



«Φακέλωμα του πολίτη»

οι νέες ηλεκτρονικές ταυτότητες



Αντί προλόγου

Οι νέες ηλεκτρονικές ταυτότητες αποτέλεσαν προτεραιότητα της Νέας Δημοκρατίας μετά τις εκλογές του Ιουνίου 2023 ήδη από τις προγραμματικές δηλώσεις. Η μακρά προϊστορία του θέματος περιλαμβάνει την «Κάρτα του Πολίτη» που θα αποτύπωνε «δικαιώματα στην σύνταξη, στην εκπαίδευση, στο επίδομα αναπηρίας και στο βιβλιário υγείας», όπως εξαγγέλθηκε από τον Γ. Παπανδρέου στη ΔΕΘ το 2010, και αργότερα από τον Αλ. Τσίπρα σε κομματικό συνέδριο το 2013. Το 2018 η κυβέρνηση ΣΥΡΙΖΑ εξέδωσε σχετική ΚΥΑ (ΦΕΚ Β΄ 1476/27-04-2018) για την «Έκδοση νέου τύπου Δελτίου Ταυτότητας Ελλήνων πολιτών», όπου ρητά αναφέρεται ότι στη νέα ταυτότητα θα ενσωματωθεί ανέπαφο chip RFID, στο οποίο θα αποθηκεύονται «τα στοιχεία που απαιτούνται για τις Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης» και μέσω της τελευταίας και με εφαρμογές του ιδιωτικού τομέα. Συμπεραίνει κανείς ότι το νέο δελτίο ταυτότητας δεν είναι απλό μέσον ταυτοποίησης, αλλά και μέσο άσκησης εκείνων των (δημοσίων και ιδιωτικών) δικαιωμάτων που έχουν υπαχθεί και θα υπαχθούν στην Ηλεκτρονική Διακυβέρνηση. Δηλαδή όλων.

Η εμμονή για ηλεκτρονικές ταυτότητες επομένως δεν έχει φραγμούς ανάμεσα στα κόμματα εξουσίας και συνεχίστηκε αδιάκοπα μέχρι την σημερινή κυβέρνηση. Όλοι όσοι ανέχθηκαν ή υποστήριξαν την εκχώρηση εθνικής κυριαρχίας και την κατάργηση των ελευθεριών μας, υπογράφοντας

μνημόνια, ξεπουλώντας τη Μακεδονία ή επιβάλλοντας παράλογες υποχρεωτικότητες, σήμερα συμφωνούν και για τις νέες ηλεκτρονικές ταυτότητες και την επιβολή τους. Ειδικά αυτή η κυβέρνηση, ως αδιαμφισβήτητη πρωταθλήτρια στην στέρηση ατομικών ελευθεριών, στις υποκλοπές και στην υποχρεωτικότητα, θέλει να μείνει στην ιστορία επιβάλλοντας ό,τι οι προηγούμενοι δεν κατάφεραν.

Μακρύ παρελθόν έχει όμως και ο αγώνας για το απόρρητο του δημόσιου και ιδιωτικού βίου. Το πιστοποιητικό πολιτικών φρονημάτων καταργήθηκε επισήμως το 1981, αν και μόλις το 1989 περισσότερα από 17 εκατομμύρια έγγραφα «φακελώματος» πολιτών ρίχθηκαν τελικώς στην πυρά. Αργότερα, με προμετωπίδα την «προστασία των προσωπικών δεδομένων», από τις αστυνομικές ταυτότητες αφαιρέθηκε το δακτυλικό αποτύπωμα, και με διχαστικό τρόπο επιβλήθηκε και η αφαίρεση του θρησκευματος. Και ερχόμαστε στο σημερινό παράλογο – να διαφημίζεται πανηγυρικά μία νέα ταυτότητα, η οποία θα είναι τεχνολογικά ικανή να προσφέρει σε αγνώστους το σύνολο σχεδόν των προσωπικών μας δεδομένων!

Οι δημοσιευμένες τεχνικές προδιαγραφές των νέων ηλεκτρονικών ταυτοτήτων (βλ. ΚΥΑ 40693-13/04/2018, 8200/0-109568/2023) στην καλύτερη περίπτωση αποτελούν το εξώφυλλο ενός τουλάχιστον 100σελίδου κειμένου, το οποίο όμως παραμένει άγνωστο με την αιτιολογία της

εμπιστευτικότητας. Ενδεχομένως μάλιστα οι τελικές τεχνικές προδιαγραφές να απέχουν από τις αρχικές, καθώς ακυρώθηκαν προηγούμενοι διαγωνισμοί και πιθανώς υπήρξε απ' ευθείας ανάθεση σε ιδιώτες. Οι τελευταίες κυβερνητικές δηλώσεις (κατά την στιγμή εκτύπωσης του παρόντος) επιβεβαιώνουν ότι οι νέες ταυτότητες «θα έχουν το ίδιο chip με αυτό των πιστωτικών καρτών» (οι οποίες όμως έχουν NFC chip ενώ οι προαναφερθείσες ΚΥΑ αναφέρουν RFID chip), ωστόσο η ύπαρξη chip είναι βέβαιη. Αυτό σημαίνει ότι θα μπορεί η νέα ταυτότητα να περιέχει και να εγγράφει στοιχεία που δεν γνωρίζει ο κάτοχός της.

Η δικαιολογημένη ανησυχία τεράστιας μερίδας συμπολιτών μας για τις επιπτώσεις της νέας ηλεκτρονικής ταυτότητας στις ατομικές μας ελευθερίες, οδήγησε αρκετούς να σπεύσουν στα αστυνομικά τμήματα να ανανεώσουν τις απερχόμενες (χάρτινες) ταυτότητες, για να εξασφαλίσουν έστω μία προσωρινή ισχύ ολίγων ετών. Δυστυχώς, δέχθηκαν ταλαιπωρία, εμπαιγμό και ειρωνείες από την κυβέρνηση και τους φίλους της.

Όμως μία κυβέρνηση οφείλει να αγαπά, να ακούει και να σέβεται τον λαό, αντί να τον διχάζει, να του στερεί ελευθερίες ή να του επιβάλλει αδικαιολόγητα μέτρα.

Η ΝΙΚΗ, πάντοτε στο πλευρό του ελληνικού λαού, στάθηκε η μόνη κοινοβουλευτική φωνή που υψώθηκε αμέσως εναντίον των ηλεκτρονικών ταυτοτήτων. Αντιλαμβάνεται τον εφιαλτικό μεσαίωνα που θα φέρει ένα τέτοιο μέτρο, όπου μέσω της τεχνολογίας το κράτος θα κυνηγά τους

ίδιους τους πολίτες του. Θα μπορεί να τους φακελώνει, να τους παρακολουθεί και σύντομα να τους αξιολογεί επί καθημερινής βάσης, όπως γίνεται ήδη σήμερα στην Κίνα.

Η κυβέρνηση αναδεικνύεται σε πρωτεργάτη του φακελώματος, με πρόσχημα την «πρόοδο», την «εξυπηρέτηση» και την δήθεν «πάταξη της φοροδιαφυγής». Ως συνοπτική απάντηση, η ΝΙΚΗ προτείνει στην κυβέρνηση να διασφαλίσει λίγο πιο απλά πράγματα, όπως ότι τα τραίνα δεν κινούνται ανάποδα και οι περιουσίες των συμπολιτών μας δεν καίγονται ούτε πλημμυρίζουν απροστάτευτες. Όσο για την πάταξη της φοροδιαφυγής, ας ξεκινήσει ελέγχοντας τους «ισχυρούς» των λιστών Λαγκάρντ.

Σε ό,τι αφορά στον απλό πολίτη, σε αυτό το φυλλάδιο τον ενημερώνουμε για το τι ισχύει και τι όχι, ώστε καθένας να μπορεί να αποφασίζει για τον εαυτό του χωρίς ψυχαναγκασμούς και ψευτοδιλήμματα.



