Smart phone: ο ψηφιακός χαφιές

Κώστας Π. Κατάρας

Η ψηφιακή τεχνολογία επέφερε ένα τεράστιο πλήγμα στην ιδιωτικότητα του ατόμου που, είτε παραδόθηκε στη σαγήνη ασήμαντων εφαρμογών (Apps) που του απομυζούν προσωπικές πληροφορίες για εμπορικούς και όχι μόνο σκοπούς, είτε προδόθηκε από το κράτος που θέλει να ξέρει όσα περισσότερα για κάθε πολίτη ώστε να τον ελέγχει και να τον χειραγωγεί, με απολυταρχικές πρακτικές.

Υπάρχουν πολλά εργαλεία ώστε οι θηρευτές πληροφοριών να απογυμνώσουν το άτομο: από την βιομετρική επιτήρηση έως τα συστήματα κοινωνικής εμπιστοσύνης (social credit systems) στη Κίνα και το ελληνικό υβρίδιό του , τον υπερ-Τειρεσία, έως φυσικά το ίντερνετ και τα social media. Όμως τίποτε δεν είναι πιο θανατηφόρο, που φέρνει και το τέλος της ιδιωτικότητας όσο δύο εργαλεία στα οποία ωθούν οι κυβερνήσεις να κάνουμε σήμερα, βίαια, μέγιστη χρήση: το κινητό τηλέφωνο και το πλαστικό/ψηφιακό χρήμα (CBDC) . Και τα δύο είναι εργαλεία που, αν το σκεφθείς, στα επιβάλει το κράτος (πχ φορολογική δήλωση, ανάληψη σύνταξης , χτίσιμο αφορολόγητου υποχρεωτικά με ηλεκτρονικά μέσα, Covid Wallet, ψηφιακή ταυτότητα, ταυτοποιητικά έγγραφα μόνο από Gov.gr, κλπ). Σε αντίθεση με άλλα εργαλεία που μπορείς ελεύθερα να αποφασίσεις εσύ για τη χρήση τους . Για παράδειγμα, για το ίντερνετ μπορείς να κάνεις ασφαλή πλοήγηση μέσα από σύνδεση VPN ή/και πιο ασφαλείς browsers, ενώ τα social media μπορείς να τα σταματήσεις ή να γίνεις σχεδόν αόρατος. (Για το πλαστικό/ψηφιακό χρήμα (CBDC) θα ασχοληθούμε σε ξεχωριστό σημείωμα)

Το VPN (Virtual Private Network), δηλαδή εικονικό ιδιωτικό δίκτυο, ως γνωστό προσφέρει υψηλής ασφάλειας κρυπτογράφηση δεδομένων που επιτρέπει άρση γεωγραφικών περιορισμών, παράκαμψη κρατικής λογοκρισίας, ασφαλή σύνδεση σε κοινόχρηστη χρήση WiFi, και πολλές κοινόχρηστες IP για απόλυτη ανωνυμία χρήστη. Υπάρχουν δωρεάν υπηρεσίες VPN (πχ ProtonVPN, Atlas VPN) και πληρωμένες με μικρό κόστος (πχ NordVPN, CyberGhost, κλπ)

Κινητό : όπως λέμε «ψηφιακές χειροπέδες» ;

