγεία, οι εταιρείες

μπορούν ακόμα να βγάλουν συμπεράσματα από δεδομένα που δεν προστατεύονται από νόμους, όπως αγορά μέσω διαδικτύου, δημοσιεύσεις κοινωνικών μέσων ή ιστορικό πλοήγησης.

Τέλος, η παρακολούθηση φέρει μακροπρόθεσμους κινδύνους στιγματισμού ορισμένων τμημάτων του πληθυσμού. Αρκετοί παράγοντες μπορεί να συμβάλουν σε αυτό, συμπεριλαμβανομένων του κατά λάθος περιορισμού των ατόμων (με κίνδυνο στιγματισμού, ειδικά για ευάλωτους αστικούς πληθυσμούς ή αγροτικούς πληθυσμούς όπου η συχνότητα εμφάνισης μολύνσεων είναι πιθανώς χαμηλότερη) και ζητήματα που σχετίζονται με την επακόλουθη χρήση των δεδομένων. Η μειωμένη πρόσβαση σε ιατρική περίθαλψη και η εισβολή στην ιδιωτική ζωή, για όσους δεν γνωρίζουν πώς να προστατεύσουν τα δεδομένα τους, οδήγησαν σε μείωση της σχέσεως εμπιστοσύνης μεταξύ κυβερνήσεων και πολιτών.

11

Συμπεράσματα

Για την καταπολέμηση της πανδημίας του COVID-19, αναπτύχθηκαν αρκετοί μηχανισμοί ανίχνευσης για τον περιορισμό της εξάπλωσης της νόσου. Σημαντικό ρόλο στον περιορισμό της εξάπλωσης της πανδημίας έχουν οι εφαρμογές ιχνηλάτησης επαφών, οι οποίες συλλέγουν διάφορα δεδομένα, ανάλογα με την τεχνολογία που χρησιμοποιούν. Οι εφαρμογές ιχνηλάτησης επαφών χρησιμοποιούν κυρίως τεχνολογίες όπως Bluetooth και GPS, ωστόσο γίνεται σταδιακή υιοθέτηση κι άλλων τεχνολογιών όπως, Blockchain, QR Code, IPS και CSLI. Στην παρούσα διπλωματική εργασία, έγινε ανάλυση τεχνολογιών, πρωτοκόλλων και εφαρμογών που υπάρχουν σε ολόκληρο τον κόσμο.

Η επιτυχία οποιασδήποτε εφαρμογής παρακολούθησης ψηφιακών επαφών, εξαρτάται σε μεγάλο βαθμό από την εμπιστοσύνη και την αξιοπιστία και από αυτό, επηρεάζεται το ποσοστό εγκατάστασης της κάθε εφαρμογής, από τους χρήστες. Δεν πρέπει να ξεχνάμε το γεγονός ότι, υπάρχουν αρκετοί πολίτες οι οποίοι δεν έχουν μεγάλη σχέση με την τεχνολογία, με αποτέλεσμα λόγω άγνοιας, να πέσουν στην παγίδα και να μοιραστούν, χωρίς να το γνωρίζουν προσωπικές τους πληροφορίες. Οι χρήστες όπως διαπιστώθηκε, διστάζουν να μοιράζονται και να μεταδίδουν προσωπικά τους στοιχεία και λεπτομέρειες εγγύτητας, καθώς δεν είναι σίγουροι για το πως, από ποιον και για πόσο, θα χρησιμοποιούνται οι πληροφορίες αυτές.

Είναι αναγκαίο να αναφέρουμε ότι υπάρχουν κεντρικές και αποκεντρωμένες προσεγγίσεις. Στην περίπτωση της αποκεντρωμένης οι λεπτομέρειες αποθηκεύονται μόνο στη συσκευή του χρήστη, η οποία δίνει στους χρήστες τη δύναμη και τον έλεγχο πάνω από τα δικά τους δεδομένα, ενώ στην

κεντρική, η ανάλυση και η επεξεργασία γίνονται στον κεντρικό διακομιστή και στην συνέχεια οι χρήστες ειδοποιούνται, εάν αυτό απαιτείται.

Το Bluetooth είναι η πιο ευρέως χρησιμοποιούμενη ασύρματη τεχνολογία σε εφαρμογές ιχνηλάτησης επαφών, το εύρος εγγύτητας δεν είναι αρκετά υψηλό, ωστόσο, είναι καλύτερο σε σχέση με την αμέσως επόμενη σε σειρά χρησιμοποίησης τεχνολογία που είναι το GPS (Global Positioning System). Το GPS δεν είναι τόσο ασφαλές και αποτελεσματικό, καθώς είναι αρκετά εύκολο να υπάρξουν κακόβουλοι εισβολείς και να δημιουργήσουν ψευδείς πληροφορίες στο δίκτυο GPS. Επίσης, τα δεδομένα γεωγραφικής θέσης ενδέχεται να μην λειτουργούν ή να μην υπάρχει ακρίβεια σε ορισμένους περιορισμένους χώρους, επειδή χρησιμοποιεί το δίκτυο κινητής τηλεφωνίας και η ακρίβεια εξαρτάται από την ισχύ του σήματος μεταξύ του κινητού τηλεφώνου και του πύργου κυψελών (cell tower).