Χρειαζόμαστε νέες ταυτότητες και γιατί;

Η απάντηση είναι ΝΑΙ αλλά όχι υποχρεωτικά ηλεκτρονικές. Οι σημερινές ταυτότητες δεν παρέχουν ισχυρή ασφάλεια και μπορούν εύκολα να πλαστογραφηθούν. Αυτή είναι η «αχίλλειος πτέρνα» της σημερινής ταυτότητας και έχουμε δεχτεί σχετικά παράπονα από την Ε.Ε. και άλλες χώρες.



Σαφώς χρειαζόμαστε νέες ταυτότητες ενισχυμένης ασφάλειας που να μην πλαστογραφούνται. Δεν υπάρχει όμως μοναδική τεχνολογική λύση. Κάθε εναλλακτική έχει διαφορετικό αντίκτυπο τόσο σε δαπάνες όσο και σε κίνδυνο απεμπόλησης ατομικών ελευθεριών.

Μας υποχρεώνει η Ευρωπαϊκή Ένωση σε ηλεκτρονικές ταυτότητες;

Η απάντηση είναι ΟΧΙ. Η Κυβέρνηση αφήνει να εννοηθεί, εσφαλμένα, ότι η έκδοση των νέων ηλεκτρονικών ταυτοτήτων δήθεν επιβάλλεται υποχρεωτικά από τη νομοθε-

σία της Ευρωπαϊκής Ένωσης, και ότι το αργότερο έως τον Αύγουστο 2026 πρέπει να αντικατασταθούν οι υπάρχουσες με νέες ηλεκτρονικές ταυτότητες. Αυτός ο κυβερνητικός ισχυρισμός όμως δεν ανταποκρίνεται στην πραγματικότητα.

Σύμφωνα με τον σχετικό Κανονισμό (ΕΕ) 2019/1157 του Ευρωπαϊκού Κοινοβουλίου για την ενίσχυση της ασφάλειας των δελτίων ταυτότητας και των εγγράφων διαμονής των πολιτών της Ένωσης:

- δεν υποχρεούνται τα κράτη-μέλη να εκδίδουν δελτία ταυτότητας, αλλά θα εξακολουθεί να είναι στη διακριτική ευχέρεια κάθε κράτους αν θα έχει δελτία ταυτότητας υποχρεωτικά, προαιρετικά ή καθόλου.
- δεν εμποδίζονται τα κράτη-μέλη «να αποδέχονται, με τρόπο που δεν εισάγει διακρίσεις, έγγραφα διαφορετικά από τα ταξιδιωτικά έγγραφα, για λόγους ταυτοποίησης, όπως άδειες οδήγησης». Δηλαδή, ακόμη και αν το κράτος αποφασίσει να εκδώσει ταυτότητα, αυτή δεν είναι απαραίτητο να είναι ηλεκτρονικού τύπου.

Ωστόσο, αν τα κράτη-μέλη αποφασίσουν να εκδώσουν ηλεκτρονικού τύπου ταυτότητες, τότε οι νέες αυτές ηλεκτρονικές ταυτότητες θα πρέπει να συμμορφώνονται με τα αντίστοιχα νέα πρότυπα ασφάλειας. Τα κράτη-μέλη ωστόσο μπορούν να διατηρήσουν τα εθνικά χαρακτηριστικά σχεδιασμού και τις υπηρεσίες ηλεκτρονικής διακυβέρνησης.

Τί συμβαίνει σε άλλες χώρες;

Υπάρχουν πράγματι πολλές χώρες όχι μόνο της Ευρωπαϊκής Ένωσης αλλά και ευρύτερα του δυτικού κόσμου, οι οποίες είτε δεν έχουν υποχρεωτική ταυτότητα είτε αρνήθηκαν την εφαρμογή της ψηφιακής ταυτότητας: Γαλλία, Ολλανδία, Φινλανδία, Νορβηγία, Αυστρία, Ιταλία, Ισλανδία, Δανία, ακόμη και η Αυστραλία.

Στην Ελβετία, σε πρόσφατο δημοψήφισμα του 2021, η συντριπτική πλειοψηφία του λαού (65%) καταψήφισε την υιοθέτηση του «Ομοσπονδιακού νόμου για τις υπηρεσίες ηλεκτρονικής ταυτοποίησης» από την κυβέρνηση. Απέρριψε δηλαδή ο λαός της Ελβετίας την εισαγωγή στο αποθηκευτικό μέσο της ταυτότητας των κωδικών της Ηλεκτρονικής Διακυβέρνησης, με άλλα λόγια δεν δέχθηκε να γίνει η ταυτότητα και Κάρτα Ασκήσεως Δικαιωμάτων.

Στο Ηνωμένο Βασίλειο, όταν ακόμη ήταν στην Ε.Ε., η κυβέρνηση απέρριψε το σχετικό νομοσχέδιο περί ηλεκτρονικών ταυτοτήτων ήδη από το 2011. Σημειωτέον ότι η Βρετανία ουδόλως υιοθετεί τον θεσμό των ταυτοτήτων. Οι πολίτες της Μεγάλης Βρετανίας, με αρχική συλλογή μόλις 10.000 υπογραφών, κατάφεραν να πετύχουν με πολιτικό αγώνα την ακύρωση εφαρμογής των ηλεκτρονικών ταυτοτήτων στη χώρα τους, εστιάζοντας στον κίνδυνο φαλκίδευσης των ατομικών ελευθεριών τους. Χαρακτηριστικά, οι Βρετανοί διαμαρτυρήθηκαν με επικεφαλής έναν λόρδο ευγενή και με προμετωπίδα το σύνθημα «να μη γί-

νουν το σφραγισμένο μωσχάρι ενός παγκόσμιου σταύλου». Η νίκη-σταθμός του Βρετανικού λαού είναι σημείο παρήγορο και για την Ελλάδα, δίνοντάς μας το μήνυμα ότι, με συντονισμένη δράση και θάρρος, είναι δυνατή η αποτροπή υλοποίησης των νέων ηλεκτρονικών ταυτοτήτων-φακέλων-καταδοτών. Αν και πρόσφατα, οι Εργατικοί επανέφεραν ζήτημα ηλεκτρονικής ταυτότητας, έλαβαν τον Φεβρουάριο 2023 ρητή απόρριψη εκ μέρους του Βρετανού πρωθυπουργού.

Όπως διαπιστώνουμε, οι ανησυχίες περί ατομικών ελευθεριών και δημοκρατίας απασχολούν και προβληματίζουν πολλές προηγμένες χώρες και τους λαούς τους. Θλιβερή η σύγκριση των ηγετών τους με τους εγχώριους «δημοκράτες» ηγέτες μας, που αντί να σέβονται τις ανησυχίες του λαού, τον διχάζουν και τολμούν να τον αποκαλούν «ψεκασμένο». Φέρουμε μεγάλη ευθύνη για το μέλλον της δημοκρατίας και την ελευθερία των παιδιών μας.



Χρειαζόμαστε chip στην ταυτότητα για να είναι επαρκώς ασφαλής;

Η απάντηση είναι ΟΧΙ.

Για να διασφαλιστεί το αδύνατο και απρόσφορο παραχάραξης, αρκεί να ακολουθήσει κανείς τις οπτικές μεθόδους σχεδιασμού και εκτύπωσης που ορίζει το έγγραφο 9303 του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας (ICAO) για τα μηχανικώς αναγνώσιμα ταξιδιωτικά έγγραφα. Αυτές οι προδιαγραφές βρίσκουν ήδη σήμερα εφαρμογή στο δίπλωμα οδήγησης, στα νέα χαρτονομίσματα ευρώ κλπ. Άρα σε τι εξυπηρετεί το chip;

Είναι χρήσιμο:

(α) για την αμεσότερη ταυτοποίησή μας συγκριτικά με τα λίγα παραπάνω δευτερόλεπτα ώστε αυτός που σε ελέγχει να δει την ταυτότητα και να σε κοιτάξει στα μάτια και

(β) για την αυτόματη **ενεργοποίηση της ηλεκτρονικής διακυβέρνησης και τη δυνατότητα να περιέχονται και να εγγράφονται στοιχεία που δεν γνωρίζει ο κάτοχος της ταυτότητας.**

Τί σημαίνει ηλεκτρονική διακυβέρνηση ενεργοποιούμενη στη νέα ταυτότητα;

Η απάντηση είναι ότι η ταυτότητα μετατρέπεται σε «φακέλωμα του πολίτη».

