

ΨΗΦΙΑΚΕΣ ΤΑΥΤΟΤΗΤΕΣ ΚΑΙ ΠΡΟΣΩΠΙΚΟΣ ΑΡΙΘΜΟΣ – ΠΡΟΑΙΡΕΤΙΚΟΤΗΤΑ ΟΧΙ ΥΠΟΧΡΕΩΤΙΚΟΤΗΤΑ

Οι ψηφιακές ταυτότητες και ο Προσωπικός Αριθμός (ΠΑ) στην Ελλάδα αποτελούν τα δύο βασικά «κλειδιά» για την πλήρη ψηφιοποίηση της σχέσης κράτους-πολίτη. Ενώ προβάλλονται ως εργαλεία εκσυγχρονισμού, η υποχρεωτικότητά τους εγείρει σοβαρά ζητήματα **ψηφιακού αυταρχισμού** και ελέγχου.

1. Η Σημασία των Υποχρεωτικών Ψηφιακών Ταυτοτήτων

Οι νέες ταυτότητες, που είναι υποχρεωτικές για ταξίδια στην ΕΕ από το καλοκαίρι του 2026, ενσωματώνουν ψηφιακό τσιπ με βιομετρικά δεδομένα.

- **Κεντρικός Έλεγχος:** Τα δεδομένα αποθηκεύονται σε μια κεντρική βάση της Γενικής Γραμματείας Πληροφοριακών Συστημάτων. Αυτή η συγκέντρωση επιτρέπει στο κράτος να έχει μια πλήρη, ψηφιακή εικόνα κάθε πολίτη.
- **Κίνδυνος Αποκλεισμού:** Η υποχρεωτικότητα σημαίνει ότι χωρίς το ψηφιακό μέσο, ο πολίτης κινδυνεύει με «ψηφιακό θάνατο», δηλαδή αδυναμία πρόσβασης σε βασικά δημόσια και ιδιωτικά αγαθά.
- **Ιχνηλασιμότητα:** Κάθε χρήση της ψηφιακής ταυτότητας αφήνει αποτύπωμα, επιτρέποντας την παρακολούθηση των κινήσεων και των συναλλαγών του ατόμου σε πραγματικό χρόνο.

2. Ο Προσωπικός Αριθμός ως «Ψηφιακό Κλειδί» Ελέγχου

Ο Προσωπικός Αριθμός (12 χαρακτήρες) είναι ένας μοναδικός, μόνιμος αριθμός που αντικαθιστά σταδιακά τον ΑΦΜ και τον ΑΜΚΑ.

- **Ενοποίηση Δεδομένων:** Λειτουργεί ως ο «συνδετικός κρίκος» που ενώνει όλες τις βάσεις δεδομένων (υγεία, εφορία, ασφάλιση, ποινικό μητρώο). Αυτό επιτρέπει στο κράτος να δημιουργήσει ένα **πλήρες προφίλ (profiling)** για κάθε πολίτη.
- **Αυτοματοποιημένος Έλεγχος:** Με έναν μόνο αριθμό, το σύστημα μπορεί να επιβάλλει αυτόματες κυρώσεις (π.χ. «πάγωμα» λογαριασμών ή πρόσβασης σε υπηρεσίες) αν ο πολίτης δεν συμμορφώνεται με κρατικές επιταγές.

- **Ευπάθεια & Υποκλοπή:** Η συγκέντρωση όλων των δικαιωμάτων σε έναν μόνο αριθμό σημαίνει ότι αν αυτός κλαπεί ή παραβιαστεί, ο πολίτης χάνει τον έλεγχο ολόκληρης της ψηφιακής του ύπαρξης.

3. Η Σύνδεση με τον Ψηφιακό Αυταρχισμό

Ο συνδυασμός ταυτότητας και ΠΑ δημιουργεί την υποδομή για ένα σύστημα **ψηφιακής επιτήρησης** όπου:

A) Η ιδιωτικότητα καταργείται, καθώς καμία συναλλαγή δεν παραμένει ανώνυμη.
B) Το κράτος αποκτά τη δύναμη να «απενεργοποιεί» πολίτες που θεωρούνται «ύποπτοι» ή μη συνεργάσιμοι.

Γ) Δημιουργείται το υπόβαθρο για συστήματα **κοινωνικής βαθμολόγησης** (τύπου Κίνας), όπου τα δικαιώματα του πολίτη εξαρτώνται από τη «βαθμολογία» που του δίνει ο αλγόριθμος.