Οι περισσότερες εφαρμογές ιχνηλάτησης επαφών, ιδίως σε χώρες που ανήκουν στην ΕΕ, χρησιμοποιούν την τεχνολογία BLE. Είναι μια τεχνολογία, την οποία μπορούν να υποστηρίξουν όλα τα smartphone που διαθέτουν Bluetooth στην συσκευή τους και καταναλώνουν λιγότερη ισχύ σε σχέση με άλλες τεχνολογίες. Επίσης, παρέχουν πιο ακριβείς μετρήσεις και οι προσεγγίσεις που βασίζονται σε αυτήν τη τεχνολογία δεν αποθηκεύουν την τοποθεσία ή δεδομένα χρηστών, ειδοποιούν μόνο τα άλλα πιθανά άτομα, χωρίς μεγάλη παρέμβαση στο το απόρρητο του χρήστη.

Άλλη μια τεχνολογία που αναλύθηκε είναι το CLSI, ωστόσο δεν είναι αρκετά ακριβής και παρέχει «φτωχότερα» αποτελέσματα σε σύγκριση με άλλες προσεγγίσεις όπως το GPS ή το Bluetooth. Σχετικά με το QR Code, η προσέγγιση αυτή περιορίζει την κυκλοφορία του πληθυσμού, καθώς οι κυβερνητικές αρχές υποχρεώνουν τη σάρωση του κωδικούς σε κάθε είσοδο καταστήματος, μετρό και άλλα δημόσια κτίρια.

Η καλύτερη τεχνολογία προς επιλογή, με τα μέχρι στιγμής στοιχεία είναι το blockchain, καθώς παρέχει στους χρήστες τον πλήρη έλεγχο των δεδομένων τους, καθ' όλη τη διάρκεια που τα δεδομένα υπάρχουν στο σύστημα και τους επιτρέπει να τα ανακαλούν, όποια στιγμή αυτοί θελήσουν. Επιπλέον, τα αποθηκευμένα δεδομένα είναι κρυπτογραφημένα (χρόνος με σφραγισμένο και αμετάβλητο τρόπο), που καθιστά αδύνατη την πρόσβαση σε οποιοδήποτε μη εξουσιοδοτημένο άτομο, προάγει τη διαφάνεια και εξαλείφει κάθε πιθανότητα ασυμφωνίας.

Ωστόσο, μέχρι και σήμερα, η εφαρμογή που βασίζεται σε τεχνολογία blockchain δεν είναι ακόμα αρκετά γνωστή και υπάρχει εκτεταμένη έλλειψη ενημέρωσης σχετικά με την χρήση του και τις δυνατότητες που προσφέρει. Επίσης, δεν διατίθενται πολλές εφαρμογές που να χρησιμοποιούν την συγκεκριμένη τεχνολογία. Συμπερασματικά, η τεχνολογία, η οποία είναι διαθέσιμη, γνωστή

και πρακτικά «καλύτερη» (αφού οι εφαρμογές που βασίζονται στο Blockchain είναι ελάχιστες), όπως διαπιστώνεται με βάση την παραπάνω ανάλυση είναι το Bluetooth.

Στην συνέχεια, έγινε ανάλυση 22 εφαρμογών παρακολούθησης επαφών που υπάρχουν μέχρι στιγμής στην ΕΕ και έχουν αναπτυχθεί για την καταπολέμηση της πανδημίας του COVID-19, επισημαίνοντας κυρίως τα δικαιώματα πρόσβασης ανά εφαρμογή. Επίσης, αναλύθηκαν κάποιες εφαρμογές οι οποίες χρησιμοποιούν είτε την τεχνολογία Bluetooth, είτε το GPS σε χώρες εκτός ΕΕ, στις οποίες η χρήση και η εγκατάσταση είναι υποχρεωτική και δεν υπάρχει περιορισμός ως προς τον τρόπο χρήσης των δεδομένων, όπως συμβαίνει στις εφαρμογές του Κατάρ και της Ταϊλάνδης.

Επίσης, έγινε εκτενής ανάλυση αναδυόμενων τεχνολογιών, όπως IoT, UAV, AI, και 5G, για τον μετριασμό των επιπτώσεων της πανδημίας COVID-19. Μέχρι να εμφανιστεί μια θεραπεία για αυτήν την ασθένεια, η ευθύνη για τη διαχείριση και τον περιορισμό των επιπτώσεών της, ανήκει σε μεγάλο βαθμό σε αυτές τις τεχνολογίες. Σε κάθε περίπτωση επιλογής κάποιας τεχνολογίας, είναι αναγκαίο να θυμόμαστε ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι αναγκαία για την διαχείριση της πανδημίας.

Η προστασία των δεδομένων είναι απολύτως απαραίτητη για την οικοδόμηση εμπιστοσύνης και τη δημιουργία των προϋποθέσεων για την κοινωνική αποδοχή οποιασδήποτε λύσης. Τα δεδομένα του κάθε χρήστη, είναι απαραίτητο να χρησιμοποιούνται για να προσφέρουν νέες δυνατότητες, όπως είναι ο περιορισμός της εξάπλωσης του ιού, και όχι για τον έλεγχο και τον στιγματισμό των ατόμων. Είναι απαραίτητο να αναφέρονται τα δικαιώματα που παρέχονται από τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) και τα δικαιώματα και οι ελευθερίες που παρέχονται και σχετίζονται με τα δεδομένα και το απόρρητο των χρηστών.