Το κράτος σήμερα έχει ανεξάρτητες βάσεις δεδομένων, ώστε να τηρείται μία βασική αρχή προστασίας προσωπικών δεδομένων, η οποία με απλά λόγια λέει ότι «δεν κρατώ περισσότερες πληροφορίες για σένα, από όσες μου είναι απολύτως απαραίτητες για να σε εξυπηρετήσω / για να ολοκληρώσουμε την *δοσοληψία* μας». Αυτό σημαίνει ότι το Υπουργείο Υγείας γνωρίζει τον φάκελο της υγείας μου και όχι τα περιουσιακά μου στοιχεία ή το ποινικό μου μητρώο. Αντίστοιχα, το Υπουργείο Οικονομικών γνωρίζει τη φορολογική μου ενημερότητα και όχι τα ιατρικά δεδομένα μου.

Όταν όμως αυτές οι ανεξάρτητες βάσεις δεδομένων διασυνδέονται, έχουμε πρακτικά λειτουργία συγκοινωνούντων δοχείων. Και τότε, γίνεται θέμα απλής άδειας πρόσβασης αν θα μπορεί ο λογιστής μου να γνωρίζει αν έχω σάκχαρο, ο ασφαλιστής μου αν έχω χρήματα, ο υποψήφιος εργοδότης μου αν έχω σκλήρυνση κατά πλάκας, και ο σερβιτόρος αν έχω προβεί σε ιατρικές πράξεις – το τελευταίο εξάλλου ήδη το βιώσαμε όλοι μας ως πρόβα, την εποχή του εγκλεισμού με το COVID PASS.

Ενεργοποιώντας την ηλεκτρονική διακυβέρνηση, η

ταυτότητα μετατρέπεται από μέσον απλής ταυτοποίησης, σε δικαίωμα (ή στέρηση) πρόσβασης σε υπηρεσίες και αγαθά. Χαρακτηριστικά τα λόγια του Ολλανδού βουλευτή F.Jansen: “Μπορούν να σας ακυρώσουν την άδεια οδήγησης επειδή οδηγείτε ένα μη φιλικό προς το περιβάλλον αυτοκίνητο. Με το πάτημα ενός κουμπιού, μπορούν να σας στερήσουν πρόσβαση σε κοινωνικά δίκτυα, να μην σας επιτρέψουν πρόσβαση σε δημόσιες ή ιδιωτικές υπηρεσίες.” Με απλά λόγια, οι διασυνδεδεμένες βάσεις δεδομένων παραβιάζουν την παραπάνω αρχή προστασίας προσωπικών δεδομένων και καταργούν την ιδιωτικότητα.

Δημιουργούνται έτσι προϋποθέσεις για διχασμό της κοινωνίας σε πολίτες με προνομιακή πρόσβαση και πολίτες με αποκλεισμό. Η ελληνική κυβέρνηση ήδη επιβραβεύει διαφορετικά τους δικαιούχους του “market pass” που το λαμβάνουν με την ειδική ψηφιακή χρεωστική κάρτα, μειώνοντας την παροχή σε όσους θέλουν κατάθεση στον τραπεζικό λογαριασμό τους, σαν με κάποιον μαγικό τρόπο αυτοί να έχουν λιγότερη ανάγκη από το βοήθημα. **Με τον τρόπο αυτόν καταλύεται η δημοκρατία και η ισότητα των πολιτών.**

Το επόμενο στάδιο ηλεκτρονικής διακυβέρνησης είναι όλα τα παραπάνω δεδομένα να μην είναι απλώς διασυνδεδεμένα στις επιμέρους βάσεις τους, αλλά να ενοποιηθούν σε μία ενιαία βάση δεδομένων, με αντιστοιχισμός κάθε προσώπου σε έναν μοναδικό και αναλλοίωτο ενιαίο αριθμό που συνοδεύει το πρόσωπο από γεννήσεως έως θανάτου.

Έναν αριθμό που θα συνδέεται με την ταυτότητα, τον ΑΦΜ, τους κωδικούς taxisnet, τον ΑΜΚΑ, τον αριθμό δημοτολογίου, το διαβατήριό, τον τραπεζικό λογαριασμό. Η ελληνική κυβέρνηση μέχρι σήμερα αρνείται να επιβεβαιώσει ή να διαψεύσει αν οι νέες ηλεκτρονικές ταυτότητες περιέχουν τέτοιο ενιαίο κωδικό.

Χάριν μιας ψευδαίσθησης από ασφάλεια και άνεση, καταργείται η ελευθερία του προσώπου. Στο κυνήγι αυτής της άνεσης που υποσκάπτει αργά την ελευθερία, κάποιοι σύντομα ίσως πιστέψουν ότι είναι ελάχιστη η διαφορά μεταξύ ενός microchip ανέπαφης δυνατότητας σύνδεσης, ενσωματωμένου στην πλαστική κάρτα-ταυτότητα, και ενός αντίστοιχου εμφυτευμένου στο σώμα.



Η ταυτότητα μας βάζει σε αυτόν τον εφιαλτικό κόσμο του απόλυτου ελέγχου και είναι η αρχή για εμφυτεύματα (ας μην ξεχνάμε το εμφύτευμα «COVID PASS» που διέθεσε στην Σουηδία η εταιρία Epicenter στο αντίτιμο των 100 ευρώ - παρόμοιο τσιπάκι με αυτό των ταυτοτήτων) και τις μετεξελίξεις σε Homo Deus (βλ. σελ. 13).

Πέντε σημεία συνοψίζουν την εναντίωση της ΝΙΚΗΣ στις νέες ηλεκτρονικές ταυτότητες

- 1. Η ΑΝΤΙΔΗΜΟΚΡΑΤΙΚΗ ΕΛΛΕΙΨΗ ΔΙΑΦΑΝΕΙΑΣ.** Τα δεδομένα που θα περιέχει και θα είναι δυνατόν να εγγραφούν στη νέα ταυτότητα, είναι άγνωστα στον κάτοχό της. Επίσης άγνωστο παραμένει το ποιός, στην Ελλάδα ή στο εξωτερικό, εκτός από την Ελληνική Αστυνομία, θα έχει πρόσβαση να δει ή να εγγράψει στοιχεία σε αυτήν. Η κυβέρνηση μάς καθησυχάζει για τα πάντα, χωρίς να απαντά ουσιωδώς, τηρώντας έτσι αδιαφανή και κρυψίνου στάση.
- 2. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΦΑΚΕΛΩΜΑ.** Η παρακολούθηση του πολίτη με τα ηλεκτρονικά ίχνη συναλλαγής, οι διασυνδεδεμένες βάσεις δεδομένων, η μετατροπή ενός απλού μέσου ταυτοποίησης σε δικαίωμα πρόσβασης σε υπηρεσίες και αγαθά, συνιστούν στυγνή καταπάτηση των ανθρωπίνων δικαιωμάτων του απορρήτου και της ιδιωτικότητας της δημόσιας και προσωπικής ζωής.
- 3. Η ΕΛΛΕΙΨΗ ΑΣΦΑΛΕΙΑΣ.** Ο ορατός κίνδυνος διαρροής δεδομένων και κυβερνοεπιθέσεων στα προσωπικά ψηφιακά μας δεδομένα, αφού η κάρτα δεν είναι ασφαλής. «Σου κλέβω την κάρτα» σημαίνει «σου κλέβω τα πάντα».
- 4. Η ΔΙΑΚΙΝΔΥΝΕΥΣΗ ΕΘΝΙΚΗΣ ΚΥΡΙΑΡΧΙΑΣ,** καθώς είναι άγνωστο, εάν τα δεδομένα των Ελλήνων πολιτών θα βρίσκονται αποθηκευμένα αποκλειστικά εντός της ελληνικής επικράτειας και ο έλεγχος στα συστήματα αποθήκευσης και διαχείρισης των δεδομένων θα γίνεται από ιδιώτες ή από το ίδιο το ελληνικό κράτος.
- 5. Η ΚΑΤΑΡΓΗΣΗ ΤΗΣ ΕΛΕΥΘΕΡΙΑΣ ΤΟΥ ΠΡΟΣΩΠΟΥ** και η συνακόλουθη προσβολή του χριστιανικού φρονήματος. Εχουν μιλήσει για τους κινδύνους αυτούς τόσο η Ιεραρχία (9.3.1993 και 17.11.2010) όσο και σύγχρονοι Άγιοι, των οποίων είναι απόλυτα σκόπιμο να χρησιμοποιήσουμε τις αυτούσιες εκφράσεις, ώστε ο καθένας να βγάλει τα συμπεράσματά του χωρίς παρωπίδες ή διαστρεβλώσεις.

