ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Ψηφιακών Συστημάτων

Πρόγραμμα Μεταπτυχιακών Σπουδών

"Δίκαιο και Τεχνολογίες Πληροφορικής και Επικοινωνιών"

Διπλωματική εργασία με θέμα:

Ζητήματα ταυτοποίησης, επεξεργασία εθνικού αριθμού ταυτότητας και ζητήματα προστασίας δεδομένων.

Γιαννακάκη Αντιγόνη(ΑΜ:ΜΔΙ 2007)

Επιβλέπουσα καθηγήτρια: Λίλιαν Μήτρου

Περιεχόμενα

Ευχαριστίες

Θα ήθελα να ευχαριστήσω από καρδιάς την επιβλέπουσα καθηγήτρια μου Λίλιαν Μήτρου, για την καθοδήγηση της ως προς την ολοκλήρωση της εργασίας μου, για τις πολύτιμες συμβουλές της, την αμέριστη υποστήριξη της, αλλά και γιατί αποτέλεσε και θα αποτελεί για εμένα υπόδειγμα επιστήμονα και ανθρώπου.

Στο ίδιο πλαίσιο ευγνωμοσύνης, θα ήθελα να ευχαριστήσω όλους τους καθηγητές του Τμήματος Ψηφιακών Συστημάτων για τη συμβολή τους στην ολοκλήρωση του μεταπτυχιακού προγράμματος.

Οφείλω να εκφράσω τις ευχαριστίες μου προς τους φίλους και συνεργάτες μου για την υπομονή τους και την ψυχική στήριξη τους για την ολοκλήρωση της εργασίας.

Τέλος, οφείλω να ευχαριστήσω την οικογένειά μου, που μου δίδαξε ότι η μάθηση δεν τελειώνει ποτέ και μου συμπαραστέκεται σε όλες μου τις επιλογές.

Περίληψη

Στην παρούσα μεταπτυχιακή εργασία βασικό ζήτημα εστίασης είναι η ταυτοποίηση του φυσικού προσώπου, η χρήση του ενός ενιαίου αριθμού και η προστασία των δεδομένων προσωπικού χαρακτήρα. Ειδικότερα θα αναλυθεί το ζήτημα και οι τρόποι ταυτοποίησης των φυσικών προσώπων στο θεωρητικό και πρακτικό του υπόβαθρο , ενώ εν συνεχεία θα αποτυπωθεί το ευρωπαϊκό νομικό πλαίσιο αλλά και παραδείγματα άλλων ευρωπαϊκών και μη χωρών. Ειδική μνεία θα γίνει στην ελληνική νομοθεσία και στους μέχρι σήμερα τρόπους ταυτοποίησης , στην θέσπιση του προσωπικού αριθμού και στα ζητήματα προστασίας προσωπικών δεδομένων στο πλαίσιο εφαρμογής των παραπάνω.

Λέξεις κλειδιά : Ταυτοποίηση, αυθεντικοποίηση, προσωπικός αριθμός, προσωπικά δεδομένα

Abstract

In this master thesis, the main focus issue is the identification of the natural person, the use of a single number and the protection of personal data. In particular, the issue and the ways of identifying natural persons in its theoretical and practical background will be analyzed, while subsequently a European legal framework and examples of other European and non-European countries will be reflected. Special mention will be made of Greek legislation and the ways of identification to date, the establishment of the personal number and the issues of personal data protection in the context of the implementation of the above.

Keywords : Identification, authentication, personal number, personal data

Ι. Η έννοια της ταυτότητας

1.Εισαγωγή

Στην καθημερινή μας ζωή, η λέξη ταυτότητα έχει πολλές σημασίες. Για τους περισσότερους ανθρώπους, ταυτότητα, σημαίνει για παράδειγμα ονοματεπώνυμο, διεύθυνση, αριθμός άδειας οδήγησης, αριθμός διαβατηρίου, μπορεί να περιλαμβάνει επίσης προσωπικές προτιμήσεις και συμπεριφορές των φυσικών προσώπων. Για τις επιχειρήσεις, η ταυτότητα περιλαμβάνει ρόλους, προνόμια, δικαιώματα και υποχρεώσεις για κάθε φυσικό πρόσωπο. Για τη δημόσια διοίκηση, η ταυτότητα είναι το ταυτοποιητικό έγγραφο, όπως για παράδειγμα το αστυνομικό δελτίο ταυτότητας, η βεβαίωση κατοικίας, η βεβαίωση κοινωνικής ασφάλισης, η απόδοση αριθμού φορολογικού μητρώου. Σύμφωνα μάλιστα με το άρθρο 4 αρ. 1 ΓΚΠΔ, ως δεδομένο προσωπικού χαρακτήρα, νοείται κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Ταυτοποιήσιμο φυσικό πρόσωπο, θεωρείται, το πρόσωπο του οποίου η ταυτότητα, μπορεί να αναγνωριστεί άμεσα ή έμμεσα, μέσω κάποιου αναγνωριστικού στοιχείου της, δηλαδή: όνομα, αριθμός ταυτότητας ή εν γένει παράγοντες που προσδιορίζουν την σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική του προέλευση. Πρόκειται στην ουσία, για κάθε πληροφορία που είτε μόνη της είτε συνδυαστικάμπορεί να οδηγήσει σε ταυτοποίηση ενός εν ζωή φυσικού προσώπου. Ωστόσο, ο ΓΚΠΔ εισάγει και ένα νεωτερισμό σε σχέση με το ζήτημα της ταυτοποίησης ενός προσώπου, θεσμοθετώντας και την έννοια των επιγραμματικών αναγνωριστικών χαρακτηριστικών (ή στοιχείων ταυτότητας) ως προσωπικών δεδομένων. Πρόκειται ουσιαστικά για διευθύνσεις IP, αυτοεγκαθιστώμενα αρχεία cookies, ετικέτες RFID, διευθύνσεις διαδικτυακού πρωτοκόλλου και εν γένει στοιχεία ταυτότητας, τα οποία αν συνδυαστούν με άλλες αναγνωριστικές πληροφορίες, μπορούν να δημιουργήσουν το προφίλ ενός ατόμου ή και να επιτρέψουν τον προσδιορισμό της ταυτότητάς του[1].

Η ταυτοποίηση των φυσικών προσώπων, ο αριθμός της εθνικής ταυτότητας, η ψηφιακή ταυτότητα, είναι το σημερινό ζήτημα, και στην παρούσα εργασία θα προσπαθήσουμε να περιγράψουμε τις απαιτήσεις που πρέπει να πληρούνται,, την ανάγκη προστασίας της ιδιωτικότητας των φυσικών προσώπων και της ασφάλειας των προσωπικών τους δεδομένων. Η ενασχόληση με τα ως άνω ζητήματα καθίσταται αρκετά περίπλοκη καθώς παρουσιάζουν τόσο κοινωνικές όσο και νομικές πτυχές, στον φυσικό αλλά και στον ψηφιακό κόσμο.

Παρακάτω θα προσπαθήσουμε να αποτυπώσουμε τις τρέχουσες και μελλοντικές τάσεις που σχετίζονται με την ταυτοποίηση και τη διαχείριση της ταυτότητας και να τονίσουμε σημαντικά θέματα τα οποία θα πρέπει να αντιμετωπιστούν.

[1] Βλ. αιτιολογική σκέψη (30) του Προοιμίου του ΓΚΠΔ

2. Ταυτότητα, Ταυτοποίηση και Πιστοποίηση/ Αυθεντικοποίηση

Στην παρούσα ενότητα δίνεται έμφαση στην **έννοια της ταυτότητας, της ταυτοποίησης και της πιστοποίησης της ταυτότητας**, προσδιορίζοντας τα μέσα με τα οποία μπορεί να αναγνωριστούν τα άτομα, λαμβάνοντας υπόψη τις σύγχρονες τεχνολογίες που μπορεί να συντελέσουν στον έλεγχο της ταυτότητας των προσώπων.

Η ταυτοποίηση αποτελεί ένα κεντρικό ζήτημα τόσο για τους δημόσιους αλλά και τους ιδιωτικούς φορείς, λαμβάνοντας υπόψη και τις περιπτώσεις των κυβερνοεπιθέσεων, οι οποίες πλέον είναι πολύ συχνές στον ψηφιακό κόσμο(λ.χ. κλοπή ταυτότητας, ηλεκτρονικά εγκλήματα, κ.λπ.). Επίσης, δεδομένου ότι η ταυτότητα ενός προσώπου, ως άυλη έννοια, απαρτίζεται από σύνολο προσωπικών στοιχείων ταυτοποίησης και συνδυασμό χαρακτηριστικών που μπορεί να είναι γενετικά, επίκτητα, κοινωνικά, οικονομικά, και άλλα., καθίσταται απτή έννοια, μέσω της χρήσης της τεκμηρίωσης ταυτότητας. Ωστόσο, κρινεται σημαντικό, στη σημερινή εποχή , τα πρόσωπα να μπορούν να αποδεικνύουν την ταυτότητά τους όχι μόνο στο φυσικό, αλλά και στον ψηφιακό κόσμο.

Πέραν των **γενετικά καθορισμένων χαρακτηριστικών** ενός προσώπου, υπάρχουν και **προσδιοριστικά στοιχεία που μπορεί να αποδίδονται στο άτομο από το κράτος, είτε κατά τη γέννηση είτε μετά τη γέννηση**, όπως η ημερομηνία γέννησης, ο τόπος γέννησης, το όνομα, κ.λπ. Επίσης, άλλα προσδιοριστικά στοιχεία του ατόμου, αποτελούν τα πρωτεύοντα κλειδιά που έχουν αποδοθεί από το κράτος, όπως ο αριθμός κοινωνικής ασφάλισης και ο αριθμός φορολογικού μητρώου. Εξάλλου, κάθε άτομο, αλληλεπιδρώντας με την κοινωνία, **αποκτά πρόσθετα χαρακτηριστικά**, όπως η διεύθυνση κατοικίας, το ιστορικό εκπαίδευσής του, το ιστορικό απασχόλησης, οι συγγενικές/ συζυγικές σχέσεις, οι απόγονοι, τα περιουσιακά στοιχεία, το ιατρικό ιστορικό, κ.λπ.

Σε κάθε περίπτωση, **η συσσώρευση προσωπικών αναγνωριστικών και ο σχηματισμός μιας σχετικής ταυτότητας έχει καταστεί απαραίτητος στη σύγχρονη κοινωνία**. Αφού η ταυτότητα του προσώπου λειτουργεί ως τεκμήριο για την προστασία του, προκειμένου να αποδείξει, και να διεκδικήσει διάφορα οφέλη, προνόμια και δικαιώματα Ωστόσο, δεν αρκούν όλα αυτά τα προσδιοριστικά χαρακτηριστικά του προσώπου, για να επαληθευτεί η ταυτότητα του αλλά η επαλήθευση αυτή, επιτυγχάνεται **μέσω ενός εγγράφου ταυτοποίησης το οποίο εμπεριέχει όλες τις απαραίτητες, έγκυρες πληροφορίες που απαιτούνται ως αποδεικτικά στοιχεία για την επαλήθευση της ταυτότητάς του**[2]. Έτσι, στη σύγχρονη εποχή, η ταυτότητα έχει μετατραπεί από κάτι άυλο σε κάτι απτό που μπορεί να αποδειχθεί, μέσω φυσικών δελτίων ταυτότητας ή άλλων πιστοποιητικών, όπως το πιστοποιητικό γέννησης, το διαβατήριο και οι άδειες οδήγησης. Τα έγγραφα αυτά επί δεκαετίες θεωρούνταν επαρκή, όμως οι τεχνολογικές εξελίξεις υπονομεύουν την ακεραιότητα του συμβατικού τύπου πιστοποίησης της ταυτότητας των προσώπων(λ.χ. πλαστογραφία), με αποτέλεσμα τόσοο έλεγχος, όσο και η επαλήθευση της ταυτότητας να αντιμετωπίζουν ζητήματα εγκυρότητας και αξιοπιστίας της γνησιότητας.