Βιβλιογραφία

Gari Singh & Jonathan Levi, 2020. *Mipasa Project and ibm Blockchain Team on Open Data Platform to Support Covid-19 Response.* [Online]
Available at: https://www.ibm.com/blogs/blockchain/2020/03/mipasa-project-and-ibm-blo%ckchain-team-on-open-data-platform-to-support-covid-19-response/
[Accessed 27 March 2020].

Επίσηση Εφημερίδα της Ευρωπαϊκής Ένωσης, 2020. Έγγραφο καθοδήγησης σχετικά με την προστασία δεδομένων στις εφαρμογές που στηρίζουν την καταπολέμηση της πανδημίας COVID-19. *ΑΝΑΚΟΙΝΩΣΕΙΣ ΤΩΝ ΘΕΣΜΙΚΩΝ ΚΑΙ ΛΟΙΠΩΝ ΟΡΓΑΝΩΝ ΚΑΙ ΤΩΝ ΟΡΓΑΝΙΣΜΩΝ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,* p. 7.

(ATT), T. A. P., n.d. [Online]
Available at: http://lpccs-docs.dialog-semiconductor.com/tutorial-custom-profile-DA145xx/att.html

11.03.2020, Π. Ν. Π. τ., 2020. *Taxheaven.* [Online]
Available at: https://www.taxheaven.gr/law/%CE%A0%CE%9D%CE%A011.03.2020/2020
[Accessed 11 March 2020].

A Review of India's Contact-tracing App, A. S., 2020. [Online]
Available at: https://www.lexology.com/library/detail.aspx?g=f54419a1-4823-404c-92f3-c5e4f193b733
[Accessed 1 September 2020].

ALTSHULER, T. S. & HERSHKOVITZ , R. A., 2020. DIGITAL CONTACT TRACING AND THE CORONAVIRUS : ISRAELI AND COMPARATIVE PERSPECTIVES. *Foreign Policy at BROOKINGS*, August, p. 13.

Anon., 2020. *github.* [Ηλεκτρονικό]
Available at: https://github.com/OpenCovidTrace/octrace-android/blob/master/README.md

Anon., 2020. *United States. Coronavirus: tiny Iceland has tested more of its population for coronavirus than anyone else and here is what they learned.* [Online]
Available at: https://www.usatoday.com/story/news/world/2020/04/10/coronavirus-covid-19-small-

nations-iceland-big-data/2959797001/

[Accessed 13 April 2020].

Application TousAntiCovid, 2020. *Gouvernement.* [Online]

Available at: https://www.gouvernement.fr/info-coronavirus/tousanticovid

[Accessed 2 December 2020].

apps, C.-1., 2020. *Wikipedia.* [Online]

Available at: https://en.wikipedia.org/wiki/COVID-19_apps

[Accessed 2020].

Apturi Covid Latvia - SPKC, 2020. *Google Play.* [Online].

Bahrain, K. a. N. c. t. a. a. m. d. f. p., 2020. *Amnesty International.* [Online]

Available at: https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/

[Accessed 16 June 2020].

beacons?, W. w. i. a. w.-f. i., 2020. *estimote community portal.* [Online]

Available at: https://community.estimote.com/hc/en-us/articles/200794267-What-are-potential-sources-of-wireless-interference-

[Accessed 15 August 2020].

Beaunoyer & Guitton, 2017. [Online].

Bettina Maria Zimmermann, et al., 2021. *Early Perceptions of COVID-19 Contact Tracing Apps in German-Speaking Countries: Comparative Mixed Methods Study.* [Online]

Available at: https://www.jmir.org/2021/2/e25525

[Accessed 8 February 2021].

BlueTrace, 2020. *BlueTrace protocol.* [Online]

Available at: https://bluetrace.io

Board, E. D. P., 2020. *European Data Protection Board, 'Statement on the Processing of Personal Data in the Context ofthe COVID-19 Outbreak.* [Online]

Available at:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

[Accessed 19 March 2020].

Carmela Troncoso, et al., 2020. *Decentralized Privacy-Preserving Proximity Tracing.* [Online]
Available at: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf
[Accessed 25 May 2020].

Comission, E., 2020. *Coronavirus: EU interoperability gateway for contact tracing and warning apps – Questions and Answers.* [Online]
Available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1905
[Accessed 19 October 2020].

Coronalert - Belgium, 2020. *GooglePlay.* [Online]
Available at: https://play.google.com/store/apps/details?id=be.sciensano.coronalert&hl=en_US&gl=US

Coronalert, 2020. [Online]
Available at: https://coronalert.be/en/

Corona-Warn-App, 2021. *Corona-Warn-App starts in Germany.* [Online]
Available at: https://www.berlin.de/en/news/coronavirus/6204357-6098215-corona-warn-app-starts-in-germany.en.html
[Accessed 1 April 2021].

Covid-19: AP Launches Telemedicine Facility., 2020. [Online]
Available at: https://www.thehindubusinessline.com/news/national/covid-19-ap-launches%-telemedicine-facility/article31332943.ece
[Accessed April 2020].