4.- Είναι εφικτή η υλοποίηση της προαιρετικότητας;

Ναι, η ύπαρξη δύο παράλληλων συστημάτων ταυτοποίησης είναι απολύτως εφικτή και αποτελεί τη βάση της **δημοκρατικής συμπερίληψης**. Για δεκαετίες το κράτος λειτουργούσε ακριβώς έτσι, και η τεχνολογία πρέπει να προστίθεται ως επιλογή, όχι να επιβάλλεται ως αποκλεισμός.

Τι ισχύει στην Ελβετία

Στην Ελβετία, μετά το δημοψήφισμα του 2021 όπου οι πολίτες απέρριψαν την ιδιωτική διαχείριση της ψηφιακής ταυτότητας (e-ID), το κράτος επανασχεδίασε το σύστημα με άξονα την **προαιρετικότητα**.

- **Παράλληλα Συστήματα:** Ο πολίτης μπορεί να κατέχει τη φυσική του ταυτότητα (κάρτα) για όλες τις συναλλαγές του. Η ψηφιακή ταυτότητα είναι μια **εθελοντική εφαρμογή** στο κινητό που αντλεί δεδομένα από την επίσημη κρατική βάση, αλλά δεν την αντικαθιστά.
- **Αυτονομία Δεδομένων:** Ο χρήστης ελέγχει ποια δεδομένα μοιράζεται (π.χ. μόνο ότι είναι άνω των 18, χωρίς να δείχνει ημερομηνία γέννησης).
- **Φυσική Παρουσία:** Κάθε ψηφιακή υπηρεσία συνοδεύεται από την υποχρέωση του κράτους να παρέχει **φυσικό σημείο εξυπηρέτησης** για όσους δεν επιθυμούν ή δεν μπορούν να χρησιμοποιήσουν το e-ID.

5.- Πώς θα ταυτοποιούνται οι «Εξαιρούμενοι» στην Ελλάδα. Η πρότασή μας

Η πρόταση της **ΕΞΟΔΟΣ** είναι πειστική γιατί είναι εφαρμόσιμη και βασίζεται στην **αρχή της ισοδυναμίας**:

Α) Κλασική Αστυνομική Ταυτότητα (Χωρίς Chip): Η ταυτοποίηση γίνεται με τη φυσική επίδειξη του εγγράφου και τη φωτογραφία, όπως γινόταν πάντα. Το κράτος οφείλει να εκδίδει ταυτότητες που συμμορφώνονται με τα διεθνή πρότυπα ασφαλείας (π.χ. ICAO) αλλά χωρίς υποχρεωτική ψηφιακή διασύνδεση/τσιπ για εσωτερική χρήση.

Β) Χρήση Υπαρχόντων Μητρώων (Offline): Αντί για τον **Προσωπικό Αριθμό**, ο πολίτης συνεχίζει να χρησιμοποιεί τον ΑΦΜ ή τον ΑΜΚΑ του ως διακριτά στοιχεία. Η ταυτοποίηση στο γκισέ γίνεται με τη φυσική παρουσία και την υπογραφή του.

Γ) Εξουσιοδοτημένα Κέντρα (ΚΕΠ): Τα ΚΕΠ πρέπει να αναβαθμιστούν σε «Αναλογικές Πύλες». Ο πολίτης που αρνείται την ψηφιακή ταυτότητα, θα πηγαίνει στο ΚΕΠ, θα ταυτοποιείται φυσικά από τον υπάλληλο, και ο υπάλληλος θα διεκπεραιώνει την ψηφιακή διαδικασία για λογαριασμό του (Proxy Identity).

Δ) Υπογραφή με Φυσική Παρουσία: Αντί για την ψηφιακή υπογραφή, παραμένει το «γνήσιο της υπογραφής» μπροστά σε δημόσιο λειτουργό.

6.- Το επιχείρημα της «διαλειτουργικότητας»

Θα μας πουν ότι αυτά δεν είναι εφαρμόσιμα, ότι «το σύστημα δεν μπορεί να έχει δύο δρόμους».

Η απάντηση είναι: **«Η τεχνολογία υπάρχει για να υπηρετεί τον άνθρωπο, όχι για να τον εξαναγκάζει».**

Οι βάσεις δεδομένων μπορούν κάλλιστα να δέχονται καταχώριση από υπάλληλο (χειροκίνητα) και όχι μόνο αυτόματα από το wallet. Απόδειξη το παράδειγμα της Ελβετίας.