[2] J. Blue, J. Condell, (2017), ‘’Identity Document Authentication using Steganographic Techniques: The Challenges of Noise’’, Ulster University, 28th Irish Systems and Signals Conference, Killarney, Ireland.

Για την ελαχιστοποίηση του κινδύνου πλαστής τεκμηρίωσης της ταυτότητας ενός προσώπου, έχουν αναπτυχθεί ανθεκτικοί μηχανισμοί ασφαλούς ελέγχου της ταυτότητας του ατόμου.[3] Για την επίτευξη του σκοπού αυτού, έχουν αναπτυχθεί μία σειρά τύπων, χαρακτηριστικών ασφαλείας και επαλήθευσης, της ταυτότητας. Δεν αρκεί, όμως, η ύπαρξη ενός φυσικού αρχείου, λ.χ. ενός δελτίου ταυτότητας, που ενώ δύναται να επαληθεύεται η γνησιότητα της κάρτας, αλλά όχι και η ταυτότητα του προσώπου που εμφανίζεται στην κάρτα. **Για να επιτευχθεί η πλήρης αντιστοίχιση ενός προσώπου, η κάρτα θα έπρεπε να διασυνδεθεί με ένα κεντρικό αποθετήριο σε πραγματικό χρόνο (on-line), ώστε να επαληθεύσει ότι το άτομο είναι όντως εξουσιοδοτημένο για την κατοχή του δελτίου ταυτότητάς, επαληθεύοντας έτσι, τη σύνδεση του κατόχου της κάρτας με την αντίστοιχη κάρτα**.

Παράλληλα ανακύπτουν ζητήματα **κυβερνοασφάλειας** όπως για παράδειγμα οι **προσπάθειες παράνομης απόκτησης προσωπικών πληροφοριών που αφορούν την ταυτότητα ενός προσώπου καθώς και η περαιτέρω χρήση των πληροφοριών αυτών, για τη δημιουργία πλαστής ταυτότητας**, μέσω πλαστών στοιχείων. Σε μία προσπάθεια εξάλειψης του φαινομένου αυτού, πολλά κράτη αναγκάζονται να ζητούν από τα άτομα να αποδείξουν ότι διαθέτουν πραγματική ταυτότητα, καθώς και να αναζητούν εναλλακτικούς ψηφιακούς τρόπους ταυτοποίησης, ως μεθόδου ελέγχου της ταυτότητας, προκειμένου να ενισχυθεί η εμπιστοσύνη των πολιτών, στην χρήση των ψηφιακών συναλλαγών. Επίσης, **εξετάζονται νέοι μέθοδοι για την επαλήθευση της ταυτότητας** τόσο με φυσικό όσο και με ηλεκτρονικό τρόπο.

3. Η λειτουργία της ψηφιακής ταυτότητας

Στη σύγχρονη εποχή, έχει γίνει η μετάβαση από την φυσική,στην δημόσια ψηφιακή ταυτότητα[4]. Εξάλλου, σήμερα, διανύουμε την εποχή της ολοένα αυξανόμενης αποϋλοποίησης των δημοσίων υπηρεσιών και της μετάβασης στην εποχή της ψηφιακής συνδιαλλαγής με τη δημόσια διοίκηση. Στο πλαίσιο αυτό, οι ψηφιακές ταυτότητες αποτελούν το εργαλείο για την ενδυνάμωση του δεσμού του πολίτη με το κράτος, ώστε να αντιμετωπίζεται ως δημόσιο αγαθό, το οποίο πρέπει να είναι προσβάσιμο σε όλους.

Η ψηφιακή ταυτότητα είναι, ως επί το πλείστον, μια προσπάθεια, να ξαναδημιουργηθούν, να ενσωματωθούν και να οργανωθούν τα δικαιώματα και οι υποχρεώσεις κάθε φυσικού προσώπου, σε όλους τους τομείς, στον διαδικτυακό ηλεκτρονικό κόσμο και να τα συνδέσει μεταξύ τους, σε υπάρχουσες «offline» ταυτότητες. Η ψηφιακή ταυτότητα εστιάζει κυρίως στην ανάπτυξη της ψηφιακής διακυβέρνησης, στη βελτίωσης της καθημερινής ζωής του πολίτη και στη διευκόλυνση των ηλεκτρονικών συναλλαγών τόσο στο δημόσιο όσο και στον

[3] J. Blue, J. Condell, (2018), 'Identity Document Authentication using Steganographic Techniques: The Challenges of Noise', Ulster University, 28th Irish Systems and Signals Conference, Killarney, Ireland.

[4] République Française. Identités numériques. Clés de voûte de la citoyenneté numérique. Rapport. Juin 2020.
GREFFET, Fabienne, WOJCIK, Stéphanie, «La citoyenneté numérique. Perspectives de recherche », Réseaux, 2014/2 (n° 184-185), p. 125-159.

ιδιωτικό τομέα. Η βελτίωση αυτή μπορεί να περιλαμβάνει διάφορα χαρακτηριστικά όπως ψηφιακά πιστοποιητικά, έξυπνες κάρτες, δομή δημοσίου κλειδιού, ρόλους και προνόμια, αυθεντικοποίηση και διαδικασίες έγκρισης. Η παρούσα αναγέννηση του διαδικτύου, που βασίζεται στις διαδικτυακές υπηρεσίες και στην πρόβλεψη ορίζει και δημιουργεί ένα νέο σύνολο ευκαιριών, όχι μόνο για τις επιχειρήσεις και τις κυβερνήσεις, αλλά και για τους ανθρώπουςσυμπεριλαμβανομένης της διαθεσιμότητας νέων διαδικτυακών υπηρεσιών και την ξεδίπλωση δομών που επιτρέπουν τις ηλεκτρονικές συναλλαγές.

Για τη λειτουργία της ψηφιακής ταυτότητας απαραίτητο είναι το τρίπτυχο, χρήστης, πάροχος και τρίτος πάροχος υπηρεσιών εμπιστοσύνης.

Ο **χρήστης** αποτελεί το φυσικό πρόσωπο που επιθυμεί να έχει πρόσβαση σε σύνολο ψηφιακών υπηρεσιών, του δημόσιου και του ιδιωτικού τομέα. Σε κάθε περίπτωση, επιδίωξη αποτελεί η ευκολία στη χρήση των υπηρεσιών αυτών (User Interface U.I και User Experience U.X), ασφάλεια των συναλλαγών του και προστασία των προσωπικών του δεδομένων.

Ο **πάροχος** δίνει τη δυνατότητα πρόσβασης στους χρήστες, ενώ η πρόσβαση του χρήστη επιτυγχάνεται μετά από προηγούμενη αυθεντικοποίηση του.

Επίσης, ο **πάροχος υπηρεσιών εμπιστοσύνης** αποτελεί το διαμεσολαβητή, που χορηγεί πρόσθετα κλειδιά, για τη διασφάλιση ενός ισχυρού και ασφαλούς επιπέδου αυθεντικοποίησης.

3.1. Οι τρεις φάσεις ζωής της ψηφιακής ταυτότητας: εγγραφή, αυθεντικοποίηση και χρήση .

Η ψηφιακή ταυτότητας προϋποθέτει τη διέλευση από τρεις φάσεις, ήτοι την εγγραφή που αντιστοιχεί στην καταχώρηση των προσωπικών στοιχείων, την αυθεντικοποίηση και τη χρήση. Είναι η στιγμή κατά την οποία η αρχή που «παραδίδει» την ψηφιακή ταυτότητα θεμελιώνει, με τρόπο σίγουρο τη σχέση ανάμεσα στον χρήστη και στην ψηφιακή ταυτότητα . Το επίπεδο ασφάλειας ποικίλλει ανάλογα με τον τρόπο της εγγραφής. Η διαδικασία της εγγραφής μπορεί, να περιλαμβάνει τη χορήγηση αναγνωριστικών, ενός password, ενός κινητού τηλεφώνου και μιας διεύθυνσης e-mail ή περισσότερων στοιχείων, για να ολοκληρωθεί η επιβεβαίωση σε ένα επίπεδο ασφαλείας πιο υψηλό.

Η φάση της εγγραφής είναι, σημαντική για την εξασφάλιση του επιπέδου ασφαλείας της χορηγούμενης ψηφιακής ταυτότητας.

3.2. Η χρήση της ψηφιακής ταυτότητας

Η χρήση της ψηφιακής ταυτότητας αναφέρεται στην είσοδο του χρήστη σε μια πληθώρα υπηρεσιών, από τη στιγμή που η αυθεντικοποίηση είναι επιτυχής.

Εμπλεκόμενοι στη διαδικασία ψηφιακής ταυτοποίησης μπορεί να είναι τόσο ο δημόσιος όσο και ο ιδιωτικός τομέας - ο δεύτερος, υπό τη μορφή παρόχων ψηφιακής ταυτότητας.

Η συνεργασία Ιδιωτικού και Δημόσιου τομέα για την έκδοση και τη λειτουργία της ψηφιακής ταυτότητας είναι απαραίτητος.

Έτσι, με την αξιοποίηση της ψηφιακής ταυτότητας διευκολύνεται η πρόσβαση των πολιτών σε ένα σύνολο υπαρχουσών και νέων υπηρεσιών.

3.2.α Ψηφιακή Ταυτότητα

Είναι χαρακτηριστικό ότι, το 1993, ο σκιτσογράφος Peter Steiner δημιούργησε μια γελοιογραφία για το περιοδικό «The New Yorker» που ισχυριζόταν ότι «**Στο διαδίκτυο, κανείς δεν ξέρει ότι είσαι σκύλος**», επισημαίνοντας με διορατικότητα ότι θεωρητικά, πίσω από μία ψηφιακή ταυτότητα μπορεί να κρύβεται οτιδήποτε, ακόμα και ένας σκύλος…[5]

Η ψηφιακή ταυτότητα **μπορεί να είναι μεταβλητή και ένα άτομο να διαθέτει περισσότερες ψηφιακές ταυτότητες στο Διαδίκτυο για διάφορους λόγους**.Όπως διαφορετικά e-mails, προσωπικά οικονομικά ή μέσα κοινωνικής δικτύωσης. Ωστόσο, έχει ιδιαίτερη βαρύτητα η ψηφιακή ταυτότητα του ατόμου για την **πρόσβαση του τόσο σε ψηφιακές υπηρεσίες «χαμηλού κινδύνου»**, όπου η απόδειξη της ταυτότητας είναι μικρότερης σημασίας, καθώς επίσης και **σε «υψηλού κινδύνου»**, όπου απαιτείται το κατάλληλο επίπεδο εμπιστοσύνης, για να διαπιστωθεί ότι το φυσικό πρόσωπο -χρήστης είναι ο νόμιμος κάτοχος της ψηφιακής ταυτότητας. Επομένως, η **έννοια «ψηφιακή ταυτότητα»** αναφέρεται στη μοναδική αναπαράσταση ενός υποκειμένου που συμμετέχει σε μία ψηφιακή/ διαδικτυακή συναλλαγή[6].