CovidSafe, 2020. *Protect yourself and the community.* [Online]
Available at: https://www.covidsafe.gov.au/

COVTracer-EN, 2020. [Online]
Available at:
https://covtracer.dmrid.gov.cy/dmrid/covtracer/covtracer.nsf/covtracer01_el/covtracer01_el?OpenDocument

COVTracer, Π. Α., 2020. *Πολιτική Απορρήτου COVTracer.* [Online]
Available at: https://covid-19.rise.org.cy/RISE_CovTracer_Privacy_Policy_GR.pdf
[Accessed 30 March 2020].

Csilla Herendy, 2020. *How were apps developed during, and for, COVID-19? : An investigation into user needs assessment and testing.* [Online]

Available at: https://ieeexplore.ieee.org/document/9237821/authors
[Accessed 23-25 September 2020].

Dan Cooper, Kristof Van Quathem & Anna Oberschelp de Meneses , 2020. *COVID-19 Apps and Websites – The "Pan-European Privacy Preserving Proximity Tracing Initiative" and Guidance by Supervisory Authorities.* [Online]
Available at: https://www.insideprivacy.com/covid-19/covid-19-apps-and-websites-the-pan-european-privacy-preserving-proximity-tracing-initiative-and-guidance-by-supervisory-authorities/
[Accessed 2 April 2020].

Dunlop, A., 2020. Covid-19 Contact tracing: data protection expectations on app development. *Burges Salmon*, 19 May.

EDPB: Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 2020. *Recommendations and functional requirements*, 21 April, p. 9.

Emre Kursat Kaya, 2020. Contact-Tracing Applications: Decentralized Model of Data Storage. *SAFETY AND PRIVACY IN THE TIME OF COVID-19: CONTACT TRACING APPLICATIONS*, June, p. 3.

Energy, B. L., n.d. *Wikipedia.* [Online]
Available at: https://en.wikipedia.org/wiki/Bluetooth_Low_Energy

eRouška, 2020. [Online]
Available at: https://apps.apple.com/cz/app/erou%C5%A1ka/id1509210215
[Accessed 2020].

Fan Yang, Luke Heemsbergen & Robbie Fordyce, 2020. *SAGE journals. Comparative analysis of China's Health Code, Australia's COVIDSafe and New Zealand's COVID Tracer Surveillance Apps: a new corona of public health governmentality?.* [Online]
Available at: https://journals.sagepub.com/doi/full/10.1177/1329878X20968277
[Accessed 29 October 2020].

forin.gr, 2020. *Π.Ν.Π. (ΦΕΚ Α 64 - 14.03.2020) Κατεπείγοντα μέτρα αντιμετώπισης της ανάγκης περιορισμού της διασποράς του κορωνοϊού COVID-19..* [Online]
Available at: https://www.forin.gr/laws/law/3851/katepeigonta-metra-antimetwpishs-ths-anagkhs-periorismou-ths-diasporas-tou-korwnoiou-covid-19#!/?article=38772,38773
[Accessed 14 March 2020].

GATT, B. A. a., χ.χ. [Ηλεκτρονικό]
Available at: https://epxx.co/artigos/bluetooth_gatt.html

GDPR, χ.χ. [Ηλεκτρονικό]
Available at: https://ntokas.gr/anonymous-data/

Guidelines, 2020. *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.* [Online]
Available at: https://iapp.org/resources/article/edpb-guidelines-04-2020-on-the-use-of-location-data-and-contact-tracing-tools-in-the-context-of-the-covid-19-outbreak/
[Accessed 21 April 2020].

Haiying Ren, Jianfeng Shen, Xiaoyong Tang & Tianyi Feng, 2020. *5G Healthcare Applications In COVID-19 Prevention And Control.* [Online]
Available at: https://ieeexplore.ieee.org/document/9303191/authors#authors
[Accessed 30 December 2020].

Hannah van Kolfschooten & Anniek de Ruijter, 2020. *COVID-19 and privacy in the European Union: A legal perspective on contact tracing..* [Online]
Available at: https://doi.org/10.1080/13523260.2020.1771509

HannaTiirinki, et al., 2020. *COVID-19 pandemic in Finland – Preliminary analysis on health system response and economic consequences.* [Online]
Available at: https://www.sciencedirect.com/science/article/pii/S2211883720300770
[Accessed December 2020].

Hart, V. et al., 2020. *Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks.* [Online]
Available at: https://ethics.harvard.edu/outpacing-virus
[Accessed 3 April 2020].

Helsinki, C. u. f., 2020. [Online]
Available at: https://www.hel.fi/helsinki/coronavirus-en/social-and-health/information-about-koronavilkku-app/
[Accessed 2020].

Homo Digitalis, 2020. *Αίτημα Γνωμοδότησης της ΑΠΔΠΧ.* [Online]
Available at: Homo Dig
[Accessed 12 August 2020].

Ichiro Nakamoto , Sheng Wang , Yan Guo & Weiqing Zhuang, 2020. *JMIR Publications. A QR Code–Based Contact Tracing Framework for Sustainable Containment of COVID-19: Evaluation of an Approach to Assist*

the Return to Normal Activity. [Online]
Available at: http://dx.doi.org/10.2196/22321
[Accessed 9 September 2020].