Η Νέα Δημοκρατία εξακολουθεί να διχάζει τον λαό, εμείς θέλουμε να ενώνουμε τον λαό και να του παρέχουμε την ελευθερία να αποφασίζει μέσω της σωστής και αντικειμενικής ενημέρωσης.

Εχουμε κάτι να κρύψουμε;

Η απάντηση είναι ΝΑΙ, χωρίς η απόκρυψη να πρέπει να σχετίζεται με κάτι παράνομο ή ανήθικο. Απλούστατα, η ιδιωτική μας ζωή αξίζει σεβασμού από όλους. «Τὰ ἐν οἴκῳ μὴ ἐν δήμῳ».

Καλλιεργείται εντέχνως στον λαό από κυβερνητικά στελέχη η ιδέα του «τι με νοιάζει εμένα, εγώ δεν έχω τίποτα να κρύψω». Αυτό περίπου το επιχείρημα παραθέτουν, λέγοντας ότι εξίσου δεν ανησυχούμε, αφού τα έξυπνα κινητά είτε η χρήση των υπηρεσιών της Google ήδη μας εντοπίζουν και μαθαίνουν προσωπικά μας δεδομένα.

Όμως, τα έξυπνα κινητά και οι υπηρεσίες της Google ανήκουν σε ιδιωτικές επιχειρήσεις. Προαιρετικά τους παραχωρούμε προσωπικά μας δεδομένα ή πληροφορίες τοποθεσίας, προκειμένου να χρησιμοποιήσουμε ιδιωτικές τους υπηρεσίες. Περαιτέρω, έχουμε δικαίωμα ανά πάσα στιγμή να απενεργοποιήσουμε την παροχή πληροφοριών, να δούμε και να διαγράψουμε τα αποθηκευμένα δεδομένα, να πούμε «ως εδώ». Η αστυνομική όμως ταυτότητα είναι ένα υποχρεωτικό έγγραφο που αφορά στο ελληνικό κράτος και δεν επιλέγουμε την χρήση της. Δυστυχώς, κάποιοι μπερδεύουν το κράτος μας με επιχείρηση.

Στο θέμα του γεωεντοπισμού, η καταγραφή του τόπου τελευταίας χρήσης της κάρτας πολίτη, ήδη δημιουργεί

δεδομένα ιχνηλασιμότητας (τάδε ημερομηνία στο δείνα μέρος κλπ). Περαιτέρω, η μετάβαση από ηλεκτρονική σε ψηφιακή ταυτότητα (δηλαδή ενσωματωμένη ως εφαρμογή στο κινητό μας τηλέφωνο) αυτόματα επιτρέπει τον γεωεντοπισμό με την κλασική του έννοια, αξιοποιώντας την δυνατότητα του κινητού μας.

Το ερώτημα «εάν έχουμε να κρύψουμε κάτι» κρύβει πονηρία. Το πραγματικό ερώτημα είναι «εάν η κυβέρνηση δικαιούται να γνωρίζει περισσότερα από όσα χρειάζεται, ώστε να διακονεί σωστά τον λαό που την εκλέγει». Και η απάντηση είναι ΟΧΙ - δεν έχει η κυβέρνηση τέτοιο δικαίωμα.

Εύστοχα έχει ειπωθεί πως «όσοι θυσιάζουν στοιχειώδεις ελευθερίες για λίγη ασφάλεια, δεν αξίζουν ούτε ελευθερία ούτε ασφάλεια». Θα συμπληρώσουμε ότι σήμερα δυστυχώς θυσιάζεται η ελευθερία ακόμη και για άνεση.



Διασφαλίζεται η εθνική ασφάλεια και κυριαρχία με τις νέες ταυτότητες;

Απάντηση: ΟΧΙ, δεν διασφαλίζεται.

Κατ' αρχήν, δεν έχουμε πληροφόρηση αν τα προσωπικά μας δεδομένα θα αποθηκεύονται σε βάσεις δεδομένων μόνο εντός της ελληνικής επικράτειας και μόνο στο Αρχηγείο της Ελληνικής Αστυνομίας όπως προβλέπει το άρθρο 10 της ΚΥΑ. Μία δεύτερη όμως δεξαμενή δεδομένων θα προκύψει από την «ηλεκτρονική διακυβέρνηση» –δηλαδή τη χρήση της ταυτότητας ως «κάρτας πολίτη» για την άσκηση των δικαιωμάτων μας– είναι άγνωστο πού θα τηρείται, καθώς είναι γνωστό ότι όλες οι ηλεκτρονικές εθνικές δεξαμενές πληροφοριών διασυνδέονται με υπερεθνικά (ευρωπαϊκά και μη) ηλεκτρονικά αρχεία. Κάλλιστα τα δεδομένα των Ελλήνων πολιτών μπορεί να αποθηκεύονται και εκτός χώρας, ώστε να ανακτηθούν από εκεί εάν υπάρξει ακραία φυσική εγχώρια καταστροφή. Η νυν κυβέρνηση οφείλει να ενημερώσει υπεύθυνα εάν κάτι τέτοιο ισχύει και σε ποιές χώρες υπάρχουν servers με δεδομένα Ελλήνων πολιτών. Εμείς πάντως δεν θα αφήναμε το πορτοφόλι μας στον γείτονα να το φυλάξει.

Περαιτέρω, η διαχείριση των βάσεων δεδομένων και των εργαλείων πληροφορικής διενεργείται από ιδιωτικές ανάδοχες εταιρείες ενώ θα έπρεπε να γίνεται μόνο από το κράτος. Η εκάστοτε ανάδοχη εταιρεία συνήθως κρατά για

τον εαυτό της το μέγιστο επίπεδο πρόσβασης στα συστήματα, αφήνοντας τα μεσαία και χαμηλότερα επίπεδα πρόσβασης για τις κυβερνητικές υπηρεσίες και τον απλό πολίτη αντίστοιχα.

Τι συμβαίνει με τα προσωπικά δεδομένα μας;

Απάντηση: Δεν μας ανήκουν.

Ανήκουν στην κυβέρνηση ή σε ιδιώτες, ανάλογα με τις δραστηριότητές μας στο διαδίκτυο και τον τρόπο με τον οποίο η κάρτα θα επικοινωνεί με τον έξω κόσμο. Ανάμεσα στους ιδιώτες, υπάρχουν και οι λεγόμενοι Μεσίτες Δεδομένων (Data Brokers) οι οποίοι συλλέγουν τεράστιο όγκο πληροφοριών για εκατοντάδες εκατομμύρια καταναλωτές, και παρέχουν πληροφορίες σχετικά με τη συμπεριφορά των καταναλωτών για να προσαρμόσουν την προβολή προϊόντων από εμπόρους. Λόγω της μεγάλης αξίας που δίνει σήμερα η παγκόσμια κοινότητα στα ψηφιακά δεδομένα, πολλοί τα αποκαλούν ως Νέο Χρυσό.

Στην θεωρία, τα δεδομένα των πολιτών είναι στην διάθεση μόνο του Κράτους ή της αρμόδιας Υπηρεσίας. Στην πράξη, φυσικά, όταν τα ψηφιακά δεδομένα γίνονται αντικείμενο πλουτισμού, μεγαλώνει και ο πειρασμός. Αρκετοί θυμούνται τον αλλοδαπό που πωλούσε προ ετών στην Ομόνοια τα αρχεία όλων των Ελλήνων φορολογουμένων (από το TAXISNET) σε ένα CD στο αντίτιμο των 60 Ευρώ.