Ωστόσο, μια ψηφιακή ταυτότητα μπορεί ή όχι να σχετίζεται με την πραγματική ταυτότητα ενός υποκειμένου και μπορεί επίσης να σχετίζεται με διάφορους οργανισμούς μέσω ηλεκτρονικών αρχείων, διαχείρισης πρόσβασης ταυτότητας, ψηφιακών υπογραφών και πιστοποιητικών και υπό πολλές άλλες διαδικτυακές συνθήκες.

Ο **όρος** «**απόδειξη ταυτότητας**» χρησιμοποιείται για να περιγράψει τη διαδικασία διαπίστωσης ότι ένα υποκείμενο που έχει πρόσβαση σε ψηφιακές υπηρεσίες είναι όντως αυτό που ισχυρίζεται ότι είναι. **Ψηφιακός έλεγχος ταυτότητας είναι ο όρος που χρησιμοποιείται, για να περιγράψει τη διαδικασία που αποδεικνύει ότι ένα υποκείμενο που επιχειρεί να αποκτήσει πρόσβαση σε μια ψηφιακή υπηρεσία έχει τον έλεγχο ενός**

[5] M. Cavna, (2013), '"NOBODY KNOWS YOU'RE A DOG': As iconic Internet cartoon turns 20, creator Peter Steiner knows the joke rings as relevant as ever', The Washington Post, (online) https://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31/73372600-f98d-11e2-8e84-c56731a202fb_blog.html?noredirect=on&utm_term=.1838265bcd92

[6] National Institute for Standards and Technology, (2017), 'Digital Identity Guidelines', NIST Special Publication 800-63-3, June, 2017.

έγκυρου εργαλείου ελέγχου ταυτότητας που σχετίζεται με την ψηφιακή ταυτότητα αυτού του υποκειμένου.

3.2.β Ψηφιακό αποτύπωμα

Ο **όρος «ψηφιακό αποτύπωμα»** χρησιμοποιείται συχνά εναλλακτικά με την «ψηφιακή ταυτότητα», ωστόσο υπάρχουν αξιοσημείωτες διαφορές μεταξύ των δύο.

Το ψηφιακό αποτύπωμα αντιπροσωπεύει την online παρουσία ενός ατόμου και παρέχει στοιχεία της ψηφιακής και πραγματικής ταυτότητάς του. Καταγράφει τα ίχνη και τα δεδομένα ή και μεταδεδομένα που άφησαν πίσω τους άτομα που αλληλεπιδρούν σε ένα ψηφιακό περιβάλλον.

Τα ψηφιακά αποτυπώματα είναι επίμονα και διαχρονικά και συνδέουν το παρελθόν με το παρόν, ανεξάρτητα από τις μεταβάσεις και τις αλλαγές στη ζωή ενός ατόμου. Απαιτούν πολλούς συμμετέχοντες, καθώς πραγματοποιείται σύνδεση με άλλους χρήστες (φυσικά ή νομικά πρόσωπα) η οποία ενισχύεται μέσω ηλεκτρονικών αρχείων όπως, ειδοποιήσεις e-mail, ψηφιακές αποδείξεις και μεταδεδομένα, που αποτελούν στοιχεία του ψηφιακού αποτυπώματος τα οποία χρησιμοποιούνται για τον εντοπισμό και την καταγραφή κάθε διαδικτυακής κίνησης.

3.2.γ Ηλεκτρονική Ταυτοποίηση (e-Identification)

Ως στοιχείο της «ηλεκτρονικής διακυβέρνησης», η ηλεκτρονική ταυτοποίηση αναφέρεται, σε μεγάλο βαθμό σε ηλεκτρονικά αρχεία που περιέχουν δεδομένα που σχετίζονται με πολίτες ενός κράτους. Εκτός από την ηλεκτρονική πρόσβαση και τον έλεγχο ταυτότητας για κρατικές υπηρεσίες, αυτός ο τύπος ψηφιακής εγγραφής συνδέεται με ένα φυσικό έγγραφο που περιέχει ένα τσιπ το οποίο επαληθεύει την ταυτότητα του κατόχου του εγγράφου.

Για το λόγο αυτό, το e-ID σε όλες τις μορφές του θεωρείται τυπικός έλεγχος ταυτότητας δύο παραγόντων, όπου ένα υποκείμενο «έχει» κάτι και «γνωρίζει» έναν κωδικό πρόσβασης για να επαληθεύσει την ταυτότητά του. Έτσι, αυτή η τεχνολογία είναι ένας συνδυασμός παραδοσιακής τεκμηρίωσης αναγνώρισης και IAM.

3.3 Αρχεία Ταυτότητας και Διαχείριση

Λαμβάνοντας υπόψη τον υπερπληθυσμό του πλανήτη, που αναμένεται έως το 2050 να ανέλθει στα 9,6 δισεκατομμύρια, οι κυβερνητικοί φορείς προσπαθούν να εφαρμόσουν συστήματα που θα επιτρέπουν τη διαφοροποίηση των ατόμων. Έτσι, οι

πολίτες διαθέτουν ένα μοναδικό σύνολο προσωπικών αναγνωριστικών που, στη συνέχεια, αποθηκεύονται σε διάφορους τύπους συστημάτων διαχείρισης ταυτότητας. **Έτσι αναζητούνται τεχνικές ανάλυσης της ταυτότητας για τον εντοπισμό δύο ξεχωριστών εγγραφών που αφορούν το ίδιο άτομο στον πραγματικό κόσμο, όπως τύπους προσωπικών αναγνωριστικών και διαχείριση αρχείων ταυτότητας.**

3.3.α. Προσωπικά αναγνωριστικά

Ένα πρώτο εργαλείο προς την κατεύθυνση αυτή είναι τα προσωπικά αναγνωριστικά του ατόμου. Εξάλλου, η πραγματική ταυτότητα ενός προσώπου αποτελείται από μία προσωπική ταυτότητα που αντιστοιχεί σε τυπικά χαρακτηριστικά και μία κοινωνική ταυτότητα.

Η προσωπική ταυτότητα αποκτάται από τη γέννηση και περιλαμβάνει αναγνωριστικά, όπως το όνομα και η ημερομηνία γέννησης, επίσημα εκχωρημένα αναγνωριστικά, όπως αριθμός κοινωνικής ασφάλισης, τρέχουσες φυσικές περιγραφές, όπως το ύψος και το βάρος, καθώς και βιομετρικά δεδομένα, όπως τα δακτυλικά αποτυπώματα.

Η κοινωνική ταυτότητα είναι η βιογραφική ιστορία ενός ατόμου, που συγκεντρώνεται κατά τη διάρκεια της ζωής του, περιγράφοντας το κοινωνικό πλαίσιο της εμπειρίας της ζωής του. Οι πληροφορίες κοινωνικού πλαισίου αναφέρονται στη «φήμη» που έχει αποκτήσει ένα άτομο με την πάροδο του χρόνου, συμπεριλαμβανομένου του ιστορικού απασχόλησης, του πιστωτικού ιστορικού, των δικτύων φιλίας και των οικογενειακών σχέσεων.

3.3.β Βιομετρικά αναγνωριστικά

Ο όρος «βιομετρική» αναφέρεται σε μια διαδικασία όπου τα βιολογικά χαρακτηριστικά ενός ατόμου μετρώνται και αναλύονται, για να αποδειχθεί η ταυτότητα. Αυτό μπορεί να περιλαμβάνει φυσικά χαρακτηριστικά, όπως δακτυλικά αποτυπώματα, μοτίβα ίριδας/ αμφιβληστροειδούς και γεωμετρία χεριών ή χαρακτηριστικά συμπεριφοράς, όπως φωνή, γραφή και βάδισμα. Η αρχή της χρήσης φυσικών ή συμπεριφορικών δεδομένων στην ταυτοποίηση βασίζεται ουσιαστικά στην ιδέα ότι κάθε άτομο είναι μοναδικό και, επομένως, μπορεί να αναγνωριστεί από τα μοναδικά ατομικά του χαρακτηριστικά. Η απόκτηση μπορεί να επιτευχθεί με τη χρήση συσκευών τύπου σαρωτή/αναγνώστη, ορισμένες από τις οποίες είναι πιο παρεμβατικές από άλλες, ανάλογα με τον τύπο των δεδομένων που συλλέγονται. Μετά την απόκτηση, το αναλογικό σήμα ψηφιοποιείται και αποθηκεύεται σε μια βάση δεδομένων ελέγχου ταυτότητας. Τα τελευταία χρόνια, οι βιομετρικές τεχνολογίες ασφάλειας έχουν προχωρήσει τόσο, ώστε να επιτρέπουν σχεδόν στιγμιαία αναγνώριση.

Οι τεχνολογίες για βιομετρικά χαρακτηριστικά που είναι σήμερα εμπορικά διαθέσιμες έχουν αρκετά απτά οφέλη, το κόστος έχει μειωθεί πολύ, οι συσκευές είναι μικρές και

συνολικά είναι σχετικά εύκολο να ενσωματωθούν. Τα εργαλεία βιομετρικής αναγνώρισης θεωρούνται βολικά και πιο ασφαλή από εναλλακτικές μεθόδους, όπως οι κωδικοί πρόσβασης, καλύπτοντας επομένως την ανάγκη για ισχυρό έλεγχο ταυτότητας. Αυτό είχε ως αποτέλεσμα την αυξημένη χρήση της τεχνολογίας βιομετρικής ασφάλειας από κυβερνήσεις, χρηματοπιστωτικά ιδρύματα και άλλους οργανισμούς.

Έτσι, έχει διαμορφωθεί ένα σενάριο όπου τα άτομα είναι πλέον υποχρεωμένα να παρέχουν τις βιολογικές τους πληροφορίες για τυπικούς σκοπούς ταυτοποίησης. Ωστόσο, η υποχρεωτική παροχή προσωπικών βιομετρικών πληροφοριών εγείρει πολλά νομικά, ηθικά και κοινωνικά ζητήματα σε σχέση με την απόκτηση, τον σκοπό και την αποθήκευση των δεδομένων.

3.3.γ Κοινωνικά αναγνωριστικά

Οι θεωρίες κοινωνικής ταυτότητας εξετάζουν τόσο τις ψυχολογικές όσο και τις κοινωνιολογικές πτυχές της ύπαρξης ενός ατόμου. **Η κοινωνική ταυτότητα ενός ατόμου και η αλληλεπίδρασή του με τον κόσμο ορίζεται από την ψυχολογική άποψη**. Οι διαπροσωπικές σχέσεις που βασίζονται σε ρόλους μεταξύ «κοινωνικών παραγόντων», όπως δάσκαλος-μαθητής και εργοδότης-εργαζόμενος τονίζονται από την κοινωνιολογική άποψη. Ο συνδυασμός αυτών των απόψεων επιτρέπει μια πιο ολοκληρωμένη κατανόηση της κοινωνικής ταυτότητας.

Έρευνα που διεξήχθη στον τομέα της ταυτότητας από τους Wang et al. έχει υποδείξει ότι η **χρήση πρόσθετων μη τυπικών χαρακτηριστικών που σχετίζονται με την κοινωνική συμπεριφορά ενός ατόμου μπορεί να συμβάλει στον έλεγχο ταυτότητας ή στη διάψευση ταυτοτήτων κατά την προσπάθεια αναγνώρισης μοναδικών ατόμων που έχουν κοινά χαρακτηριστικά**[7].