Immuni, 2020. [Online]
Available at: https://www.immuni.italia.it/

Ingram, D., 2020. *NBC news. How contact tracing could use Bluetooth to track coronavirus on your smartphone.* [Online]
Available at: https://www.nbcnews.com/tech/tech-news/how-contact-tracing-could-use-bluetooth-track-coronavirus-your-smartphone-n1187796
[Accessed 27 March 2020].

Introduction, B. L. E. (. 1. T. I., 2020. [Online]
Available at: https://atadiat.com/en/e-bluetooth-low-energy-ble-101-tutorial-intensive-introduction/
[Accessed 2 December 2020].

Janosch Delcker & Stephen Brown, 2020. *Europe Shares Code for New Coronavirus Warning App - POLITICO.* [Online]
Available at: https://www.politico.eu/article/europe-cracks-code-for-coronavirus-warning-app/
[Accessed 1 April 2020].

Jan-Willem van't Klooste, et al., 2021. Corona Notification App. *First Eyetracking Results of Dutch CoronaMelder Contact Tracing and Notification App*, p. 2.

Johannes Abeler, Matthias Bäcker, Ulf Buermeyer & Hannah Zillessen, 2020. COVID-19 Contact Tracing and Data Protection Can Go Together. *JMIR MHEALTH AND UHEALTH*, 14 Apr, pp. 1-2.

Julian Sanchez & Matthew Feeney, 2020. *Cato Institute. Protect Privacy When Contact Tracing..* [Online]
Available at: https://www.cato.org/publications/pandemics-policy/protect-privacy-when-contact-tracing?queryID=352bdac87e46830646920d35a966c116
[Accessed 15 September 2020].

Justin Petrone, 2020. *Estonia's coronavirus app HOIA – the product of a unique, private-public partnership.* [Online]
Available at: https://e-estonia.com/estonias-coronavirus-app-hoia-the-product-of-a-unique-private-public-partnership/
[Accessed September 2020].

Kitchin, R., 2020. *The Programmable City. Using digital technologies to tackle the spread of the coronavirus: Panacea or folly?.* [Online]
Available at: https://progcity.maynoothuniversity.ie/wp-content/uploads/2020/04/Digital-tech-spread-of-coronavirus-Rob-Kitchin-PC-WP44.pdf
[Accessed 21 April 2020].

Korona Stop LT, 2020. [Ηλεκτρονικό]
Available at: https://play.google.com/store/apps/details?id=lt.nvsc.coronawarnapp&hl=en_US&gl=US

Kristin B Sandvik, 2020. *"Smittestopp": If you want your freedom back, download now.* [Online]
Available at: https://journals.sagepub.com/doi/full/10.1177/2053951720939985
[Accessed 28 July 2020].

Laura Bradford, Mateo Aboy & Kathleen Liddell, 2020. *COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes.* [Online]
Available at: https://academic.oup.com/jlb/article/7/1/lsaa034/5848138?login=true
[Accessed January 2020].

Lazaridou, M., 2020. *Mondaq.* [Online]
Available at: https://www.mondaq.com/cyprus/government-measures/938326/data-protection-and-covid-19-one-step-forward-two-steps-back
[Accessed 20 May 2020].

Lempers, Timo, 2021. *Educating the public about the safety of Contact Tracing Apps.,* s.l.: s.n.

Liang, F., 2020. *SAGE journals. COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China.* [Online]
Available at: https://doi.org/10.1177/2056305120947657
[Accessed 11 August 2020].

Luccio, M., 2020. *GPS World. Using contact tracing and GPS to fight spread of COVID-19.* [Online]
Available at: https://www.gpsworld.com/using-contact-tracing-and-gps-to-fight-spread-of-covid-19/
[Accessed 3 June 2020].

M S Abubakari & Mashoedah, 2021. *The Internet of Things (IoT) as an Emerging Technological Solution for the Covid-19 Pandemic Mitigation: An Overview.* [Online]
Available at: https://iopscience.iop.org/article/10.1088/1742-6596/1737/1/012003/pdf
[Accessed 5 October 2020].

Malgieri, G., 2020. Data protection and research: A vital challenge in the era of COVID-19 pandemic. *CLSR*, 12 July, pp. 1-2.

Mamumi Das, 2020. *Role of AI soars in tackling Covid-19 pandemic.* [Online]
Available at: https://www.thehindubusinessline.com/info-tech/role-of-ai-soars-in-tackling-covid-19-pandemic/article31197098.ece
[Accessed 29 March 2020].

Mathieu Cunche, et al., 2020. *On using Bluetooth-Low-Energy for contact tracing.* [Online]
Available at: https://hal.inria.fr/hal-02878346v5/document
[Accessed 1 Sep 2020].

Mozur, P., Zhong, R. & Krolik, A., 2020. *In Coronavirus fight, China gives citizens a color code, with red flags.The New York Times..* [Online]
Available at: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
[Accessed 1 March 2020].

NADEEM AHMED, et al., 2020. *A Survey of COVID-19 Contact Tracing Apps.* [Online]
Available at: https://ieeexplore.ieee.org/document/9144194
[Accessed 15 July 2020].

