HADPP ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ & ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Εφαρμογές ιχνηλάτησης και ιδιωτικότητα

Covid-19: Δικαϊκές Επιπτώσεις & Προοπτικές
eThemis - 20 & 21 Νοεμβρίου 2020

Σπύρος Τάσσης
Δικηγόρος (LL.M),
Πρόεδρος Ένωσης Προστασίας Προσωπικών Δεδομένων και Ιδιωτικότητας

Πανδημία και Ιδιωτικότητα

Μοιάζει να έχουμε σύγκρουση θεμελιωδών δικαιωμάτων:

1. **Το άρθρο 21 παρ. 3 κατοχυρώνεται ως (αρνητικό) ατομικό αλλά και ως κοινωνικό δικαίωμα, το ίδιο και το άρθρο 9 παρ. 1 που ορίζει απαραβίαστη την ιδιωτική και οικογενειακή ζωή του ατόμου.**

1. **Όμως, το δικαίωμα στην προστασία των δεδομένων μας δεν είναι ένα απόλυτο δικαίωμα, το ορίζει αυτό εξαρχής ο ίδιος ο Γενικός Κανονισμός. Πρέπει να εκτιμάται κι αυτό σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται με άλλα θεμελιώδη δικαιώματα, σύμφωνα με την αρχή της αναλογικότητας.**

Σπύρος Τάσσης

Το διακύβευμα μίας παράξενης εποχής

Σε όλη αυτή την περίοδο των περιορισμών στην μετακίνηση και την αναγκαία επεξεργασία προσωπικών δεδομένων και, δη, ευαίσθητων (ειδικής κατηγορίας κατά τον ΓΚΠΔ) αναπτύχθηκαν σχεδόν αυτόματα δύο εκ διαμέτρου αντίθετες απόψεις για την διαχείριση της κρίσης:

- **Η πρώτη θεωρεί αδιανόητη την συζήτηση για προστασία των προσωπικών δεδομένων και της ιδιωτικότητας σε τέτοιες καταστάσεις και επιμένει ότι στο πλαίσιο της αντιμετώπισης της πανδημίας θα πρέπει να ληφθούν ακόμα και τα πιο επαχθή μέτρα που εισάγουν μεθόδους πραγματικού γεωεντοπισμού του γενικού πληθυσμού και την επεξεργασία ταυτοποιήσιμων δεδομένων όχι μόνο για όσους νοσούν αλλά και για έναν ευρύ οικογενειακό και κοινωνικό κύκλο γύρω τους.**
- **Η δεύτερη άποψη ακολουθώντας την ίδια απολυτότητα στην λογική της διαστρωμάτωσης των επιχειρημάτων θεωρεί ότι οποιαδήποτε μορφή περιορισμού της γενικής προστασίας και των περιορισμών στην επεξεργασία προσωπικών δεδομένων είναι αδιανόητη αφού ουσιαστικά θα οδηγήσει σε μία νέα κατάσταση εποπτείας των υποκειμένων που θα οδηγήσει σε μία κοινωνία υπό διαρκή εποπτεία (surveillance society).**

Σπύρος Τάσσης

Ιχνηλάτηση ή μαζική παρακολούθηση;

Πράγματι, ένας τέτοιος μηχανισμός ιχνηλάτησης έχει τη δυνατότητα να αποτελέσει εργαλείο μαζικής παρακολούθησης, κακής χρήσης προσωπικών δεδομένων και καταστρατήγησης των θεμελιωδών δικαιωμάτων.

Το κατά πόσο αυτό θα αποφευχθεί εξαρτάται από τον τρόπο υλοποίησης, τη διαφάνεια λειτουργίας τους, και την εμπιστοσύνη των πολιτών προς τους θεσμούς και τις εταιρίες τεχνολογίας. νόμιμη βάση επεξεργασίας

Πώς λειτουργεί μία εφαρμογή ιχνηλάτησης

Συστήματα centralized και decentralized

Τεχνολογία γεωεντοπισμού (GPS) και BLTE (Bluetooth Low Energy)

Στα συστήματα γεωεντοπισμού γίνεται αναγκαστική χρήση των δεδομένων θέσης και κίνησης των κινητών συσκευών.