Παραδοσιακά, τα τυπικά χαρακτηριστικά προσωπικής ταυτότητας στα συστήματα διαχείρισης αρχείων χρησιμοποιήθηκαν για τη διαφοροποίηση μεταξύ ατόμων. Ωστόσο, η ποιότητα των δεδομένων μπορεί να επηρεάσει αυτά τα χαρακτηριστικά. Τα βιομετρικά δεδομένα είναι δυνητικά πιο αξιόπιστα ως αναγνωριστικά, ωστόσο λόγω υψηλού κόστους και ζητημάτων εμπιστευτικότητας, οι συγκεκριμένες πληροφορίες, συχνά δεν είναι διαθέσιμες.

Το Υπουργείο Εσωτερικών του Ηνωμένου Βασιλείου διεξήγαγε μια μελέτη για την απάτη ταυτότητας[8] και κατέδειξε ότι τα εγκλήματα που αφορούσαν την ταυτότητα συνήθως περιλάμβαναν αρχεία όπου παραδοσιακά προσωπικά αναγνωριστικά χρησιμοποιήθηκαν ή

[7] G.A. Wang, H.C. Chen, J..J. Xu and H. Atabakhsh, (2006), 'Automatically detecting criminal identity deception: an adaptive detection algorithm', IEEE Transport Systems Management, Part A-Systems Humans 36, pp. 988–999.

[8] United Kingdom Home Office, (2002), 'Identity Fraud: A Study', (online) http://www.homeoffice.gov.uk/cpd/id_fraud-report.pdf

τροποποιήθηκαν παράνομα. Κατά την απόκλιση από τη χρήση των παραδοσιακών αναγνωριστικών, το κοινωνικό πλαίσιο ενός ατόμου θα πρέπει να διαθέτει χαρακτηριστικά που πιστοποιούν την αναμφισβήτητη ταυτότητά του.

Πρόσφατες μελέτες έχουν αναγνωρίσει την αξία των δεδομένων κοινωνικού πλαισίου, όπως οι σχέσεις και οι κοινωνικές συμπεριφορές στην επίλυση ταυτότητας. Για παράδειγμα, οι Köpcke και Rahm[9] επινόησαν ένα κατηγορηματικό σχήμα που βασιζόμενοι σε αντιστοιχίσεις χαρακτηριστικών-τιμών αποκλειστικά περιγραφικού τύπου ώστε να εξετάσουν δεδομένα που συλλέγονται από συνδέσμους κοινωνικής αλληλεπίδρασης.

Η τάση προς την ψηφιοποιημένη ύπαρξη και η αυξανόμενη δημοτικότητα των πλατφορμών μέσων κοινωνικής δικτύωσης, όπως το Facebook, το Twitter και το Instagram, έχουν σίγουρα διευκολύνει τη στροφή προς τη χρήση και των δύο τυπικών προσωπικών αναγνωριστικών εκτός από πληροφορίες κοινωνικού περιεχομένου για τη διαφοροποίηση μεταξύ ατόμων που μοιράζονται χαρακτηριστικά, όπως όνομα, ημερομηνία γέννησης και κατοικημένη περιοχή μεταξύ άλλων.

3.4. Αρχεία Ταυτότητας και Συστήματα Διαχείρισης

Η τεχνολογία έχει βελτιώσει τον τρόπο με τον οποίο καταγράφονται και αποδεικνύονται οι ταυτότητες, με τους οργανισμούς να βασίζονται περισσότερο σε ηλεκτρονικά αρχεία για να εκτελέσουν το ίδιο. Το ISO/IEC 24760-1 ορίζει την ταυτότητα ως **«σύνολο χαρακτηριστικών που σχετίζονται με μια οντότητα»**. Οι πληροφορίες που περιέχονται σε ένα ψηφιακό αρχείο επιτρέπουν την αξιολόγηση και τον έλεγχο ταυτότητας ατόμων που αλληλεπιδρούν με οργανισμούς, συχνά χωρίς τη συμμετοχή ανθρώπινων χειριστών[10]. **Τα κρατικά αρχεία ορίζονται ως καταγεγραμμένες πληροφορίες σε οποιαδήποτε μορφή, που δημιουργούνται ή λαμβάνονται κατά τη διεξαγωγή κρατικών εργασιών και τηρούνται ως αποδεικτικά στοιχεία δραστηριοτήτων και συναλλαγών.** Αυτός ο ορισμός δίνει έμφαση στον σκοπό και όχι στη φυσική μορφή ή το μέσο εγγραφής. Ο ορισμός περιλαμβάνει παραδοσιακά έντυπα αρχεία και αρχεία σε όλες τις άλλες μορφές, συμπεριλαμβανομένων των ηλεκτρονικών.

Η διαχείριση αρχείων αναφέρεται παραδοσιακά στις πολιτικές και τις διαδικασίες ενός οργανισμού για τη διαχείριση συστημάτων αρχείων και την απόρριψη των εγγραφών, όταν δεν χρειάζονται πλέον. Τα τελευταία χρόνια, η προσοχή έχει μετατοπιστεί στην ανάγκη δημιουργίας αξιόπιστων και επικαιροποιημένων αρχείων δεδομένων σε ηλεκτρονική μορφή και η «διαχείριση αρχείων» κατανοείται ευρύτερα ως η συνολική διαχείριση των αρχείων από την αρχική τους δημιουργία έως την τελική τους διάθεση. Τα αρχεία αυτά

[9] H. Köpcke and E. Rahm, (2010), 'Frameworks for entity matching: a comparison'. Data and Knowledge Engineering, Elsevier, Volume 69, Issue 2, page 197–210.

[10] International organization for Standardization, (2011), 'Information technology - Security techniques - A framework for identity management -- Part 1: Terminology and concepts', ISO/IEC 24760-1.

διακρίνονται από τεράστιο όγκο και πολυπλοκότητα και η ευχερής τους χρήση εξαρτάται από την ταχύτητα εύρεσης των απαραίτητων κάθε φορά στοιχείων.

Η επικύρωση επιτρέπει τον εντοπισμό των πλαστών, διπλών και εσφαλμένων αρχείων στο πλαίσιο των συστημάτων διαχείρισης αρχείων ταυτότητας, αλλά πολλά σχήματα ταυτότητας δεν διαθέτουν την απαιτούμενη ακεραιότητα, για την επαλήθευση με ορθό τρόπο της ταυτότητας.

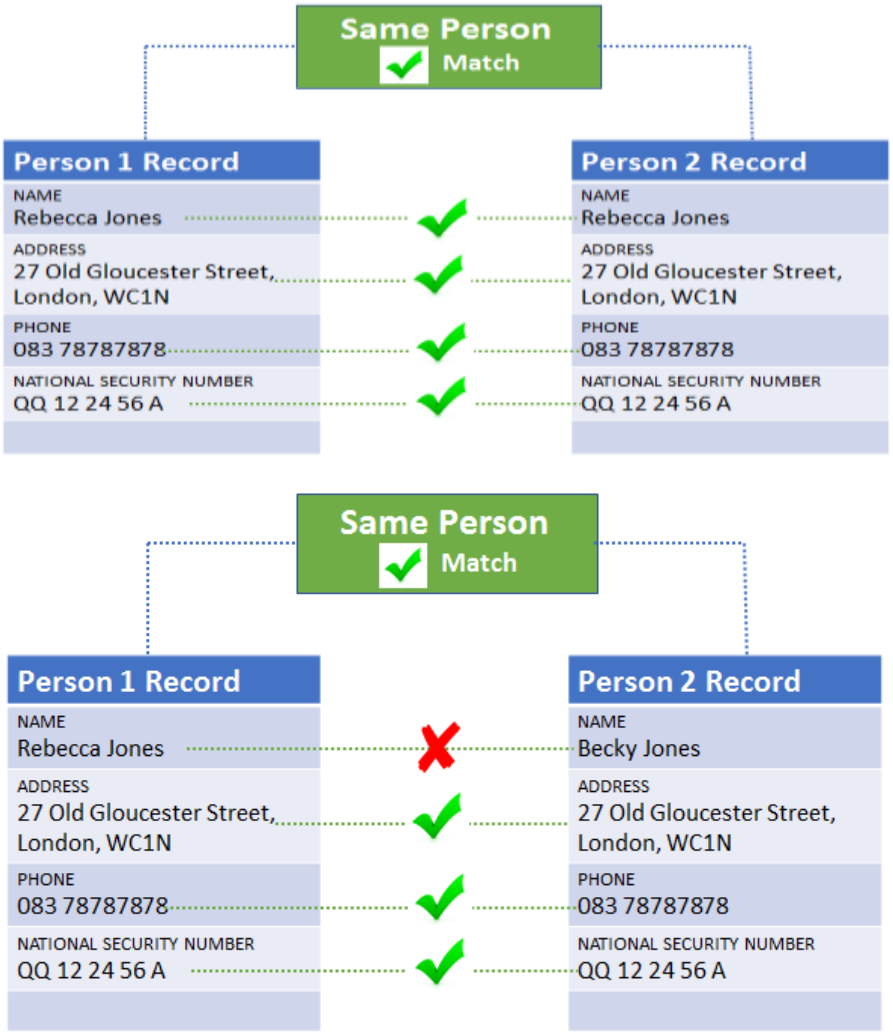
3.4.α Ανάλυση Ταυτότητας

Η ανάλυση ταυτότητας είναι μια διαδικασία που ερευνά εάν μια μεμονωμένη ταυτότητα είναι η ίδια, όταν περιγράφεται διαφορετικά. Ο στόχος της ανάλυσης ταυτότητας είναι να ανιχνεύσει αρχεία ταυτότητας που αφορούν το ίδιο άτομο. Ερευνητές βάσεων δεδομένων και στατιστικής έχουν προτείνει μια πληθώρα τεχνικών μέτρων για την εφαρμογή μορφών ανάλυσης ταυτότητας.

Παραδοσιακά, οι τεχνικές αυτές βασίζονται σε βασικά χαρακτηριστικά, όπως αριθμούς αναγνώρισης, τα ονόματα και την ημερομηνία γέννησης προκειμένου να υλοποιηθεί ο εντοπισμός αντιστοιχιών μεταξύ των εγγραφών. Τα κοινά αυτά χαρακτηριστικά λειτουργούν ως απλοί περιγραφείς ενός ατόμου, τα περισσότερα άτομα τα διαθέτουν και είναι διαθέσιμα στα περισσότερα συστήματα διαχείρισης αρχείων. Ωστόσο, τα ίδια χαρακτηριστικά ταυτότητας ποικίλλουνκαι διακρίνονται, ως προς τη διαθεσιμότητα και την αξιοπιστία τους στα ετερογενή συστήματα. Λόγω λανθασμένης ή/ και απουσίας εισαγωγής δεδομένων, δεν μπορούμε να βασιστούμε αποκλειστικά στην ακρίβεια των χαρακτηριστικών αυτών και, επομένως, δεν παρουσιάζουν μια αξιόπιστη πηγή πληροφοριών βάσει της οποίας μπορεί να πραγματοποιηθεί έλεγχος ταυτότητας.

Η ανάλυση ταυτότητας μπορεί να χρησιμοποιηθεί, για να προσδιοριστεί εάν μια μεμονωμένη ταυτότητα έχει αντιγραφεί, όταν περιγράφεται από παραλλαγμένα προσωπικά αναγνωριστικά σε ξεχωριστές εγγραφές, με στόχο την ανίχνευση εγγραφών ταυτότητας που αναφέρονται σε ένα μεμονωμένο άτομο, όπως απεικονίζεται στην Εικόνα 1. Σε μια προσπάθεια βελτίωσης της ακρίβειας για τον εντοπισμό διπλότυπων και δυνητικά πλαστών ταυτοτήτων, οι τεχνικές ανάλυσης που προτάθηκαν πρόσφατα εξέτασαν τη χρήση πρόσθετων χαρακτηριστικών που μπορεί, επίσης, να συμβάλουν στον έλεγχο ταυτότητας ή στη διάψευση ταυτοτήτων, όπως οι πληροφορίες κοινωνικού περιεχομένου.