Nick Abrahams, et al., 2020. Contact tracing apps in. 2 June, pp. 3-4.

O'Neill, P. H., Ryan-Mosley, T. & Johnson, B., 2020. A flood of coronavirus apps are tracking us. Now it's time to keep track of them.. *MIT Technology Review*, 7 May.

Open Gonernment Deutshland, 2020. *Successful Open Government Response to Covid-19.* [Ηλεκτρονικό]
Available at: https://www.open-government-deutschland.de/opengov-en/content/germany-s-corona-warn-app-1767074
[Πρόσβαση 2020].

overflow, S., n.d. *What is a UUID?.* [Online]
Available at: https://stackoverflow.com/questions/292965/what-is-a-uuid

Parliament, E., 2020. *Covid-19 tracing apps: ensuring privacy and use across borders.* [Ηλεκτρονικό]
Available at: https://www.europarl.europa.eu/news/en/headlines/society/20200429STO78174/covid-19-tracing-apps-ensuring-privacy-and-use-across-borders
[Πρόσβαση 1 December 2020].

Patrick Howell O'Neill , Tate Ryan-Mosley & Bobbie Johnson, 2020. *A flood of coronavirus apps are tracking us. Now it's time to keep track of them..* [Online]

Available at: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/
[Accessed 7 May 2020].

PEPP-PT, 2020. Data Protection and Information Security Architecture. *pan-European Privacy-Preserving Proximity Tracing*, 20 April, pp. 9-23.

Philipp H. Kindt, Trinad Chakraborty & Samarjit Chakraborty, 2020. *How Reliable is Smartphone-based Electronic Contact Tracing for COVID-19? A Look through the Lens of Neighbor Discovery Protocols.* [Online]
Available at: https://arxiv.org/pdf/2005.05625.pdf
[Accessed 22 May 2020].

primer, B. t. a. C.-1. A. t., 2020. [Online]
Available at: https://privacyinternational.org/explainer/3536/bluetooth-tracking-and-covid-19-tech-primer
[Accessed 31 March 2020].

Privacy and how we use your data, 2020. [Online]
Available at: https://www2.hse.ie/conditions/coronavirus/covid-tracker-app/privacy-and-how-we-use-your-data.html

Privacy notice • #OstaniZdrav App, 2020. [Online]
Available at: https://podatki.gov.si/sites/default/files/reports/Privacy%20notice.pdf
[Accessed 28 July 2020].

Privacy Policy – COVID Alert Malta, 2020. *COVIDAlert.* [Online]
Available at: https://covidalert.gov.mt/privacy-policy/

Protégete y protege a los tuyos, 2020. [Online]
Available at: https://radarcovid.gob.es/preguntas-frecuentes

Q&A, M. L. D. a. C.-1., 2020. *Mobile Location Data and Covid-19: Q&A.* [Online]
Available at: https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa
[Accessed 13 May 2020].

Qingchuan Zhao, et al., 2020. *On the Accuracy of Measured Proximity of Bluetooth-based Contact Tracing Apps*, p. 3.

Qingchuan Zhao, et al., 2020. Proximity Measurement in BLE-based Contact Tracing. In: *On the Accuracy of Measured Proximity of Bluetooth-based Contact Tracing Apps.* s.l.:s.n., p. 3.

RAJAN GUPTA, et al., 2020. *ACM DL. Analysis of COVID-19 Tracking Tool in India: Case Study of Aarogya Setu Mobile Application.* [Online]
Available at: https://dl.acm.org/doi/10.1145/3416088
[Accessed August 2020].

Raymond Johnston, 2020. *Smartphone app eRouška will track potential contacts with coronavirus carriers.* [Ηλεκτρονικό]
Available at: https://news.expats.cz/weekly-czech-news/smartphone-app-erouska-will-track-potential-contacts-with-coronavirus-carriers/
[Πρόσβαση 15 October 2020].

Ronald L. Rivest, και συν., 2020. *Massachusetts Institute of Technology.* [Ηλεκτρονικό]
Available at: https://people.csail.mit.edu/rivest/pubs/RACCS-2020-PACT.pdf
[Πρόσβαση 4 August 2020].

Samer Obeidat, 2020. *How Artificial Intelligence Is Helping Fight The COVID-19 Pandemic.* [Online]
Available at: https://www.entrepreneur.com/article/348368
[Accessed 30 March 2020].

Sera Whitelaw , Mamas A Mamas, Eric Topol & Harriette G C Van Spall, 2020. Applications of digital technology in COVID-19 pandemic planning and response.. *Viewpoint*, 29 June, p. 1.

Serge Vaudenay, 2020. *Centralized or Decentralized? The Contact Tracing Dilemma.* [Online]
Available at: https://eprint.iacr.org/2020/531.pdf
[Accessed 6 May 2020].

Sheikh Mohammad Idrees, Mariusz Nowostawski & Roshan Jameel, 2020. *Blockchain based Digital Contact Tracing Applications for Pandemic Management (COVID-19): Issues, Challenges, Solutions and Future Directions.* [Online]
Available at: https://preprints.jmir.org/preprint/25245
[Accessed 8 December 2020].