Η τεχνολογία BTLE έχει εμβέλεια περίπου 80 μέτρα. Επειδή οι κωδικοί μεταδίδονται σε μικρά διαστήματα (4-5 φορές το δευτερόλεπτο), το σύστημα μπορεί να καταχωρίσει για παράδειγμα μόνο κωδικούς που λαμβάνονται για περισσότερο από 2 λεπτά σε απόσταση λιγότερη από 5 (περίπου) μέτρα. Το τηλέφωνό του χρήστη κατεβάζει ανά τακτικά διαστήματα (π.χ., μία φορά τη μέρα) το αρχείο με όλους τους κωδικούς από άτομα που έχουν διαγνωστεί θετικά τις τελευταίες 2 εβδομάδες στη περιοχή τους. Το τηλέφωνο συγκρίνει τους κωδικούς της λίστας με τους κωδικούς που έχει καταγράψει στη μνήμη τις τελευταίες 14 ημέρες. Δεν απαιτείται ταυτοποίηση του χρήστη, αλλά εθελοντική του γνωστοποίηση εφόσον έχει βρεθεί σε επαφή ή ύποπτη εγγύτητα με κρούσμα.

Ρυθμιστικό πλαίσιο

Ο EDPB, όπως και η ΑΠΔΠΧ, θεωρεί ότι το υπάρχον θεσμικό πλαίσιο για την προστασία των δεδομένων λαμβάνει ήδη υπόψη τις διαδικασίες επεξεργασίας δεδομένων που είναι απαραίτητες για να συμβάλουν στην καταπολέμηση μιας επιδημίας, επομένως δεν υπάρχει λόγος να αρθούν οι διατάξεις του GDPR, αλλά, αντιθέτως, θα πρέπει να τηρηθούν, ακόμα και στα άκρα όρια του.

«Όταν η επεξεργασία προσωπικών δεδομένων είναι απαραίτητη στο πλαίσιο του COVID-19, η προστασία δεδομένων είναι απαραίτητη για την οικοδόμηση εμπιστοσύνης, την δημιουργία προϋποθέσεων για κοινωνική αποδοχή οποιασδήποτε πιθανής λύσης και, ως εκ τούτου, για τη διασφάλιση της αποτελεσματικότητας αυτών των μέτρων» (Andrea Jelinek)

Νόμιμη βάση επεξεργασίας δεδομένων

- Για όσα δεδομένα δημιουργούνται στο πλαίσιο ηλεκτρονικών επικοινωνιών εφαρμόζονται οι ρυθμίσεις της 58/2002 που σημαίνει ότι ο πάροχος δεν μπορεί να τα διαβιβάσει σε δημόσιες αρχές, παρά μόνο με συγκατάθεση του υποκειμένου ή αφού έχουν καταστεί ανώνυμα (και 3471/2006 άρθρα 6.4 ανώνυμα και 6.5 κατάσταση ανάγκης)

- Για τα δεδομένα μέσω εφαρμογών (υπηρεσίες ΚτΠ) είτε η συγκατάθεση (με ότι αυτή η βάση απαιτεί και συνεπάγεται), όταν η χρήση της εφαρμογής γίνεται σε εθελοντική βάση, είτε τα άρθρα 6.1.ε (και 9.1.θ;) του Κανονισμού όταν η χρήση της εφαρμογής είναι υποχρεωτική από τις αρμόδιες Αρχές για τον έλεγχο της εξάπλωσης της πανδημίας.

Οριοθέτηση εφαρμογής και χρήσης

- Τα δεδομένα θέσης συλλέγονται είτε από τους παρόχους ηλεκτρονικών επικοινωνιών είτε από παρόχους υπηρεσιών ΚτΠ μέσω πρόσθετων εφαρμογών.

- Θα πρέπει να είναι μέρος μίας δομημένης δημόσιας πολιτικής πρόληψης της πανδημίας.

- Αρχή της αναλογικότητας σε κάθε εφαρμογή

- Να συνοδεύεται από εγκεκριμένα κατάλληλα μέτρα.

- Πρέπει να προτιμώνται τα ανώνυμα δεδομένα και μόνο εφόσον οι στόχοι δεν επιτυγχάνονται να γίνεται επεξεργασία και ταυτοποιήσιμων δεδομένων.

Αρχές λειτουργίας

- Οι εφαρμογές ιχνηλάτησης επαφών θα πρέπει να διέπονται από τις αρχές της ελαχιστοποίησης και της προστασίας των δεδομένων από τον σχεδιασμό και εξ' ορισμού.
- Δεν φαίνεται απαραίτητο (και αναλογικό) να γίνεται και γεωεντοπισμός του χρήστη αλλά μόνο τα δεδομένα εγγύτητας με άλλους χρήστες.
- Τα δεδομένα να αποθηκεύονται καταρχήν στην συσκευή του χρήστη και μόνο οι απαραίτητες πληροφορίες και αφού υπάρχει ενεργοποίηση της επισήμανσης, να αποστέλλονται σε υπηρεσία δομημένης δημόσιας πολιτικής πρόληψης της πανδημίας,
- Το αποκεντρωμένο σύστημα (decentralized) φαίνεται να είναι το προτιμότερο για την μεγαλύτερη δυνατότητα προστασίας των υποκειμένων από περιττή επεξεργασία και δημιουργία προφίλ.