Η ηλεκτρονική ταυτότητα «χακάρεται»; Είναι τα δεδομένα μας ασφαλή;

Απάντηση : ΝΑΙ «χακάρεται» - ΟΧΙ δεν είναι ασφαλή τα δεδομένα μας.

Να διαχωρίσουμε εδώ 2 διαφορετικά είδη κινδύνων:

α) Επίθεση στην ίδια την κάρτα: αντιγραφή, αλλοίωση δεδομένων – ιδιαίτερα αν η νέα ηλεκτρονική ταυτότητα είναι, ή σχεδιάζεται να γίνει, επανεγγράψιμη. Οσον αφορά στην πρώτη κατηγορία, ο κίνδυνος είναι να σου υποκλέψουν τα στοιχεία σου και να υποδύονται ότι είσαι εσύ, αυτό τους δίνει άμεση πρόσβαση σε όλες τις βάσεις δεδομένων με τις οποίες μπορείς να διασυνδεθείς: Ασφαλιστικά σου ταμεία, εφορία, κτηματολόγια, και ... σύντομα και τράπεζα. Δύσκολο για τον ευκαιριακό «χάκερ», εύκολο για τον επιστήμονα-επαγγελματία «χάκερ».

β) Επίθεση στις βάσεις δεδομένων με τις οποίες μπορεί να διασυνδεθεί (εφόσον ενεργοποιείται η ηλεκτρονική διακυβέρνηση). Πρόκειται για τον μεγαλύτερο κίνδυνο, καθώς οι κυβερνοεπιθέσεις είναι πλέον επιστήμη, και οι επίδοξοι «χάκερς» δεν είναι απλοί κλέφτες. Είναι εκείνοι οι οποίοι θα απενεργοποιήσουν τον οποιονδήποτε συναγερμό σε σπίτι, επιχείρηση, αυτοκίνητο ή τράπεζα.

Ποια είναι όμως η διαφορά ανάμεσα σε ένα κλέφτη και

ένα «χάκερ»; Ο μεν κλέφτης θα φύγει με ό,τι κατάφερε να κλέψει από ένα συγκεκριμένο μέρος, εάν δεν έγινε αντιληπτός. Ο δε «χάκερ» θα φύγει με ό,τι έχεις και δεν έχεις. Εφόσον μάλιστα μιλάμε για ενοποιημένες βάσεις δεδομένων, οτιδήποτε είναι διασυνδεδεμένο, από δεδομένα υγείας μέχρι στοιχεία τράπεζας, μπορούν να πέσουν στα χέρια του.

Σήμερα η Ιαπωνία, αν και πρωτοπόρος παγκοσμίως στο πεδίο των νέων ψηφιακών τεχνολογιών, ωστόσο αντιμετωπίζει έντονο κοινωνικό προβληματισμό αφού μέχρι τώρα έχουν καταγραφεί πολλές διαρροές προσωπικών δεδομένων, αλλά και λάθη διασύνδεσης του ψηφιακού ιατρικού φακέλου με ηλεκτρονικές ταυτότητες άλλων προσώπων.

Η Εσθονία, ως γνωστόν, αποτέλεσε πρότυπο για την ελληνική κυβέρνηση στο πεδίο των νέων ταυτοτήτων. Ωστόσο συνδέθηκε με μία από τις μεγαλύτερες διαρροές προσωπικών δεδομένων, καθώς μίσυσε την ανάδοχο εταιρεία (Gemalto) για «ελαττώματα». Η Gemalto παραδέχθηκε ότι αντιμετώπισε πλημμελώς το θέμα, καθώς αποδείχθηκε ότι αντί να ενσωματώσει κωδικούς κλειδιού στο chip των κυβερνητικών ταυτοτήτων, έμεινε ευάλωτη σε εξωτερικές επιθέσεις.

Κυβερνοεπιθέσεις: μία πραγματικότητα που ήρθε για να μείνει.

Μέσα ήδη στο 2023, πέντε μεγάλοι μεγέθους κυβερνοεπιθέσεις κατεγράφησαν, περιλαμβάνοντας ως στόχους τα υπουργεία της κυβέρνησης της Νορβηγίας, το αμερικανικό δίκτυο φαρμακείων PharMerica, την εφαρμογή “MOVEit” της Genworth Financial, την MCNA Dental και τη Latitude Financial. Συνολικά, περισσότερα από 30 εκατομμύρια προσωπικά αρχεία παραβιάστηκαν.

Στην τελευταία δεκαετία, πέντε από τις χαρακτηριστικότερες μεγάλης κλίμακας κυβερνοεπιθέσεις συνέβησαν εις βάρος της Yahoo! (2014, 500 εκατομμύρια λογαριασμοί), της River City Media (2017, 1.4 δισεκατομμύρια αρχεία), της εφαρμογής MyFitnessPal της Under Armour (2018, 144 εκατομμύρια επαφές), του Πενταγώνου των ΗΠΑ, καθώς και πυρηνικού σταθμού σύμφωνα με τον πρόεδρο του Διεθνούς Οργανισμού Ατομικής Ενέργειας (ΔΟΑΕ) Y. Amano.

Στην Ελλάδα, σημαντικές κυβερνοεπιθέσεις έχουν στοχεύσει μεταξύ άλλων υπηρεσίες των Gov.gr και TAXISnet (όπου άγνωστοι κυβερνοεγκληματίες από την Ολλανδία με πρωτοφανή επίθεση επιχείρησαν να θέσουν εκτός λειτουργίας 800 κυβερνητικές ιστοσελίδες, «παγώνοντας» ηλεκτρονικές ιατρικές συνταγές), το Υπουργείο Παιδείας (με στόχο μια κεντρική πλατφόρμα εξετάσεων λυκείου και υπολογιστές σε 114 χώρες, προκαλώντας διακοπές λειτου-

ργίας και καθυστερήσεις στις εξετάσεις λυκείου), το Υπουργείο Προστασίας του Πολίτη, την ιστοσελίδα αξιολόγησης του ΙΕΠ, το Υπουργείο Εξωτερικών (θύμα των Anonymous), το Εθνικό Τυπογραφείο, τη Βουλή των Ελλήνων (θύμα των «Real Democracy Reverse Engineering»).

Εν κατακλείδι, δεν υπάρχει καμμία εγγύηση ότι η νέα ηλεκτρονική ταυτότητα, τα συστήματα που την υποστηρίζουν καθώς και οι βάσεις δεδομένων τους είναι ασφαλή. Μία επίθεση στην ταυτότητα-κάρτα ή στα δεδομένα μας μπορεί να μας στοιχίσει «όλη μας τη ζωή».

Αφορισμοί επομένως περί απόλυτης ασφάλειας καλό θα είναι να αποφεύγονται από την κυβέρνηση. Εάν η κυβέρνηση απαντά σοβαρά σε επιχειρήματα που παρατίθενται, εάν δεν εθελουφλεί και δεν απαξιώνει προσάπτοντας «ταμπέλες» σε όσους διαφωνούν μαζί της, τότε θα αρχίσουμε να απομακρυνόμαστε από το ολιγαρχικό καθεστώς που βιώνουμε και θα ανακαλύπτουμε χαρακτηριστικά μιας υγιούς δημοκρατίας.



Τι θα γίνει αν αύριο έχουμε ένα (επίσημα) απολυταρχικό καθεστώς;

Βιώνουμε σήμερα μία αρρωστημένη εκδοχή δημοκρατίας όπου ναι μεν ακόμα έχουμε το δικαίωμα ψήφου, αλλά διαπιστώνουμε καθημερινά το έλλειμμα δημοκρατίας, την απουσία διαλόγου, την ασέβεια, και τη δολοφονία του χαρακτήρα όποιου δεν συμφωνεί. Οι περιορισμοί ελευθεριών έχουν ενταθεί: Η υποχρεωτικότητα, η στέρηση προσωπικών ελευθεριών, η τελευταία θέση κατάταξης στην Ε.Ε. σε δείκτες «ελευθερίας του τύπου». Η αποθράσυνση της εξουσίας σηματοδοτείται όταν δεν υπάρχει διάκριση των εξουσιών, όταν ο πρωθυπουργός της χώρας διορίζει βάσει της προσωπικής αρεσκείας του τους επικεφαλής της δικαιοσύνης, των ενόπλων δυνάμεων και γενικώς, κάθε διοικητικό στέλεχος του κρατικού μηχανισμού, καθώς και από την συστηματική ατιμωρησία και έλλειψη απόδοσης ευθυνών.