Sheikh Mohammad Idrees, Mariusz Nowostawski & Roshan Jameel, 2021. *JMIR Publications.* [Online]
Available at: https://medinform.jmir.org/2021/2/e25245
[Accessed 24 October 2020].

smitte|stop, 2020. *Smittestop.* [Online]
Available at: https://smittestop.dk/

STAYAWAY COVID app, 2020. [Online]
Available at: https://ciencias.ulisboa.pt/en/stayaway-covid-app

STAYAWAY COVID, 2020. [Online]
Available at: https://stayawaycovid.pt/frequently-asked-questions/
[Accessed 2020].

STOP COVID ProteGO Safe, 2020. *gov.pl.* [Online]
Available at: https://www.gov.pl/web/protegosafe
[Accessed 2020].

Stop COVID-19, 2020. *koronavirus.gr.* [Online]
Available at: https://www.koronavirus.hr/stop-covid-19-723/723?__cf_chl_jschl_tk__=40ce1a0158c1c4a961377d6c6f0e8fb03bccf165-1618586638-0-AdCEIAUaVMA0_xX-ZzYy7vn53rZh397XWhm5a4Swc_yXM3amNXD3ykbgfrZS5a24LIk5bwS8KJw3vkW5jqtDuBzDuUNW-NNj4vA4jSP37jMWDZ37_R57yzI3SVkLoAqfnj0T

Stopp Corona App, 2020. *How the "Stopp Corona" App Can Help Your Peace of Mind.* [Ηλεκτρονικό]
Available at: https://www.austria.info/en/service-and-facts/coronavirus-information/app
[Πρόσβαση 2020].

T. Wright, 2020. *Blockchain App Used to Track COVID-19 Cases in Latin America.* [Online]
Available at: https://cointelegraph.com/news/blockchain-app-used-to-track-covid-19-ca%ses-in-latin-america
[Accessed April 2020].

Tania Martin, et al., 2020. *Demystifying COVID-19 Digital Contact Tracing: A Survey on Frameworks and Mobile Apps.* [Online]
Available at: https://www.hindawi.com/journals/wcmc/2020/8851429/
[Accessed 16 July 2020].

Tanvir Rahman, Taslima Ferdaus Shuva, Risala Tasin Khan & Mostofa Kamal Nasir, 2021. A Review of Contact Tracing Approaches for Controlling COVID-19 Pandemic. *Global Journal of Computer Science and Technology: HInformation & Technology*, p. 33.

Tawari, 2020. An introduction to QR code technology. *International Conference on Information Technology*, 22-24 December, p. 1.

The #OstaniZdrav mobile application, 2020. *The #OstaniZdrav mobile application.* [Online]
Available at: https://www.gov.si/en/topics/coronavirus-disease-covid-19/the-ostanizdrav-mobile-application/

The Smittestopp app, 2020. [Online]
Available at: https://www.helsenorge.no/en/smittestopp/#smittestopp-protects-your-privacy

Tianshi Li, et al., 2020. *DECENTRALIZED IS NOT RISK-FREE: UNDERSTANDING PUBLIC PERCEPTIONS OF PRIVACY-UTILITY TRADE-OFFS IN COVID-19 CONTACT-TRACING APPS*, 26 May, pp. 7-8.

Tobias Weitze & Henrique Barros, 2020. CONTACT TRACING APPS - Repository of Basic Technical Terms for Public Health Professionals. *The Associaton of Schools of Public Health in the European Region (ASPHER)*, July, p. 3.

Turki Alanzi, 2021. *A Review of Mobile Applications Available in the App and Google Play Stores Used During the COVID-19 Outbreak.* [Online]
Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7812813/
[Accessed 12 January 2021].

Umaer Naseer, et al., 2020. *Use of the Smittestopp app for contact tracing: validation study protocol*, 23 June, pp. 8-9.

Védd meg magad a koronavírustól, 2020. *virusradar.hu.* [Online]
Available at: https://virusradar.hu/

Vi Hart, et al., 2020. Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks. 3 April, p. 18.

Vikram Sharma Mailthody, et al., 2021. *Safer Illinois and RokWall: Privacy Preserving University Health Apps for COVID-19.* [Online]
Available at: https://arxiv.org/pdf/2101.07897.pdf
[Accessed 2021].

Vinay Chamola, Vikas Hassija, Vatsal Gupta & Mohsen Guizani, 2020. *A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact.* [Online]
Available at: https://ieeexplore.ieee.org/document/9086010/authors#authors
[Accessed 13 May 2020].

Vinay Chamola, Vikas Hassija, Vatsal Gupta & Mohsen Guizani, 2020. *A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact.* [Online]

Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9086010
[Accessed 4 May 2020].

VirusRadar, 2020. *GooglePlay.* [Online]
Available at: https://play.google.com/store/apps/details?id=hu.gov.virusradar&hl=en_CA&gl=US

W.H.P, 2020. *Coronavirus disease (COVID-19).* [Online]
Available at: https://www.who.int/news-room/q-a-detail/q-a-coronaviruses
[Accessed 12 October 2020].

What are broadcasting power, r. a. o. c. o. a. b. s., 2020. *estimote community portal.* [Online]
Available at: https://community.estimote.com/hc/en-us/articles/201636913-What-are-Broadcasting-Power-RSSI-and-othercharacteristics-of-a-beacon-s-signal-
[Accessed 15 August 2020].