Εφαρμογές ιχνηλάτησης στην ΕΕ

Ορισμένες χώρες επιλέγουν centralized ιχνηλάτηση με διακρίβωση τοποθεσίας βάσει κινητού δικτύου αντί για εφαρμογές και χωρίς την ανάγκη λήψης μιας εφαρμογής. Οι λύσεις αυτές δίνουν πρόσβαση σε δεδομένα τοποθεσίας και έχουν σημαντικά πιθανά ζητήματα με το απόρρητο των επικοινωνιών.

Ο στόχος των decentralized λύσεων είναι να μειωθεί ο αντίκτυπος για την προστασία της ιδιωτικής ζωής, ανταλλάσσοντας ανώνυμα κλειδιά που δεν περιλαμβάνουν ταυτοποιήσιμες πληροφορίες… (όμως χρειάζεται >80% χρηστών για αποτελεσματικότητα)

Πολλές χώρες που ξεκίνησαν με centralized ιχνηλάτηση (όπως π.χ. Γερμανία και Η.Β.) στην πορεία επέλεξαν τις decentralized λύσεις.

Εφαρμογές ιχνηλάτησης στην ΕΕ

Οι Apple και Google άνοιξαν τις σχετικές λειτουργίες των λογισμικών τους στα κινητά τηλέφωνα και δημιούργησαν μία πλατφόρμα ιχνηλάτησης που επιτρέπει στα κινητά τηλέφωνα με λογισμικό iOS και Android να ιχνηλατούν το ένα το άλλο μέσω τεχνολογίας BLTE με τρόπο που, όπως ισχυρίζονται, δεν αποκαλύπτονται προσωπικά δεδομένα και είναι σχεδιασμένη ώστε να αποτελεί το ένα μόνο κομμάτι μίας συνολικής τεχνολογικής λύσης που στο σύνολο της δεν ανήκει σε αυτές αλλά ούτε και στις δημόσιες αρχές.

Περαιτέρω, τα κράτη ανά το κόσμο καλούνται να αναπτύξουν το άλλο κομμάτι, που θα είναι μία εφαρμογή για κινητά, που θα βασίζεται και χρησιμοποιεί την πλατφόρμα των Apple/Google και η εγκατάσταση της από τους πολίτες θα γίνεται εθελοντικά.

Συμπέρασμα 1/2

Τέτοιου είδους μηχανισμοί θεωρούνται απαραίτητοι για την έξοδο από τα μέτρα καραντίνας, στα οποία βρίσκονται πολλές χώρες, όπως και η Ελλάδα, με στόχο το άνοιγμα της οικονομίας και την πιο ελεύθερη μετακίνηση των πολιτών με παράλληλο περιορισμό τυχόν επανεκκίνησης μίας εκθετικής μετάδοσης του ιού.

Εκτός από τα άμεσα και μεσοπρόθεσμα οφέλη για την συγκεκριμένη πανδημία του Covid-19, η καθιέρωση μιας τέτοιας τεχνολογικής λύσης μπορεί να αποτελέσει και έναν αποτελεσματικό τρόπο για την καλύτερη και πιο έγκαιρη διαχείριση παρόμοιων κρίσεων στο μέλλον.

Συμπέρασμα 2/2

Όμως:

- χρειάζεται μία εξισορρόπηση του κοινωνικού οφέλους για την δημόσια υγεία έναντι του κρατικού περιορισμού των ατομικών δικαιωμάτων
- χρειαζόμαστε «εκτιμήσεις επιπτώσεων στα ανθρώπινα δικαιώματα»
- ο μεγαλύτερος κίνδυνος είναι να εθιστούμε στον περιορισμό των δικαιωμάτων μας ως απαραίτητο μέτρο για την επιβίωση μας
- απαιτείται πλήρης διαφάνεια της λειτουργίας τους και επαρκής λογοδοσία
- απαιτείται σεβασμός στις ανάγκες και τις ανησυχίες των πολιτών
- χρειάζεται περιορισμός της έκτασης του μέτρου, του χρόνου εφαρμογής και επαρκής ασφάλεια για τα δεδομένα
- χρειάζεται να υπάρχει εμπιστοσύνη προς τους δημόσιους φορείς
- στόχος δεν μπορεί να είναι η σύγκρουση αλλά η σωρευτική προστασία των δικαιωμάτων

Ευχαριστώ

Σπύρος Τάσσης

HADPP ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ & ΙΔΙΩΤΙΚΟΤΗΤΑΣ

www.dataprotection.gr
Info@dataprotection.gr
info@tassis.com