Ιδιαίτερα από το 2007 που ήρθε στην αγορά το iPhone, οι φόβοι για την απώλεια της ιδιωτικότητας από τα κινητά τηλέφωνα αυξάνονται. Φυσικά, στην πλειοψηφία αφορούν την εμπορική εκμετάλλευση προσωπικών δεδομένων του ατόμου, αλλά υπάρχει και το κρίσιμο θέμα της παρακολούθησης - με εγκατάσταση στο κινητό λογισμικού κατασκοπίας - πολιτικών αντιπάλων, στρατιωτικών, δημοσιογράφων, οικονομικών παραγόντων, κτλ όπως έδειξε το σκάνδαλο Predator / Pegasus στην Ελλάδα. Η Ελλάδα δεν είναι η μόνη χώρα που συμβαίνει κάτι τέτοιο, αφού ιδιαίτερα το Pegasus (που δίνει 100% πρόσβαση στα προσωπικά δεδομένα του στόχου και έχει τεχνολογία "zero click", δηλαδή δεν απαιτεί ο χρήστης να πατήσει κάποιο λίνκ/σύνδεσμο ή να κάνει κάποια κίνηση στο κινητό του), είναι το λογισμικό που προτιμούν κράτη στην ΕΕ αλλά και καταπιεστικά καθεστώτα σε όλο το κόσμο. Έτσι το βρίσκουμε από τα ΗΑΕ, την Ταϊλάνδη, την Rwanda και την Σ. Αραβία ,έως την Ουγγαρία και την Ισπανία. (R. Deibert: *"The Autocrat in your iPhone",* Foreign Affairs, Jan 2023).

Η εντυπωσιακή αύξηση της υφαρπαγής των προσωπικών δεδομένων όλων των κατόχων κινητού τηλεφώνου και η παρακολούθηση στόχων όπως με το Predator, οφείλεται μεταξύ άλλων:

Πρώτον, λόγω της παγκόσμιας προώθησης και ανάπτυξης μιας ψηφιακής κουλτούρας που λέει «πάντα διαθέσιμοι – πάντα συνδεδεμένοι» με το κινητό μας τηλέφωνο. Δεύτερον, το σύγχρονο κακόβουλο λογισμικό προσφέρει κομψούς τρόπους παράκαμψης του εμποδίου της κρυπτογράφησης (end-to-end encryption) που αποτελούσε εμπόδιο στα μαζικά προγράμματα επιτήρησης διαφόρων κυβερνητικών «υπηρεσιών / οντοτήτων» . Ένας τρίτος παράγοντας ώθησης του «κλάδου» ήταν η ανάπτυξη κινημάτων διαμαρτυρίας που έγιναν εφικτά με τη βοήθεια της ψηφιακής τεχνολογίας (πχ από την πλατεία Tahrir / Αίγυπτος 2010/11, έως το Ιράν το 2022 με την #MalisaAmini) και η αντιμετώπισή τους από τις κυβερνήσεις. Τέταρτον, η «ιδιωτικοποίηση» της εθνικής ασφάλειας και των εθνικών υπηρεσιών πληροφοριών από πλευράς κυβερνήσεων, που για μια σειρά από λόγους (πχ προηγμένη τεχνολογία, αποποίηση ευθυνών, αποφυγή θεσμικού ελέγχου, κα) στράφηκαν στο λεγόμενο «μισθοφορικό λογισμικό κατασκοπίας» (mercenary spyware), δηλαδή ιδιωτικές εταιρείες πρώην στελεχών κρατικών υπηρεσιών, όπως η πολύ γνωστή Ισραηλινή NSO Group που έχει το Pegasus.

Αλλά αν τα πιο πάνω είναι μάλλον αναμενόμενα και αφορούν κύρια πολιτικές, στρατιωτικές, οικονομικές και μιντιακές ελίτ, καθώς και παιχνίδια δύναμης και εξουσίας, για τον συνηθισμένο πολίτη η αγωνία του είναι η χαμένη ιδιωτικότητά του και η εμπορική εκμετάλλευση από τρίτους όχι μόνο των προσωπικών του πληροφοριών, αλλά τελικά ο περιορισμός της ελεύθερης βούλησης και των δημοκρατικών διεκδικήσεων. Κάτι τέτοιο αποτελεί σημαντικό πλήγμα της αυτονομίας του, κάτι που θέλει και έχει δικαίωμα να προστατεύσει.