Αντίθετα, βλέπουμε ενθουσιασμό και ευθυγράμμιση του πρωθυπουργού μας και των στενών συνεργατών του με τους ... οραματιστές της «Μεγάλης Επανεκκίνησης» κ.κ. Κλάους Σβάμπ και Γιουβάλ Νάε Χαράρι. Μιλούν για τον λεγόμενο «Μετάνθρωπο», την εξέλιξη του Homo Sapiens σε Homo Deus (δηλαδή από «σοφό άνθρωπο» σε «άνθρωπο-θεό»), την σωματική αναβάθμιση, ως προϊόν της λεγόμενης «τέταρτης βιομηχανικής επανάστασης» όπου συγκλίνουν η μοριακή βιολογία, η πληροφορική και η τεχνητή

νοημοσύνη. Ένας βιολογικά μεταλλαγμένος άνθρωπος, γεμάτος τσιπάκια και πρόσθετα μηχανικά μέλη, που νομίζει ότι θα νικήσει ακόμα και τον βιολογικό θάνατο και θα ζήσει για πάντα επί γης.

Κοντά στον Μετανθρωπισμό, κερασάκι στην τούρτα οι εφαρμογές της «γενικής» Τεχνητής Νοημοσύνης που κινδυνεύουν να δημιουργήσουν μία άλλη, εφιαλτική έκδοση της ανθρωπότητας. Ο γνωστός Έλον Μάσκ, προβληματισμένος, είπε ότι «η Τεχνητή Νοημοσύνη είναι πολύ πιο επικίνδυνη από τα πυρηνικά όπλα», ενώ ο κ.Τζέφρι Χίντον, υψηλόβαθμο στέλεχος της Google και γνωστός ως «νονός της τεχνητής νοημοσύνης» δήλωσε «φοβισμένος από την εξέλιξη της τεχνολογίας και ιδιαίτερα της Τεχνητής Νοημοσύνης». **Θα μας χαρακτήριζε κάποιος ως «συνομωσιολόγους», εάν δεν επρόκειτο για δικά τους λόγια.**

Είναι άκρως επικίνδυνο να αφήσουμε ανεξέλεγκτο το μέλλον της πατρίδας μας. Ο υφ. Προστασίας του Πολίτη κ.Κατσαφάδος υπεκφεύγει όταν δηλώνει για την εξέλιξη της ηλεκτρονικής ταυτότητας ότι «δε μπορεί να γνωρίζει το μέλλον, δεν είναι προφήτης». Η κυβέρνηση ξέρει πολύ καλά τί θέλει ο κ. Σβάμπ για το μέλλον μας. Ομως η ευθύνη των αποφάσεων του σήμερα είναι η κληρονομιά του αύριο. Κάθε δικαίωμα που παραδίδουμε σήμερα, θα μπορεί να το καταχραστεί μία μελλοντική κυβέρνηση σε 20 χρόνια από τώρα.

Το Σύστημα Αξιολόγησης Πολιτών της Κίνας

Οι πολίτες αξιολογούνται καθημερινά μέσω συγκεκριμένων δεικτών που μπορεί να τους προσθέσουν ή αφαιρέσουν κοινωνικά δικαιώματα.

Η πλήρης εφαρμογή της ταυτότητας-κάρτας πολίτη βρίσκεται στο σύστημα «κοινωνικής πίστωσης» της Κίνας: πρόκειται για ένα ευρύ ρυθμιστικό πλαίσιο που βαθμολογεί την «αξιοπιστία» των ατόμων, των εταιρειών και των κυβερνητικών οντοτήτων σε ολόκληρη την Κίνα. Τον Ιούνιο του 2022, θεσπίστηκε πενταετές σχέδιο για το «κράτος δικαίου» εντός της Κίνας, με καθοδήγηση από το Κρατικό Συμβούλιο.

Βασικοί άξονες του συστήματος αυτού:

- Ο στόχος του συστήματος κοινωνικής πίστωσης της Κίνας είναι να παρέχει ολιστική αξιολόγηση της αξιοπιστίας ενός ατόμου ή μιας εταιρείας.

- Οι συνέπειες ενός κακού κοινωνικού πιστωτικού αποτελέσματος θα μπορούσαν να είναι πάρα πολύ σοβαρές. Μπορεί να επηρεάσει τις ταξιδιωτικές προοπτικές, την απασχόληση, την πρόσβαση σε χρηματοδότηση και την ικανότητα σύναψης συμβάσεων. Από την άλλη, ένα θετικό πιστωτικό αποτέλεσμα θα μπορούσε να διευκολύνει μια σειρά επιχειρηματικών συναλλαγών.

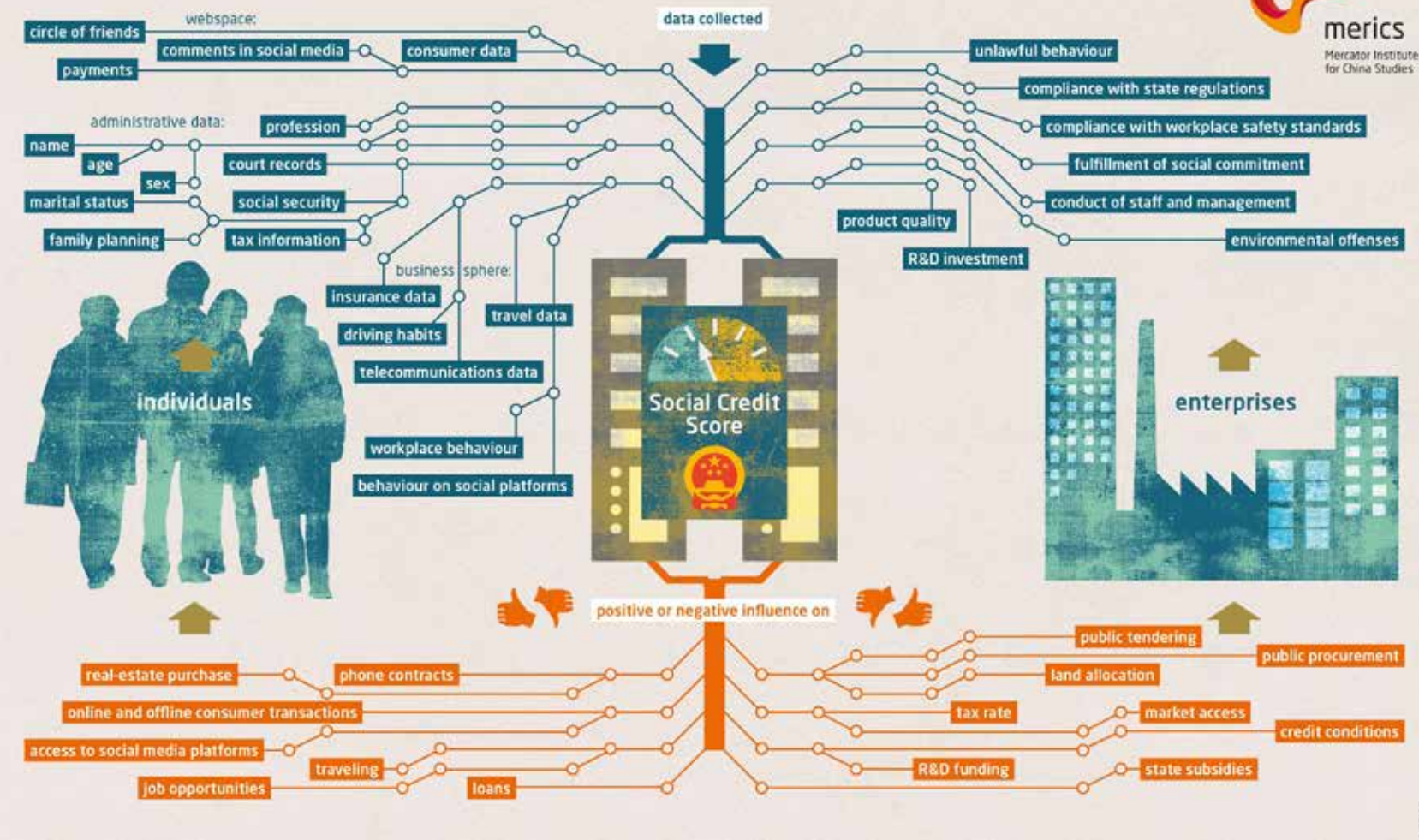
- Είναι σημαντικό κάθε ξένη επιχείρηση που επιθυμεί να εδραιώσει την παρουσία της στην Κίνα να αναζητήσει επαγγελματικές συμβουλές για τη διαχείριση ενός κοινωνικού πιστωτικού αποτελέσματος. Αυτό ισχύει τόσο για τις ατομικές βαθμολογίες όσο και για το εταιρικό κοινωνικό πιστωτικό αποτέλεσμα.