Οι τύποι χαρακτηριστικών και μέθοδοι αντιστοίχισης αρχείων έχουν διαφορετικό βαθμό αποτελεσματικότητας, όταν λειτουργούν ως μέσο για τον εντοπισμό διπλότυπων και δυνητικά πλαστών ταυτοτήτων σε ετερογενή συστήματα διαχείρισης ταυτότητας. Τα χαρακτηριστικά ταυτότητας παρέχουν πολύτιμες διαβεβαιώσεις κατά τη διεξαγωγή υπολογιστικής ανάλυσης ταυτότητας, ειδικά όταν λαμβάνονται υπόψη τόσο τα χαρακτηριστικά προσωπικής ταυτότητας όσο και τα χαρακτηριστικά κοινωνικής ταυτότητας. Οι τρέχουσες τεχνικές αντιστοίχισης περιλαμβάνουν αντιστοίχιση κατά ζεύγη, μεταβατικό κλείσιμο και συλλογική ομαδοποίηση.



Εικόνα 1: Ανάλυση ταυτότητας πανομοιότυπων και μη ταυτόσημων διπλών εγγραφών

4. Τεκμηρίωση ταυτότητας και έλεγχος ταυτότητας

Οι **τάσεις** στην τεκμηρίωση ταυτότητας έχουν μεταμορφωθεί με την πάροδο του χρόνου, σε κάθε στάδιο, δίνοντας έμφαση στους διαθέσιμους πόρους και την τεχνολογία. Το γεγονός αυτό, δημιουργεί πληθώρα παραλλαγών και αποδεκτών μορφών **τεκμηρίωσης που μπορούν να χρησιμοποιηθούν για την επαλήθευση μιας ταυτότητας.**

Η ενότητα αυτή εξετάζει διάφορες εφαρμογές τεκμηρίωσης ταυτοποίησης. Οι εφαρμογές αυτές κυμαίνονται από παραδοσιακά έντυπα έγγραφα και ηλεκτρονικές υλοποιήσεις όπως e-ID, ePassports και eBorders, έως πιο πρόσφατες ψηφιακές υλοποιήσεις που περιλαμβάνουν σύστημα υπολογιστή Identity Access Management (IAM), Identity-as-a-Service, ψηφιακές υπογραφές και ψηφιακά πιστοποιητικά.

4.1.Τεκμηρίωση παραδοσιακής ταυτότητας σε χαρτί

Επί του παρόντος, οι κυβερνήσεις, τα χρηματοπιστωτικά ιδρύματα και άλλοι επίσημοι οργανισμοί βασίζονται σε μεγάλο βαθμό στην ικανότητα ενός ατόμου να παράγει έντυπη τεκμηρίωση που μπορεί να επαληθεύσει την υποτιθέμενη ταυτότητά του. Αυτό βασίζεται σε πρωτογενείς πόρους που ήταν διαθέσιμοι από το δεύτερο μισό του 19ου αιώνα μέχρι τις σημερινές εφαρμογές. **Η έντυπη τεκμηρίωση ταυτότητας μπορεί να κυμαίνεται από πιστοποιητικά γέννησης, άδειες οδήγησης και τα διαβατήρια μέχρι άλλα έγγραφα που είναι «δύσκολο» να αποκτηθούν, όπως αρχεία εκπαίδευσης και υγείας, τίτλοι ιδιοκτησίας γης και αποδεικτικά στοιχεία λογαριασμών κοινής ωφελείας.** Ανάλογα με τον τύπο της τεκμηρίωσης που διαθέτει ένα άτομο, ενδέχεται να του ζητηθεί να προσκομίσει περαιτέρω «αποδεικτικά στοιχεία» προκειμένου να εξακριβωθεί ότι διαθέτει έγκυρη ταυτότητα.

Την περίοδο όπου δεν ήταν αρκετά ανεπτυγμένη η τεχνολογία των εκτυπώσεων τα έγγραφα ταυτοποίησης ήταν σε μεγάλο βαθμό χειρόγραφα και επαληθεύονταν από ένα έγκυρο άτομο που εκπροσωπούσε έναν επίσημο οργανισμό. Στησύγχρονη εποχή τα έγγραφα αυτά και δεν θεωρούνται πλέον αξιόπιστα, χωρίς περαιτέρω αποδεικτικά στοιχεία ταυτότητας. Μετά τη βιομηχανική εποχή, οι τεχνολογικές εξελίξεις επιτρέπουν την μαζική εκτύπωση και την ευρεία διάδοση και χρήση εγγράφων με άμεση εμφάνιση αναγνωριστικών , όπως όνομα, ημερομηνία γέννησης ακόμη και φωτογραφίες ενός ατόμου και για την περαιτέρω προστασία της γνησιότητας της έντυπης τεκμηρίωσης. Στον παρακάτω Πίνακα, Εικόνα 2 παρουσιάζονται τα επίπεδα ασφαλείας με ορισμένα χαρακτηριστικά και παραδείγματα για τις αντίστοιχες κατηγορίες.

Security Level	Attributes	Examples
Level 1: Overt	• Basic requirement • Lowest level security • Visual verification via discernible features • Overtly printed features • Characterised by method of production • Physical additives to card substrate and laminate	• Visible watermarks • Holograms • Fine printing • Fibres • Security laminates • Overt biographic data • Embossed ridges
Level 2: Covert	• Compliment level 1 features • Not readily perceivable • Requires basic specialist tools to capture, register and authenticate data (lighting, magnification)	• Smart chips • Contactless chips • Magnetic Stripes • Radio Frequency ID • UV Ink • Microprinting
Level 3: Forensic	• Optimum security • Complex & Specialized • Visually perceivable data combined with secret data • Requires specialist forensic tools to capture, register and authenticate data (unique algorithms) • Optimal schemes link to a real-time digital central repository	• Steganography • Barcodes • Qode, • QR Code • Nexcode • SecureText™

Εικόνα 2: Επίπεδα ασφάλειας εγγράφων ταυτότητας

4.2. Τεκμηρίωση Ηλεκτρονικής Διακυβέρνησης και Ηλεκτρονικής Ταυτοποίησης

Τις τελευταίες δεκαετίες, είναι διαδεδομένη η έμφαση στις πολιτικές που στηρίζονται στην «ηλεκτρονική διακυβέρνηση». Σε παγκόσμιο επίπεδο, οι κυβερνήσεις έχουν αναγνωρίσει πολλαπλά οφέλη όπως τόνωση της αποτελεσματικότητας στη διαχείριση έργων, μείωση του κόστους, διασπορά στην κατανομή κινδύνων, βελτίωση της ποιότητας των υπηρεσιών παρέχοντας υψηλή προστιθέμενη αξία και ενίσχυση της τεχνολογικής καινοτομίας στη χρήση ψηφιακών υποδομών και στην επιδίωξη πρωτοβουλιών ηλεκτρονικής διακυβέρνησης.

Μέσω αυτού του αυξανόμενου φαινομένου, παραδείγματα εφαρμογών ηλεκτρονικής διακυβέρνησης περιλαμβάνουν την ηλεκτρονική ταυτότητα, τα ηλεκτρονικά διαβατήρια και τα ηλεκτρονικά σύνορα ως μηχανισμούς διακυβέρνησης που θεσπίζονται στις πολιτικές ηλεκτρονικής διακυβέρνησης.

4.2.α. Ηλεκτρονική Αναγνώριση (e-ID)

Η ηλεκτρονική αναγνώριση (e-ID) αποτελεί βασικό παράδειγμα ανάπτυξης κοινών ψηφιακών υποδομών. Ο συγκεκριμένος τύπος ψηφιακής λύσης παρέχει απόδειξη ταυτότητας στους πολίτες, ώστε να πιστοποιούν εύκολα την ταυτότητά τους, όταν έχουν πρόσβαση σε παροχές ή υπηρεσίες που παρέχονται από κυβερνητικές αρχές,

χρηματοπιστωτικά ιδρύματα και άλλους οργανισμούς. Εκτός από τον διαδικτυακό έλεγχο ταυτότητας και τη σύνδεση, τα συστήματα αυτά μπορούν, να περιλαμβάνουν τη χρήση ψηφιακών υπογραφών που χρησιμοποιούνται για την «υπογραφή» ηλεκτρονικών εγγράφων.

Συνήθως, αυτός ο τύπος εγγράφου ταυτοποίησης λειτουργεί ως έλεγχος ταυτότητας δύο παραγόντων, καθώς στους χρήστες παρέχεται μια φυσική ταυτότητα που μπορεί να χρησιμοποιηθεί για έλεγχο ταυτότητας στο διαδίκτυο ακόμη και εκτός σύνδεσης. Η ηλεκτρονική αναγνώριση είναι ένα παράδειγμα τεχνολογίας έξυπνων καρτών που περιλαμβάνει φανερά εμφανιζόμενα προσωπικά αναγνωριστικά και διαθέτει παράλληλα ένα ενσωματωμένο μικροτσίπ RFID που αποθηκεύει προσωπικά αναγνωριστικά τα οποία σχετίζονται με το άτομο. Οι πληροφορίες αυτές μπορεί να περιλαμβάνουν εικόνες και βιομετρικές πληροφορίες, όπως δακτυλικά αποτυπώματα.

Ο τύπος συστήματος e-ID έχει εφαρμοστεί από μια πληθώρα χωρών σε όλη την Ευρώπη, τη Νότια Αμερική, την Ασία και τη Μέση Ανατολή.

Σύμφωνα με τον κανονισμό της Ε.Ε. για τις υπηρεσίες ηλεκτρονικής αναγνώρισης και εμπιστοσύνης (eIDAS), περιγράφεται ως ένα πανευρωπαϊκό σύστημα σύνδεσης**, όπου όλοι οι οργανισμοί που παρέχουν δημόσιες ψηφιακές υπηρεσίες σε ένα κράτος-μέλος της Ε.Ε. θα δέχονται ηλεκτρονική αναγνώριση από όλα τα κράτη-μέλη της Ε.Ε.** από τον Σεπτέμβριο του **2018**[11]. Τα e-IDs έχουν αξιολογηθεί από πολλές οπτικές γωνίες, συμπεριλαμβανομένων των τεχνολογικών αποφάσεων[12], της εμπιστοσύνης και της δημόσιας αξίας[13], της επιτήρησης[14] και της ασφάλειας[15]. Ένα άλλο σύνολο μελετών από τους Melin et al.[16] διαπίστωσε ότι υπάρχουν σημαντικές προκλήσεις που εμπλέκονται στη διαχείριση του e-ID, κυρίως, λόγω θεμάτων που σχετίζονται με την τεχνολογική ολοκλήρωση και τη διακυβέρνηση σε αυτά τα έργα.

4.2.β Ηλεκτρονικά Διαβατήρια (e-Passports) και e-Borders

[11] European Parliament, (2018), 'Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC'.

[12] E.A. Whitley and I.R. Hosein, (2008), 'Doing the politics of technological decision making: due process and the debate about identity cards in the U.K.', European Journal of Information Systems, Volume 17, Issue 6, pp. 668-677.

[13] P. Seltsikas and R.M. O'Keefe, (2010), 'Expectations and outcomes in electronic identity management: the role of trust and public value' European Journal of Information Systems, Volume 19, Issue 1, pp. 93-103.

[14] D. Lyon, (2009), 'Identifying citizens: ID cards as surveillance' Polity Press, Cambridge, UK.