Μπορείς να προστατέψεις την ιδιωτικότητά σου από το κινητό;

Η γρήγορη απάντηση δυστυχώς είναι όχι. Πρακτικά δεν υπάρχει σήμερα τρόπος κάποιος να προστατέψει τα προσωπικά δεδομένα του, τις επικοινωνίες του, τη θέση όπου βρίσκεται ή βρέθηκε, τη δραστηριότητα του και κάθε πληροφορία στο έξυπνο τηλέφωνό του (smart phone), αλλά και σε έξυπνα ρολόγια, ηχεία, «έξυπνους» εικονικούς βοηθούς (Google Assistant, Amazon Alexa, Apple Siri).

Ενδεικτικά να αναφερθούμε πχ στο γεωεντοπισμό, μια από τις πολλές τεχνικές επιτήρησης μέσω του κινητού τηλεφώνου. Η τεχνολογία ενός διαφημιστή στις ΗΠΑ με τη χρήση «γεωφράκτη» (geo-fencing), επιτρέπει να εντοπίζουν και να στέλνουν προπαγάνδα οργανώσεων εναντίον των αμβλώσεων, απευθείας στο τηλέφωνο μιας γυναίκας ενώ αυτή βρίσκεται σε μια αίθουσα αναμονής μιας κλινικής αμβλώσεων ή να την περιμένουν με πλακάτ και συνθήματα κατά την έξοδό της (WSJ: *"Phones know who went to an abortion clinic"*, 7/8/2022). Φυσικά παρόμοιες εφαρμογές μπορούν να υπάρχουν για κάθε χώρο που βρισκόμαστε με ένα κινητό στη τσέπη μας: από μια αντικαρκινική κλινική και ένα ιατρείο γνωστού ανδρολόγου ή στο… ενεχυροδανειστήριο Ριχάρδος, ή αν τρώμε κάθε βράδυ ¨χρυσές μπριζόλες¨ αξίας χιλιάδων ευρώ στη Μύκονο στο μαγαζί του Salt Bae (ενδιαφέρει τις φορολογική αρχές να βλέπουν ονομαστικά από το κινητό τους και σε πραγματικό χρόνο ποιοι είναι εκεί , ενώ δηλώνουν ετήσιο εισόδημα 5.000 ευρώ, όπως το 40% των Ελλήνων φορολογουμένων!!)

Για όσους πιστεύουν ότι μια τέτοια φασιστική επιτήρηση παραβαίνει την κόκκινη γραμμή των ηθικών και δημοκρατικών αξιών τους και την ελευθερία τους, θα πρέπει ίσως να σκεφθούν να βγάλουν από την ντουλάπα και να χρησιμοποιήσουν το παλαιό, με πλήκτρα, κινητό τους από το οποίο να βγάζουν τη μπαταρία όταν δεν κάνουν χρήση, κάτι που δεν είναι εφικτό στα σημερινά «έξυπνα» κινητά.

Για όσους δεν μπορούν να αποχωριστούν το έξυπνο κινητό τους , ίσως μπορούν να πάρουν κάποια ελάχιστα μέτρα προστασίας της ιδιωτικότητάς τους, όπως : επιλογή Airplane Mode όταν δεν χρειάζονται να κάνουν ή να λάβουν τηλεφωνήματα/μηνύματα , κλπ, απαγόρευση γεωεντοπισμού/γνωστοποίηση τοποθεσίας γενικά αλλά και στις εφαρμογές (apps) που ζητούν κάτι τέτοιο (πχ φωτογραφίες), απαγόρευση / ελαχιστοποίηση εγκρίσεων (permissions) στις διάφορες εφαρμογές, χρήση λιγότερο «κατασκοπευτικών» προγραμμάτων πλοήγησης (πχ DuckDuckGo), προτίμηση σε εφαρμογές με κρυπτογράφηση, δηλαδή end-to-end encryption (πχ για εφαρμογές μηνυμάτων πολλοί σήμερα προτιμούν το signal), όχι χρήση δημόσιου wi-fi,κλπ. Επιπλέον, αν είναι εφικτό, χρησιμοποιείστε μόνο τον Η/Υ στο σπίτι σας, με μια σύνδεση VPN που κερδίζει συνεχώς έδαφος ή/και μη-ταυτοποιήσιμο λογαριασμό email (πχ Tutanota, Mail.com) με τα οποία δεν μπορούν (;) να κλέψουν τα προσωπικά σας δεδομένα. Βέβαια, για καλό και κακό, βάλτε και ένα αυτοκόλλητο στη κάμερα του υπολογιστή σας!!