- Πιο συγκεκριμένα, μέσω της διευκόλυνσης της εμπιστοσύνης, το σύστημα κοινωνικής πίστωσης της Κίνας υποστηρίζει τους ακόλουθους στόχους: Χρηματοοικονομική πιστοληπτική ικανότητα, Δικαστική εκτέλεση, Εμπορική αξιοπιστία, Κοινωνική αξιοπιστία, Κυβερνητική ακεραιότητα, Συλλογή και κοινή χρήση δεδομένων, Επιμέλεια μαύρων και κόκκινων λιστών, Τιμωρίες, κυρώσεις και ανταμοιβές.

Το 2018, ο πρώην αντιπρόεδρος των ΗΠΑ, Μάικ Πενς, έκρουσε τον κώδωνα του κινδύνου για το σύστημα κοινωνικής πίστωσης της Κίνας, δηλώνοντας ότι «οι ηγέτες της Κίνας στοχεύουν να εφαρμόσουν ένα οργουελιανό σύστημα που βασίζεται στον έλεγχο σχεδόν κάθε πτυχής της ανθρώπινης ζωής - το λεγόμενο «κοινωνικό πιστωτικό αποτέλεσμα».

Εν αντιθέσει, ο κ. Κλάους Σβάμπ, εκθειάζοντας το σύστημα αυτό είπε ότι **«θα μπορούσε να αποτελέσει πρότυπο σε πολλά έθνη»**.

The all-seeing state: China's plans for total data control



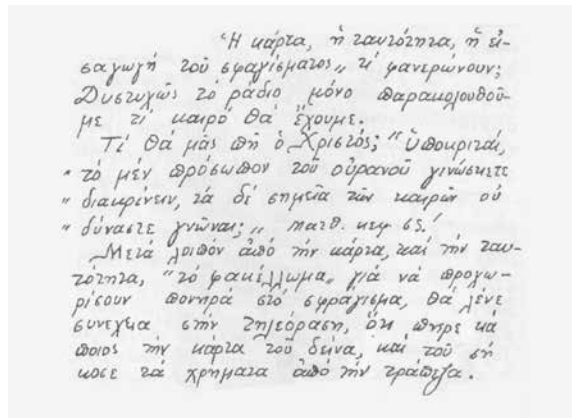
Ο εύλογος προβληματισμός των πιστών

Η Ορθόδοξη Εκκλησία μας έχει κατά καιρούς εκφράσει σαφή και συγκεκριμένη θέση, εκφράζοντας επιφυλάξεις και ανησυχίες για τις απόπειρες κατάργησης των προσωπικών ελευθεριών διαμέσου της κάρτας του πολίτη.

- Η Ιερά Σύνοδος της Εκκλησίας της Ελλάδος με το Ανακοινωθέν 17/11/2010, τόνιζε, εκτός των άλλων, κατηγορηματικά, ότι «...κατ' ούδένα τρόπο πρέπει να παραβιάζονται με αυτήν (την «κάρτα του πολίτη») οι προσωπικές ελευθερίες». Σε παλαιότερο ανακοινωθέν (9/3/1993) η Ιερά Σύνοδος της Εκκλησίας της Ελλάδος, αναδεικνύοντας τούς κινδύνους των ηλεκτρονικών ταυτοτήτων (όταν ακόμη περιείχαν μαγνητικές λωρίδες και όχι τα έξυπνα μικροτσιπ (RFID) τόνιζε ότι «...υπάρχει η δυνατότης μιάς έφιαλτικής άπειλης κατά τών άτομικών ελευθεριών του πολίτου...». Στο ίδιο μήκος κύματος εκινείτο και η Ανακοίνωση της Ιεράς Κοινότητας του Αγίου Όρους, αλλά και οι Ιερές Μονές των Αγίων Μετεώρων (13-6-1997).

- Σε χειρόγραφη επιστολή του το έτος 2015, ο π. Γρηγόριος του Ιερού Ησυχαστηρίου Αγ. Ιωάννου Προδρόμου στη Μεταμόρφωση Χαλκιδικής, μαρτυρεί: «Πριν από 30 χρόνια περίπου ο άγιος Παΐσιος μου είχε πει θα σας συνηθίσουν στις κάρτες (που δεν είναι τίποτε) έως ότου φθάσουν στην έξυπνη κάρτα που θα είναι για όλες τις χρήσεις: Ταυτότητα, διαβατήριο, υγεία, για ψώνια, για όλα. Αυτήν είπε να μην την πάρετε. Δεν είναι το σφράγισμα, αλλά έχει σχέση με το σφράγισμα.»

- Στο περίφημο χειρόγραφο του «Τά σημεία τών καιρών» ο άγιος Παΐσιος ο Αγιορείτης αναφέρει: «Η κάρτα, ή ταυτότητα, ή είσαγωγή του σφραγίσματος» τί φανερώνουν; Δυστυχώς τό ράδιο μόνο παρακολουθούμε τί καιρό θά έχουμε. Τί θά μās πῆ ὁ Χριστός; «ὑποκριταί, τό μέν πρόσωπον τοῦ οὐρανοῦ γινώσκετε διακρίνειν, τά δέ σημεία τών καιρών οὐ δύναστε γνῶναι;» Ματθ. κεφ. 16,3. Μετά λοιπόν ἀπό τήν κάρτα, καί τήν ταυτότητα, «το φακέλλωμα» γιά νά προχωρίσουν πονηρά στό σφράγισμα, θά λένε συνέχεια στήν τηλεόραση, ὅτι πήρε κάποιος τήν κάρτα τοῦ δεινά, καί τοῦ σήκωσε τά χρήματα ἀπό τήν τράπεζα».



- Αξίζει να σημειωθεί ότι ο οποιοσδήποτε αριθμός μπορεί να συμβολίζει τη νέα ηλεκτρονική ταυτότητα. Ακόμη και τον Σταυρό να έβαζε η κυβέρνηση επάνω της, την απορρίπτουμε και επιφυλασσόμαστε για αυτό που αντιπροσωπεύει και για αυτό στο οποίο μπορεί να εξελιχθεί.

Στοιχεία που ενσωματώνει η ηλεκτρονική ταυτότητα

Όπως ειπώθηκε εισαγωγικά, οι δημοσιευμένες τεχνικές προδιαγραφές αποτελούν, στην καλύτερη περίπτωση, απλώς το εξώφυλλο ενός τουλάχιστον εκατοντασέλιδου βιβλίου το οποίο παραμένει άγνωστο με την αιτιολογία της εμπιστευτικότητας.

Τα ορατά στοιχεία της ηλεκτρονικής ταυτότητας (βάσει ΚΥΑ 10/4/2018 αρ. 8200/0-297647, 19/4/2019 αρ. 8200/0-181623 και 17/2/2023 αρ. 8200/0-109568) περιέχουν επώνυμο, όνομα, φύλο, ημερομηνία γέννησης, ιθαγένεια, όνομα πατρός και μητρός, τόπο γέννησης, ομάδα αίματος, ύψος, υπογραφή, φωτογραφία βιομετρικών προδιαγραφών, καθώς και στοιχεία μηχανικής ανάγνωσης του δελτίου ταυτότητας.