[15] E. Wihlborg, (2013), 'Secure electronic identification (eID) in the intersection of politics and technology', International Journal of Electronic Governance, Volume 6, Issue 2, pp. 143-151.

[16] U. Melin, K. Axelsson, and F. Söderström, (2016), 'Managing the development of e-ID in a public e-service context: Challenges and path dependencies from a life-cycle perspective', Emerald Insight, Transforming Government: People, Process and Policy, Volume 10, Issue 1, pp. 72-98.

Το e-Passport, γνωστό και ως βιομετρικό διαβατήριο, είναι ένα παραδοσιακό έντυπο έγγραφο που εμφανίζει απροκάλυπτα προσωπικά αναγνωριστικά που σχετίζονται με ένα άτομο και περιέχει, επίσης, ένα ενσωματωμένο ηλεκτρονικό τσιπ μικροεπεξεργαστή. Το ενσωματωμένο τσιπ αποθηκεύει προσωπικά αναγνωριστικά που μπορεί να χρησιμοποιηθούν για την περαιτέρω επαλήθευση της ταυτότητας του κατόχου του διαβατηρίου. Αυτή η μορφή ηλεκτρονικής αναγνώρισης βασίζεται στην τεχνολογία έξυπνων καρτών όπου τα προσωπικά αναγνωριστικά που είναι αποθηκευμένα στο τσιπ επιτρέπουν στις αρχές την επικύρωση της ταυτότητας του εγγράφου, διασφαλίζοντας ότι οι πληροφορίες που εμφανίζονται φανερά ταιριάζουν με αυτές που είναι κρυφές[17]. Ο έλεγχος ταυτότητας επιτυγχάνεται με την υποδομή δημόσιου κλειδιού (PKI)[18], μειώνοντας την ευκολία με την οποία μπορεί να παραβιαστεί το έγγραφο. Από τον Ιούνιο του 2018, περισσότερες από 150 χώρες εκδίδουν ηλεκτρονικά διαβατήρια αυτού του τύπου.

Οι περισσότερες χώρες παρέχουν τη δική τους εφαρμογή των e-Passports, ωστόσο **η ασφάλεια του e-Passport πρέπει να συμμορφώνεται με τα διεθνή δημόσια πρότυπα του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας (ICAO) αναφορικά με το απόρρητο, την ακεραιότητα και την αυθεντικότητα των δεδομένων του διαβατηρίου**. Επί του παρόντος, τα τυπικά βιομετρικά στοιχεία που χρησιμοποιούνται για τα ηλεκτρονικά διαβατήρια είναι τα δακτυλικά αποτυπώματα, η αναγνώριση προσώπου και η ίριδα. Η αναγνώριση, όπως ορίζεται από το Έγγραφο ICAO-9303 του ICAO και η επαλήθευση των βιομετρικών χαρακτηριστικών πραγματοποιούνται στο e-Borders. Το γεγονός αυτό ενθάρρυνε τα διεθνή αεροδρόμια να διευκολύνουν τα e-Borders ως «αυτόματες πύλες συνοριακού ελέγχου» ικανές να επαληθεύουν βιομετρικά στοιχεία, χωρίς την ανάγκη ανθρώπινης παρέμβασης.

Ωστόσο, προς όφελος της μελλοντικής προστασίας, οι νέες τάσεις στα ταξιδιωτικά έγγραφα είναι η εισαγωγή σελίδων από πολυανθρακικό αδιάβροχο που μειώνουν δραματικά τον κίνδυνο απάτης εγγράφων. Αυτός ο τύπος υποστρώματος εισήχθη στο βρετανικό διαβατήριο του 2019. Υπάρχει, επίσης, η προσδοκία ότι τα ταξιδιωτικά έγγραφα θα ψηφιοποιηθούν περαιτέρω και τα δεδομένα από το e-Passport ενδέχεται να αποθηκευτούν στο έξυπνο τηλέφωνο του χρήστη. Η νέα τεχνολογία που σχεδιάστηκε από την ομάδα εργασίας ICAO New Technologies ονομάζεται Logical Data Structure Version 2 (LDS2) και θα εισαγάγει ψηφιακά ηλεκτρονικά διαβατήρια με δυνατότητα ανάγνωσης και εγγραφής. Αυτό θα διευκολύνει τη συνοδευτική εφαρμογή του e-Passport για την αποθήκευση e-Visas και, σφραγίδων εισόδου/ εξόδου που θα υποστηρίζουν τον αποτελεσματικό έλεγχο της μετανάστευσης. Η τεχνολογία έχει ήδη προχωρήσει, ώστε να επιτρέπει τους χρήστες να χρησιμοποιούν κάρτες επιβίβασης που είναι αποθηκευμένες σε ψηφιακή μορφή στα smartphone τους ως εναλλακτική της έντυπης μορφής. Επί του παρόντος, κυκλοφορούν περισσότερα από 1.000 εκατομμύρια ηλεκτρονικά διαβατήρια, με αποτέλεσμα να επιτυγχάνεται η ταχύτερη ανάδυση, ανάπτυξη και εδραίωση των e-Borders και των έξυπνων αεροδρομίωνων

[17] J.H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk and R.W. Schreur, (2006), 'Crossing Borders: Security and Privacy Issues of the European e-Passport', IWSEC 2006: Advances in Information and Computer Security, pp. 152-167.

[18] International Civil Aviation Organisation (ICAO), (2015), 'Machine Readable Travel Documents', Document 9303, Seventh Edition.

4.3. Συμπεράσματα

Όπως προκύπτει, η απαίτηση για απόδειξη της ταυτότητας είναι διαχρονική, ενώ οι μέθοδοι επίτευξης εξαρτώνται από τους διαθέσιμους κάθε φορά πόρους καθώς και την εξέλιξη της τεχνολογίας. Επίσης, παρότι η «ταυτότητα» εμφανίζεται ως κάτι άυλο, μέσω της τεκμηρίωσης μοναδικών προσωπικών αναγνωριστικών στοιχείων, καθίσταται κάτι αρκετά απτό.

Εξετάστηκαν λοιπόν, τα στοιχεία και οι ιδιότητες που συμβάλλουν στην ανάπτυξη της ταυτότητας. Έγινε αναφορά στα τυπικά προσωπικά αναγνωριστικά (όνομα, ημερομηνία γέννησης, βιομετρικά στοιχεία, δεδομένα κοινωνικής συμπεριφοράς, κ.ά.), υποδείχθηκαν οι κίνδυνοι των ψεύτικων-πλαστώνταυτοτήτων μέσω της ανάλυσης ταυτότητας προσώπων και αναδείχθηκε η ανάγκη για ψηφιοποιημένα αρχεία που συνοδεύουν την ηλεκτρονική τεκμηρίωση, όπως οι ηλεκτρονικές ταυτότητες, τα ηλεκτρονικά διαβατήρια και τα ηλεκτρονικά σύνορα. Η τάση προς την παγκόσμια ψηφιοποίηση αξιοποιεί τα προσωπικά αναγνωριστικά και τις νέες βιομετρικές τεχνολογίες. Οι τεχνολογίες αυτές συνεπάγονται ουσιαστικά τον έλεγχο ταυτότητας δύο παραγόντων, καθώς επίσης περιλαμβάνουν ένα έγγραφο το οποίο περιέχει έξυπνο τσιπ και μία ηλεκτρονική εγγραφή που συνδέεται με όνομα χρήστη και κωδικό πρόσβασης.

Η αυξημένη χρήση διαδικτυακών υπηρεσιών έχει επίσης οδηγήσει τα άτομα να αποδεικνύουν την πραγματική και ψηφιακή τους ταυτότητα, μέσω τεχνολογιών, όπως το IAM, IDaaS, ψηφιακές υπογραφές και ψηφιακά πιστοποιητικά τα οποία προσφέρουν καινοτόμες προσεγγίσεις συνεχώς αυξανόμενων και βελτιωμένων λύσεων. Παράλληλα, τεχνολογίες προστασίας του μέλλοντος στοχεύουν στη χρήση καινοτόμων τεχνολογιών όπως blockchain για την αποθήκευση ταυτοτήτων, ωστόσο αυτές εξυπηρετούν τους σκοπούς των IAM και των διαδικτυακών συναλλαγών και την αντικατάσταση της παραδοσιακής έντυπης τεκμηρίωσης. Επομένως, εντοπίζεται σαφής τάση σταδιακούς κατάργησης της «απτής» ταυτοποίησης και αντικατάστασή της από έναν υποκατάστατο «άυλο» ψηφιακό εκπρόσωπο. Ωστόσο, μια πραγματική εναλλακτική λύση «ψηφιακής ταυτοποίησης» που αποδεικνύει μια πραγματική ταυτότητα χωρίς παραδοσιακή έντυπη τεκμηρίωση, δεν έχει εξελιχθεί ακόμη.

5. Παραδείγματα ψηφιακών ταυτοτήτων στα κράτη-μέλη της Ε.Ε.

Στην παρούσα ενότητα **επιχειρείται η παρουσίαση παραδειγμάτων ψηφιακών εγγράφων σε διάφορα κράτη-μέλη της Ε.Ε.**, που αποτυπώνουν την έννοια της ψηφιακής ταυτοποίησης. Χαρακτηριστικά παραδείγματα είναι αυτά της ταυτότητας, της ψηφιακής ταυτότητας, της κάρτας άδειας διαμονής και της ψηφιακής ταυτότητας e-Resident, δηλαδή της κατοικίας.

Τα ψηφιακά έγγραφα είναι έγγραφα που μπορεί να χρησιμοποιηθούν για την εκτέλεση προσωπικής ταυτοποίησης, την επιβεβαίωση συναλλαγών και την παροχή υπογραφών σε ηλεκτρονικά κανάλια.

5.1. Εσθονία

Η Εσθονία **αποδίδει ιδιαίτερη έμφαση στην αξιόπιστη και ασφαλή ταυτοποίηση**, καθώς η φυσική και ψηφιακή διαχείριση ταυτότητας αποτελούν τη βάση για μία αξιόπιστη διαδικασία έκδοσης εγγράφων ταυτότητας. Μάλιστα, η Εσθονία έχει μακροχρόνια εμπειρία στη χρήση του ηλεκτρονικού ελέγχου ταυτότητας και είναι παγκόσμιος ηγέτης στο πλαίσιο της ηλεκτρονικής διακυβέρνησης.

Σημειώνεται ότι η εσθονική ταυτότητα αποτελεί έγγραφο που αντιστοιχίζει τα χαρακτηριστικά του εσθονικού διακριτικού eID που βασίζεται στην εσθονική ταυτότητα με τις απαιτήσεις των επιπέδων διασφάλισης eIDAS, όπως **ορίζονται στον Εκτελεστικό Κανονισμό (ΕΕ) αριθ. 2015/1502 της Επιτροπής, σύμφωνα με την παρ. 3 του άρθρου 8 του Κανονισμού eIDAS (ΕΕ) αριθ. 910/2014.**

Η Εσθονία **εκδίδει το δελτίο ταυτότητας ως το κύριο και υποχρεωτικό έγγραφο για την ταυτοποίηση των πολιτών της και των πολιτών της Ε.Ε. που ζουν στην Εσθονία**. **Οι κάτοχοι ταυτότητας έχουν το δικαίωμα να έχουν ένα πρόσθετο φορέα ψηφιακής ταυτότητας ή διακριτικό eID, όπως Digi-ID ή Mobiil-ID.** Η κάρτα chip που εκδίδεται είναι ένα φυσικό έγγραφο ταυτοποίησης και διαθέτει προηγμένες ηλεκτρονικές λειτουργίες που διευκολύνουν τον ασφαλή έλεγχο ταυτότητας και την ειδική ηλεκτρονική υπογραφή. Τα πρώτα εσθονικά δελτία ταυτότητας εκδόθηκαν στις 28/01/2002. Η κάρτα στοχεύει στην **καθολικότητα**με την έννοια ότιοι λειτουργίες της είναι προσβάσιμες και μπορούν να χρησιμοποιηθούνσε οποιαδήποτε μορφή επιχειρηματικής, κυβερνητικής ή ιδιωτικής επικοινωνίας. Στόχος είναι η υποστήριξη και η διευκόλυνση της επικοινωνίας καθώς επίσης και η απλούστευση των διαδικτυακών συναλλαγών των ατόμων.