Όλα αυτά φαντάζουν λίγο ύποπτα, αλλά έχουμε ήδη μπει σε μία εποχή όπου η ιδιωτικότητα της ζωής μας αντιμετωπίζεται ως συνώνυμη της συνωμοτικότητας!!

"Έρχεται η στιγμή που η ιδιωτικότητα θα λογίζεται ως πράξη τρομοκρατική";

Ο συνθέτης Δ. Παπαδημητρίου σε πρόσφατη συνέντευξή του (24/7, 16/12/2022), δίνει μια μοναδικής διαύγειας περιγραφή για τη χαμένη ιδιωτικότητα του σύγχρονου ανθρώπου.

…. " Πλησιάζει η στιγμή - αν δεν ήρθε ήδη μεταμφιεσμένη- που η ανωνυμία του πολίτη θα είναι παράνομη και μέγιστο έγκλημα και η ιδιωτικότητα της ζωής του θα θεωρείται συνώνυμη της συνωμοτικότητας, δηλ. θα λογίζεται από το κράτος αλλά και τους άλλους ανθρώπους ως πράξη τρομοκρατική. Οι σύγχρονοι άνθρωποι διψώντας για οιαδήποτε ψευδο- επωνυμία, για οιοδήποτε κέρδος και πάντα με άλλοθι την "ασφάλεια" θα εκχωρήσουν χωρίς δισταγμό στο κράτος κάθε δικαίωμα ιδιωτικότητας και κάθε ατομική ελευθερία σκέψης.

Στο μέλλον ελεύθεροι, αν και παράνομοι, θα είναι οι ανώνυμοι που θα μπορούν να ζουν απαρατήρητοι στο πλαίσιο μιας ιδιωτικότητας ύποπτης και ανεπίτρεπτης. Όποιος τολμάει να δηλώνει πως σκέφτεται διαφορετικά, απλά θα εξορίζεται, θα τιμωρείται. Οι αποφάσεις θα είναι δια βοής σε τεράστια λαϊκά ψηφιακά δικαστήρια δίχως νόμους. "

Και όμως τι κρίμα. Γιατί όπως λένε οι επιστήμονες «το πραγματικό ενδιαφέρον των ατόμων δεν είναι να αποκρύψουν τα προσωπικά δεδομένα τους, αλλά να έχουν τον έλεγχό τους, και αυτό αποτελεί βασικό στοιχείο της ανθρώπινης ελευθερίας» (Μ. Καρύδα, καθηγήτρια Παν. Αιγαίου, ΚΑΘΗΜΕΡΙΝΗ, 4/12/2022).

Ή όπως έλεγε και το γνωστό τραγούδι των Zig Zag πριν πολλά χρόνια «Ήρεμα ήρεμα δεν είμαι τρομοκράτης…….. είμαι το θύμα μιας αγάπης».