Wikipedia, 2020. *Wikipedia.* [Online]
Available at: https://en.wikipedia.org/wiki/Pan-European_Privacy-Preserving_Proximity_Tracing
[Accessed 2020].

Wikipedia, 2020. *Wikipedia - Decentralized Privacy-Preserving Proximity.* [Ηλεκτρονικό]
Available at: https://en.m.wikipedia.org/wiki/Decentralized_Privacy-Preserving_Proximity_Tracing
[Πρόσβαση 2020].

Wikipedia, χ.χ. *Gathering of personally identifiable information.* [Ηλεκτρονικό]
Available at: https://en.wikipedia.org/wiki/Gathering_of_personally_identifiable_information

Wiley Online Library, 2020. *Herd-immunity across intangible borders: Public policy responses to COVID-19 in Ireland and the UK.* [Online]
Available at: https://doi.org/10.1002/epa2.1096
[Accessed 26 November 2020].

Αντιγόνη Λογοθέτη, et al., 2020. *COVID - 19 & ΨΗΦΙΑΚΑ ΔΙΚΑΙΩΜΑΤΑ ΣΤΗΝ ΕΛΛΑΔΑ.* [Online]
[Accessed 22 April 2020].

διατάξεις., Φ. 7. Α. 3. Π. Ν. Π. Μ. α. τ. π. τ. κ. C.-1. κ. ά. κ., 2020. *Helenic Hoteliers Federation.* [Online]
Available at: https://www.hhf.gr/2020/03/31/%CF%86%CE%B5%CE%BA-75-%CE%B1-30-3-2020-%CF%80%CF%81%CE%B1%CE%BE%CE%B7-%CE%BD%CE%BF%CE%BC%CE%BF%CE%B8%CE%B5%CF%84%CE%B9%CE%BA%CE%BF%CF%85-%CF%80%CE%B5%CF%81%CE%B9%CE%B5%CF%87%CE%BF%CE%BC%CE%B5%CE%BD/
[Accessed 30 March 2020].

ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΒΙΟΗΘΙΚΗΣ, 2020. *COVID 19 (ΚΟΡΩΝΟΙΟΣ) - ΖΗΤΗΜΑΤΑ ΙΧΝΗΛΑΤΗΣΗΣ ΚΡΟΥΣΜΑΤΩΝ ΚΑΙ ΕΠΑΦΩΝ ΤΟΥΣ.* [Online]
Available at: http://www.bioethics.gr/images/pdf/GNOMES/Contact_tracing_COVID-19_Final_GR.pdf
[Accessed 2020].

Ιακωβίδης, Σ., 2020. *Κορωνοϊός, το παράδειγμα Ταϊβάν, Ν. Κορέας, Σιγκαπούρης- Η σωτήρια συνταγή: Έγκαιρη προετοιμασία, τεχνολογία, διαφάνεια..* [Online]
Available at: https://www.apopseis.com/koronoios-to-paradeigma-taivan-n-koreas-sigkapoyris-i-sotiria-syntagi-egkairi-proetoimasia-technologia-diafaneia/eia/
[Accessed 2020].

Παναγοπούλου-Κουτνατζή, Φ., 2020. Ειδικότερα το ζήτημα της ιχνηλατήσεως. In: *Η προστασία προσωπικών δεδομένων σε περίοδο πανδημίας. .* s.l.:s.n., p. 10.

Πράξη Νομοθετικού Περιεχομένου της 14.03.2020 Κατεπείγοντα μέτρα αντιμετώπισης της ανάγκης περιορισμού της διασποράς του κορωνοϊού COVID-19, κ. μ. τ. 4., 2020. *TaxHeaven.* [Ηλεκτρονικό]
Available at: https://www.taxheaven.gr/law/%CE%A0%CE%9D%CE%A014.03.2020/2020
[Πρόσβαση 14 March 2020].

Πράξη Νομοθετικού Περιεχομένου της 25.02.2020 Κατεπείγοντα μέτρα αποφυγής και περιορισμού της διάδοσης κορωνοϊού., κ. μ. τ. 4., 2020. *TAXHEAVEN.* [Online]
Available at: https://www.taxheaven.gr/law/%CE%A0%CE%9D%CE%A025.02.2020/2020
[Accessed 2 Feb 2020].

Τσιάκα, Β., 2020. *Η συμβολή της τεχνολογίας στην αντιμετώπιση των προκλήσεων της υγείας του 21ου αιώνα και ειδικότερα της πανδημίας Covid-19.* [Online]
Available at:
http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/13024/%ce%a4%cf%83%ce%b9%ce%ac%ce%ba%ce%ba%ce%b1%20%ce%92%ce%b1%cf%83%ce%b9%ce%bb%ce%b9%ce%ba%ce%ae.pdf?sequence=1&isAllowed=y
[Accessed 26 October 2020].

Τσιλιώτης, Χ., 2020. *https://www.syntagmawatch.gr/.* [Online]
Available at: https://www.syntagmawatch.gr/trending-issues/pandimia-kai-perioristika-metra-meros-ii-oi-arxes-tis-analogikotitas-kai-tis-apagorefsis-paraviasis-tou-pirina-tou-dikaiomatos/
[Accessed 9 April 2020].