Σύμφωνα με δηλώσεις του υπουργού Ψηφιακής Διακυβέρνησης κ. Δ. Παπαστεργίου, από το τέλος του 2023 θα συμπεριλαμβάνεται στην ταυτότητα και ο προσωπικός αριθμός (Π.Α.)

Το ενσωματωμένο τσίπ, τύπου NFC, θα συμπεριλαμβάνει εκτός των ανωτέρω στοιχείων και τα δακτυλικά αποτυπώματα των δύο δεικτών. Σημειώνουμε ότι στο παρελθόν τα δακτυλικά αποτυπώματα είχαν καταργηθεί από τις ταυτότητες, καθώς το κράτος δεν είχε λόγο να προσβάλλει τους πολίτες του θεωρώντας τους «σεσημασμένους». Σήμερα είναι σαφές πως ο πρωθυπουργός θεωρεί τον λαό, τον οποίο υποτίθεται ότι υπηρετεί, και «ψεκασμένο» και «σεσημασμένο».



Η πρόταση της ΝΙΚΗΣ

Α. Για λόγους δημοκρατίας, η ΝΙΚΗ ζητά **πλήρη και σαφή ενημέρωση** στους πολιτικούς φορείς και στον ελληνικό λαό από τις αρμόδιες υπηρεσίες, αν και άρχισε η έκδοση των νέων ταυτοτήτων, όχι μόνο για τα τεχνικά χαρακτηριστικά τους, αλλά κυρίως για τη φύση, τον χαρακτήρα και τους κινδύνους που εγκυμονούν για την ελευθερία του. Ως εκ τούτου, μέχρι να υπάρξει έγκυρη υπεύθυνη ενημέρωση, καλούμε τους πολίτες **να μην παραλάβουν τις νέες ταυτότητες**.

Β. Η ταυτότητα να επιτελεί αυτό που σχεδιάστηκε να κάνει. Να είναι μέσον ταυτοποίησης και όχι μέσον άσκησης δικαιωμάτων. Εάν σκοπεύει η Κυβέρνηση σε επόμενο χρόνο να προσθέσει και να αποθηκεύσει στη νέα ταυτότητα και τα στοιχεία της Ηλεκτρονικής Διακυβέρνησης, να λειτουργεί δηλαδή όχι μόνο ως μέσο ταυτοποίησης, αλλά συγχρόνως και ως μοναδικό μέσο άσκησης δικαιωμάτων, απορρίπτουμε το τελευταίο κατηγορηματικά και απόλυτα. Πολύ περισσότερο αν καταστεί και «ηλεκτρονικό πορτοφόλι» αποθήκευσης του σχεδιαζόμενου ψηφιακού ευρώ.

Γ. Η ταυτότητα να είναι ασφαλής χωρίς δυνατότητα πλαστογράφησης. Αποδεχόμαστε ως χρήσιμη και αναγκαία την έκδοση νέων ασφαλών αστυνομικών ταυτοτήτων που θα αποκλείουν τη δυνατότητα πλαστογράφησης. Αυτό μπορεί να επιτευχθεί με την καθιέρωση συμβατικών ταυτοτήτων –μη ηλεκτρονικών– που όμως με τη προσθήκη

κατάλληλων υδατογραφημάτων, γραμματοκοσμημάτων και ασφαλιστικών δαπέδων θα είναι απρόσφορες σε πλαστογράφηση. Η σύγχρονη επιστήμη της εκτύπωσης κρατικών εγγράφων παρέχει τη δυνατότητα εκτύπωσης απλαστογράφητων δελτίων ταυτότητας με τη μέθοδο ξηράς OFFSET που θα περιλαμβάνει σύνθετα γραμματοκοσμήματα και ασφαλιστικά πολύχρωμα δάπεδα στην πρόσθια και την οπίσθια όψη.

Εναλλακτικά, μπορεί να χρησιμοποιηθεί η τελευταία μεθοδολογία εκτύπωσης χαρτονομισμάτων του ευρώ που παρέχει σχεδόν απόλυτη ασφάλεια. Στα τραπεζογραμμάτια ευρώ έχουν ενσωματωθεί ποικίλα και προηγμένα χαρακτηριστικά ασφαλείας, τα οποία εξασφαλίζουν την εύκολη αναγνώρισή τους από τους πολίτες και τα προστατεύουν από την παραχάραξη.

Δ. Σε κάθε περίπτωση, ζητούμε ο πολίτης να έχει πρόσβαση και γνώση για τα συλλεγόμενα και αποθηκευόμενα προσωπικά του δεδομένα. Να ελέγχει το είδος και το περιεχόμενο των καταγεγραμμένων και αρχειοθετουμένων σε τράπεζα δεδομένων και πληροφοριών (μέσω του RFID chip της ταυτότητάς του), που αφορούν άμεσα το πρόσωπό του. Η δεξαμενή των σημαντικών πληροφοριών που θα δημιουργηθεί από τα ανωτέρω στοιχεία, θα τηρείται στην Διεύθυνση Κρατικής Ασφαλείας του Αρχηγείου της Ελληνικής Αστυνομίας (άρθρο 10 ΚΥΑ). Το άλλο όμως μεγάλο

αρχείο-«δεξαμενή», που θα προκύψει από τα δεδομένα της Ηλεκτρονικής Διακυβέρνησης –εξ αιτίας της προαναφερόμενης λειτουργικής χρήσης της ταυτότητας ως μέσου ασκήσεως δικαιωμάτων– είναι άγνωστο ακόμη που θα τηρείται και ποιός θα έχει πρόσβαση σε αυτό. Ερωτούμε και θέλουμε απάντηση, διότι είναι γνωστό ότι όλες οι ηλεκτρονικές εθνικές δεξαμενές πληροφοριών διασυνδέονται με υπερεθνικά (ευρωπαϊκά και μη) ηλεκτρονικά αρχεία.

Ε. Θεωρούμε αυτονόητο ότι οι βάσεις δεδομένων με τα αποθηκευμένα στοιχεία των Ελλήνων πολιτών θα βρίσκονται **αποκλειστικά επί ελληνικού εδάφους** και πουθενά αλλού.

ΣΤ. Επίσης θεωρούμε αυτονόητο να γνωστοποιηθεί το **ποιός θα έχει πρόσβαση ή/και δικαίωμα επεξεργασίας στα στοιχεία** που θα συλλέγονται.

Ζ. **Αρνούμαστε και απορρίπτουμε τον υποχρεωτικό χαρακτήρα των νέων ηλεκτρονικών ταυτοτήτων.** Ζητούμε να είναι προαιρετική η λήψη τους. Να είναι δυνατή η πιστοποίηση του πολίτη και η είσοδος του στην Ηλεκτρονική Διακυβέρνηση με εναλλακτικούς τρόπους, όπως συμβαίνει σε πολλές χώρες του κόσμου και της Ευρώπης.

Σε διαφορετική περίπτωση, ευθαρσώς δηλώνουμε ότι για λόγους ελευθερίας και δημοκρατικής συνειδήσεως, ΔΕΝ θα παραλάβουμε τις νέες ταυτότητες και τις μελλοντικές αναβαθμίσεις τους.

Καλούμε τον Ελληνικό λαό να προβληματιστεί γι αυτό το πολύ σοβαρό ζήτημα, να ενημερωθεί πλήρως και σε βάθος από αντικειμενικές πηγές για τους κινδύνους που θα προκύψουν από τις ηλεκτρονικές ταυτότητες για τις ελευθερίες και τα δικαιώματά του. Η μαζικότητα της αντίστασης θα κάμψει την επιβαλλόμενη υποχρεωτικότητα. Θα αναγκαστούν να μας εξασφαλίσουν εναλλακτικό τρόπο πιστοποίησης.



*«Οὐ παντελῶς δεῖ τοῖς πονηροῖς ἐπιτρέπειν,
ἀλλ' ἀντιτάττεσθαι.»*

Μένανδρος