Το Υπουργείο Εσωτερικών της Εσθονίας είναι υπεύθυνο για την ανάπτυξη πολιτικών διαχείρισης ταυτότητας και πολιτικών σε σχέση με την έκδοση εγγράφων ταυτότητας σε Εσθονούς πολίτες και αλλοδαπούς.

Παρακάτω, αποτυπώνεται το **πλαίσιο γενικών αρχών της εσθονικής πολιτικής για τη διαχείριση ταυτότητας και τα προσωπικά έγγραφα ταυτοποίησης:**

- Το κράτος καθορίζει την ταυτότητα του ατόμου.
- Κάθε άτομο έχει μια ταυτότητα.
- Απαγορεύεται η χρήση ταυτότητας ή εγγράφου ταυτότητας άλλου ατόμου.
- Η διαχείριση ταυτότητας πραγματοποιείται από το κράτος, με συγκεντρωτικό τρόπο.
- Τόσο τα φυσικά όσο και τα ψηφιακά προσωπικά έγγραφα ταυτοποίησης συνδέονται άρρηκτα και μοναδικά με την ταυτότητα του χρήστη του εγγράφου.

- Πιστοποιητικά που επιτρέπουν την ψηφιακή ταυτοποίηση και την ειδική ηλεκτρονική υπογραφή για την ψηφιακή ταυτότητα ενός εγγράφου συνδέονται μοναδικά με τα προσωπικά δεδομένα του χρήστη.
- Τα δεδομένα τόσο των φυσικών όσο και των ψηφιακών εγγράφων, συμπεριλαμβανομένων των πιστοποιητικών για έλεγχο ταυτότητας και της ηλεκτρονικής υπογραφής, είναι δημόσια επαληθεύσιμα.
- Τα έγγραφα ταυτότητας και το υποστηρικτικό λογισμικό είναι ασφαλή.

Η Αστυνομία της Εσθονίας είναι υπεύθυνη για τη διαχείριση ταυτότητας και την έκδοση προσωπικών εγγράφων ταυτοποίησης. Η έκδοση εγγράφων ταυτότητας ρυθμίζεται από τον νόμο περί εγγράφων ταυτότητας.

Το εσθονικό σύστημα eID βασίζεται στη χρήση PKI με κρυπτογραφία, σύμφωνα με τις βέλτιστες πρακτικές και στη χρήση έξυπνων καρτών SSCD/QSCD. Ο εκδότης προσδιορίζει φυσικά το πρόσωπο κατά τη διαδικασία έκδοσης. Η εσθονική προδιαγραφή εφαρμογής ηλεκτρονικής ταυτότητας (EstEID) πληροί τις απαιτήσεις του προτύπου ISO/IEC 7816 για λειτουργίες ηλεκτρονικής αναγνώρισης και υπογραφής. Τα πιο πρόσφατα πρότυπα EstEID, προφίλ πιστοποιητικών και προδιαγραφές είναι διαθέσιμα στο κοινό. Το όνομα του πιστοποιητικού εσθονικής ταυτότητας είναι EstEID. Στο τσιπ της εσθονικής ταυτότητας, υπάρχουν δύο ιδιωτικά κλειδιά με τα αντίστοιχα δημόσια κλειδιά στα πιστοποιητικά μορφής X.509. Τα πιστοποιητικά αποθηκεύονται τόσο στο chip όσο και στο αποθετήριο LDAP (διαθέσιμο για ηλεκτρονικές υπηρεσίες):

1) πιστοποιητικό για ηλεκτρονικό έλεγχο ταυτότητας και κρυπτογράφηση

2) πιστοποιητικό παροχής ειδικής ηλεκτρονικής υπογραφής.

Τα πιστοποιητικά ισχύουν μέχρι την ημερομηνία λήξης του δελτίου ταυτότητας, δηλαδή έως και πέντε (5) χρόνια, ανάλογα με την ισχύ της φυσικής ταυτότητας.

Από ένα πιστοποιητικό, μπορεί να αναγνωστούν οι ακόλουθες πληροφορίες σχετικά με τα δεδομένα του κατόχου της ταυτότητας, χωρίς την εισαγωγή του κωδικού PIN1:

• όνομα,

• επώνυμο,

• ημερομηνία γέννησης (μέρος του κωδικού αναγνώρισης του ατόμου),

• κωδικός ταυτότητας ατόμου,

• φύλο (μέρος του κωδικού αναγνώρισης του ατόμου),

• εκδότης πιστοποιητικού,

• αύξων αριθμός του πιστοποιητικού,

• ημερομηνία λήξης του πιστοποιητικού,

•ημερομηνία έκδοσης του πιστοποιητικού.

Τα **στοιχεία των τεχνικών προδιαγραφών και των διαδικασιών** που περιγράφονται στο Παράρτημα του Εκτελεστικού Κανονισμού (ΕΕ) αριθ. 2015/1502 της Επιτροπής, χρησιμοποιούνται για τον προσδιορισμό του τρόπου με τον οποίο οι απαιτήσεις και τα κριτήρια του άρθρου 8 του Κανονισμού (ΕΕ) αριθ. 910/2014, θα εφαρμόζονται ως μέσα ηλεκτρονικής αναγνώρισης που εκδίδονται στο πλαίσιο συστήματος ηλεκτρονικής αναγνώρισης.

Το δελτίο ταυτότητας της Εσθονίας (ταυτότητα) είναι ένα έγγραφο ταυτότητας υποχρεωτικό για τους Εσθονούς πολίτες και τους πολίτες της Ε.Ε. που ζουν στην Εσθονία.

Το δελτίο ταυτότητας και οι υποχρεώσεις του κατόχου ρυθμίζονται από τον κανονισμό eIDAS, τον νόμο περί εγγράφων ταυτότητας, τον νόμο περί ηλεκτρονικών ταυτοτήτων και υπηρεσιών εμπιστοσύνης για ηλεκτρονικές συναλλαγές, την Πολιτική πιστοποιητικού για την ταυτότητα και το πιστοποιητικό, Προφίλ CRL και OCSP για έγγραφα προσωπικής ταυτοποίησης της Δημοκρατίας της Εσθονίας.

Σύμφωνα με την ενότητα 114 του νόμου περί εγγράφων ταυτότητας, το αρχικό δελτίο ταυτότητας μπορεί να ζητηθεί μόνο αυτοπροσώπως (ή μέσω νόμιμου εκπροσώπου) σε γραφείο της αρχής έκδοσης ή στην επίσημη ξένη αντιπροσωπεία της Δημοκρατίας της Εσθονίας. Σε περιπτώσεις λήξης, απώλειας ή κλοπής, οι Εσθονοί πολίτες και οι πολίτες της Ε.Ε. είναι δυνατό να υποβάλουν αίτηση για ανανέωση της ταυτότητας με μία από τις ακόλουθες μεθόδους:

- σε γραφείο της αρχής έκδοσης.
- στην επίσημη ξένη αντιπροσωπεία της Δημοκρατίας της Εσθονίας.
- μέσω ταχυδρομείου.
- μέσω e-mail.
- σε ηλεκτρονικό περιβάλλον (προς το παρόν διατίθεται μόνο για Εσθονούς πολίτες που έχουν προηγουμένως εκδώσει ταυτότητα).

Οι βασικοί όροι και προϋποθέσεις που σχετίζονται με τη χρήση των μέσων ηλεκτρονικής αναγνώρισης της εσθονικής ταυτότητας παρατίθενται σε έντυπη μορφή με δελτίο ταυτότητας και εισάγονται από την αρχή έκδοσης κατά τη διαδικασία έκδοσης. Το έντυπο αποτελείται από δύο μέρη: πρώτον, τους όρους και τις προϋποθέσεις, δεύτερον, το μέρος της αναγνώρισης. Ο παραλήπτης υπογράφει το έντυπο φυσικά, αναγνωρίζοντας και αποδεχόμενος τους όρους και τις προϋποθέσεις. Στη συνέχεια το τμήμα βεβαίωσης διαχωρίζεται από έναν υπάλληλο της αρχής έκδοσης καιαρχειοθετείται η υπογεγραμμένη σε χαρτί απόδειξη .Ο παραλήπτης λαμβάνει το μέρος των όρων και προϋποθέσεων εγγράφως συνονοδευόμενο με ένα ενημερωτικό φυλλάδιο.

Επιπλέον, στον ιστότοπο της εκδίδουσας αρχής υπάρχει υπενθύμιση για την ασφαλή χρήση του δελτίου ταυτότητας, η οποία είναι επίσης διαθέσιμη σε έντυπο φυλλάδιο στο σημείο εξυπηρέτησης της αρχής έκδοσης. Επιπλέον, μια λεπτομερής έκδοση των όρων και προϋποθέσεων για τη χρήση πιστοποιητικών εγγράφων προσωπικής ταυτοποίησης είναι δημόσια διαθέσιμη στον ιστότοπο του παρόχου υπηρεσιών πιστοποίησης (CSP) και μπορεί να ζητηθεί εκτύπωση από την αρχή έκδοσης ή την επίσημη ξένη αντιπροσωπεία της Δημοκρατίας της Εσθονίας.

Η αρχή έκδοσης πρέπει να βεβαιωθεί ότι ο αιτών γνωρίζει τις συνιστώμενες προφυλάξεις ασφαλείας που σχετίζονται με τα μέσα ηλεκτρονικής αναγνώρισης. Οι υποχρεώσεις του κατόχου και η επιστροφή του δελτίου ταυτότητας αναφέρονται στην ενότητα 14 του νόμου περί εγγράφων ταυτότητας. Επιπλέον, οι συνιστώμενες προφυλάξεις ασφαλείας σχετικά με τα μέσα ηλεκτρονικής ταυτοποίησης παρατίθενται στο ενημερωτικό φυλλάδιο, στην υπενθύμιση για την ασφαλή χρήση της ταυτότητας και στους όρους και προϋποθέσεις για τη χρήση των πιστοποιητικών. Για παράδειγμα, ο κάτοχος οφείλει να μην παραδώσει την ταυτότητα τρίτου, να κρατήσει μυστικούς τους κωδικούς PIN μιας κάρτας τρίτων, να διασφαλίσει ότι η ταυτότητα χρησιμοποιείται μόνο υπό τον έλεγχο του κατόχου της, να ειδοποιήσει αμέσως την αρχή έκδοσης, προκειμένου να αναστείλει τα πιστοποιητικά σε περίπτωση απώλειας, κλοπής ή ξεχασμένου κωδικού PIN.