Προς μια βίαιη «κινεζοποίηση» της ψηφιακής ζωής

Μέσα σε αυτό το περιβάλλον είναι παρήγορο να βλέπουμε εφήβους να απομακρύνονται από την τοξική και απογυμνωτική επίδραση του κινητού. Για παράδειγμα το Luddite Club στη Ν. Υόρκη (Business Insider, *"Why teens are giving up their smartphones"*, 24/10/2022) όπου τα μέλη του, έφηβοι, κλείνουν smartphones και κινητά με πλήκτρα - τα τελευταία ως γνωστόν έχουν επιστρέψει και είναι πολύ cool σε πολλές χώρες (ιδιαίτερα με βγαλμένη μπαταρία) – και δημιουργούν ποιοτικό χρόνο και δραστηριότητες, μεταφέροντας το μήνυμα ότι η απεξάρτηση από το κινητό είναι δυνατή και ότι πρέπει να αντιστεκόμαστε σε όσους βάζουν τα χρήματα πάνω από την ιδιωτικότητα, την ελευθερία και αυτονομία του ανθρώπου, και από τις ηθικές και δημοκρατικές αξίες μας.

Και το κίνημα απελευθέρωσης από το κινητό δυναμώνει παντού: και στην Ελλάδα δυναμώνουν πλέον οι φωνές εναντίον της επιχειρούμενης υποχρεωτικής επιβολής του κινητού τηλεφώνου στους πολίτες, οι οποίοι αναρωτιούνται σε ποιο άρθρο του Συντάγματος αναφέρεται ότι για να εξυπηρετηθείς από τις κρατικές υπηρεσίες ή άλλες ιδιωτικές εταιρείες ιδιοκτησίας ξένων funds (ΟΤΕ, ΔΕΗ , Τράπεζες, κλπ) ή να υποβάλεις

φορολογική δήλωση ή να εξυπηρετηθείς από το taxisnet επιβάλλεται να έχεις κινητό τηλέφωνο? Μια βίαιη ¨κινεζοποίηση¨ πραγματοποιείται με αυτή τη ψηφιακή επιτήρηση στη χώρα, κάτω από τον μανδύα του ψηφιακού εκσυγχρονισμού, σε ένα κράτος που ούτε για τα cookies δεν μπορεί να επιβάλει το νόμο, δηλ. να έχουν τρείς επιλογές όπως ορίζει ο νόμος στην ΕΕ!! Στη μοναδική χώρα στη Ευρώπη που εισέρχεσαι ψηφιακά στις κρατικές υπηρεσίες για να εξυπηρετηθείς, μέσω τραπεζών, δηλαδή ιδιωτικών εταιρειών που επιπλέον καμία πια δεν είναι Ελληνική, παρά τα τεράστια ποσά που έδωσαν οι φορολογούμενοι για τη «σωτηρία» τους !! (κάποιοι υπολογισμοί μιλούν για συνολικά 183 δις ευρώ ή το 85% του ΑΕΠ το 2011, ενώ το 61% του δημοσίου χρέους δημιουργήθηκε για να σωθούν οι τράπεζες..)

Μέσα σε αυτό το γκρίζο τοπίο , φαντάζουν σοφά τα λόγια του κου Χ.Ράμμου του Συμβουλίου Επικρατείας, Προέδρου της ΑΔΑΕ (Αρχή Διασφάλισης Απορρήτου Επικοινωνιών), που μνημονεύει με αφορμή το σχετικό σκάνδαλο των υποκλοπών από το γνωστό βιβλίο (S.Levitsky & D.Ziblatt : *“How Democracies Die”,* 2018) «στις μέρες μας οι δημοκρατίες δεν απειλούνται τόσο από τα τανκς, όσο από την ατροφία των θεσμών τους, την παραίτηση από την υπεράσπιση τους και από το μαρασμό τους…. και όλα αυτά σταδιακά και υποδόρια, ώστε να μην τα συνειδητοποιήσουμε παρά μόνο όταν είναι πολύ αργά». !!

Τώρα λοιπόν γνωρίζεις. Η δημοκρατία σε χρειάζεται.

(ΣΗΜ. Ο γράφων δεν έχει καμία οικονομική ή άλλη σχέση, με τις εταιρείες/προϊόντα που αναφέρονται στο άρθρο για καθαρά ερευνητικούς σκοπούς.)