Η εκδούσα αρχή συλλέγει τα σχετικά δεδομένα ταυτότητας που απαιτούνται για την απόδειξη και επαλήθευση ταυτότητας. Η συλλογή των σχετικών στοιχείων ταυτότητας που απαιτούνται για τον έλεγχο ταυτότητας και την εξακρίβωση ρυθμίζεται με βάση τον Κανονισμό αριθ. 77 του Υπουργού Εσωτερικών, από τις 18/12/2015. Η συλλογή των αιτήσεων και των σχετικών δεδομένων ταυτότητας που απαιτούνται για την απόδειξη ταυτότητας στην επίσημη ξένη αντιπροσωπεία της Δημοκρατίας της Εσθονίας ρυθμίζεται επιπρόσθετα από τον προξενικό νόμο και τους κανονισμούς του αρμόδιου υπουργού. Τα δεδομένα ταυτότητας που συλλέγονται ελέγχονται σύμφωνα με τη βάση δεδομένων του μητρώου πληθυσμού της Εσθονίας και τη βάση δεδομένων εγγράφων ταυτότητας.

Για την απόδειξη ταυτότητας, ο αιτών παρέχει τις ακόλουθες πληροφορίες στην αρχή έκδοσης:

- έγκυρο έγγραφο ταυτότητας ή ταξιδιωτικό έγγραφο (εκτός από τις περιπτώσεις που η αίτηση γίνεται μέσω κανονικού ταχυδρομείου, από εκπρόσωπο ή ηλεκτρονικά).
- φωτογραφία απότο σημείο εξυπηρέτησης της αρχής έκδοσης ή μεμονωμένα το πολύ έξι (6) μήνες πριν από την ημερομηνία υποβολής της αίτησης (οι απαιτήσεις ορίζονται στον Κανονισμό αριθ. 62 του Υπουργού Εσωτερικών, που εγκρίθηκε την 01/12/2015).
- καταβολή κρατικών τελών.
- το ελάχιστο σύνολο δεδομένων όπως αναφέρεται στο άρθρο 24 του Κανονισμού αριθ. 77 του Υπουργού Εσωτερικών, από τις 18/12/2015, που περιλαμβάνει τη συλλογή των σχετικών δεδομένων ταυτότητας που απαιτούνται για την επαλήθευση της ταυτότητας ενός ατόμου χωρίς αμφιβολία κατά τη στιγμή της αίτησης, συμπεριλαμβανομένων των εξής:

  1) προσωπικά δεδομένα (όνομα(τα), επώνυμο(α), προσωπικός κωδικός αναγνώρισης της Εσθονίας ή ημερομηνία γέννησης, τόπος γέννησης, φύλο)·

  2) υπηκοότητα

  3) στοιχεία επικοινωνίας (οδός, σπίτι, διαμέρισμα, πόλη ή χωριό, νομός, ταχυδρομικός κώδικας, χώρα, τηλέφωνο, διεύθυνση ηλεκτρονικού ταχυδρομείου).

  4) τόπος έκδοσης.

5) λόγος υποβολής αίτησης.

6) ημερομηνία.

Απόδειξη και επαλήθευση ταυτότητας (φυσικό πρόσωπο): Έχει επαληθευτεί ότι το πρόσωπο έχει στην κατοχή του αποδεικτικά στοιχεία που αναγνωρίζονται από το κράτος μέλος στο οποίο υποβάλλεται η αίτηση ηλεκτρονικής ταυτότητας. Παράλληλα τα αποδεικτικά στοιχεία ελέγχονται για να διαπιστωθεί ότι είναι γνήσια ή, σύμφωνα με μια έγκυρη πηγή. που σχετίζεται με ένα πραγματικό πρόσωπο και επιβεβαιώνει την ύπαρξή του και έχουν ληφθεί μέτρα για να ελαχιστοποιηθεί ο κίνδυνος του ενδεχομένου η ταυτότητα του ατόμου να μην είναι η αναγνωρισμένη ταυτότητα, λαμβάνοντας υπόψη για παράδειγμα τους κινδύνους της απώλειας, κλοπής, της περίπτωσης αναστολής, ανάκλησης ή λήξης αποδεικτικών στοιχείων.

Το εσθονικό eID εκδίδεται πάντα συνοδευόμενο από το εσθονικό διακριτικό eID, το οποίο αναφέρεται σε αυτό το έγγραφο, ως εσθονική ταυτότητα. Το δελτίο ταυτότητας της Εσθονίας εκδίδεται τόσο σε Εσθονούς πολίτες όσο και σε πολίτες της Ε.Ε.. Το δελτίο ταυτότητας που εκδίδεται σε πολίτες της Ευρωπαϊκής Ένωσης ισχύει για χρήση ηλεκτρονικών υπηρεσιών της Εσθονίας, αλλά δεν αναγνωρίζεται ως ταξιδιωτικό έγγραφο. Τα δεδομένα για κάθε αίτηση ταυτότητας καταγράφονται στη βάση δεδομένων εγγράφων ταυτότητας. Οι αλλοδαποί για τους οποίους έχει εκδοθεί εσθονικό έγγραφο ταυτότητας βάσει του Νόμου περί Εγγράφων Ταυτότητας και όλοι οι Εσθονοί πολίτες έχουν προσωπικό κωδικό αναγνώρισης και καταγράφονται κεντρικά στο εσθονικό μητρώο πληθυσμού. Ο προσωπικός δε κωδικός αναγνώρισης χρησιμοποιείται, ως μοναδικός αναγνωριστικός κωδικός.

Όταν ένας Εσθονός πολίτης υποβάλλει αίτηση για δελτίο ταυτότητας, τα δεδομένα του ελέγχονται βάσει του μητρώου πληθυσμού και της βάσης δεδομένων των εγγράφων ταυτότητας, σύμφωνα με τον νόμο περί εγγράφων ταυτότητας και τους κανονισμούς που εκδίδονται βάσει αυτού του νόμου. Η βάση δεδομένων εγγράφων ταυτότητας επαληθεύει την εγκυρότητα ενός εσθονικού εγγράφου ταυτότητας, παρέχοντας ταυτόχρονα πληροφορίες σχετικά με τα προσωπικά δεδομένα του κατόχου του εγγράφου (συμπεριλαμβανομένης της εικόνας του προσώπου), καθώς και για την κατάσταση της ταυτότητας που είχε εκδοθεί προηγουμένως έγγραφα, συμπεριλαμβανομένων πληροφοριών σχετικά με το εάν τα έγγραφα έχουν χαθεί, κλαπεί, ανακληθεί ή λήξει.

Όταν ένας πολίτης της Ε.Ε. υποβάλλει αίτηση για δελτίο ταυτότητας, τα δεδομένα του ελέγχονται, επίσης, σε σχέση με το μητρώο πληθυσμού και τη βάση δεδομένων των εγγράφων ταυτότητας για να διαπιστωθεί εάν έχουν υπάρξει προηγούμενες συναντήσεις με τη Δημοκρατία της Εσθονίας. Ένας πολίτης της Ε.Ε., όταν υποβάλλει αίτηση για δελτίο ταυτότητας, πρέπει να προσκομίσει έγκυρο έγγραφο ταυτότητας που έχει εκδοθεί από το κράτος-μέλος της Ε.Ε. της ιθαγένειάς του. Για την επαλήθευση της εγκυρότητας και της γνησιότητας του προσκομιζόμενου εγγράφου ταυτότητας, τα δεδομένα του εγγράφου ελέγχονται σε σχέση με το Σύστημα Πληροφοριών Σένγκεν (SIS) και τη βάση δεδομένων της INTERPOL που αφορά απολεσθέντα και κλεμμένα έγγραφα. Η γνησιότητα του προσκομιζόμενου εγγράφου ταυτότητας επαληθεύεται, σύμφωνα με τα δείγματα εγγράφων που υποβλήθηκαν από άλλα κράτη-μέλη.

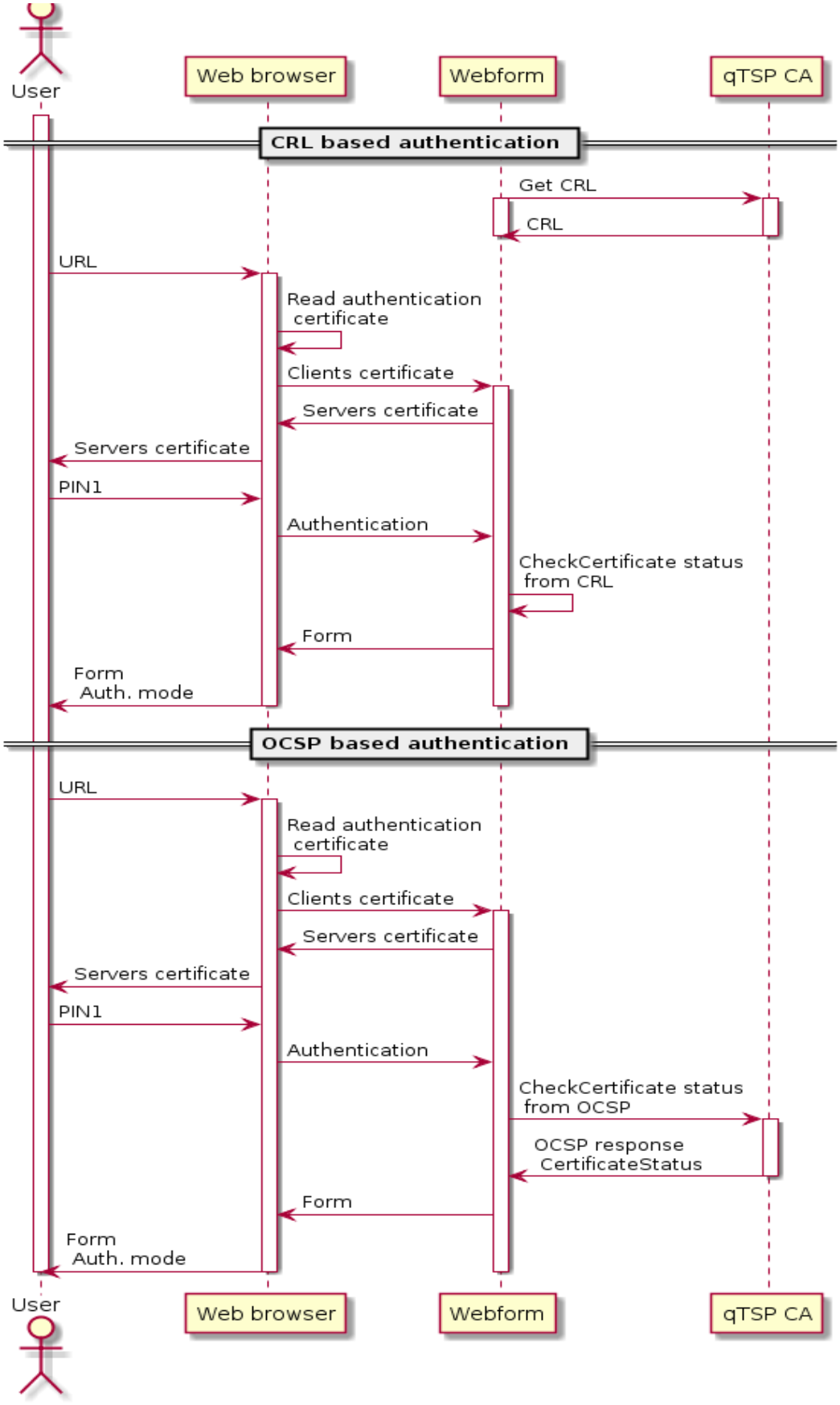
Ένα έγγραφο ταυτότητας προσκομίζεται κατά τη διαδικασία καταχώρισης στο κράτος-μέλος όπου εκδόθηκε το έγγραφο. Το έγγραφο φαίνεται να σχετίζεται με το πρόσωπο που το προσκομίζει και έχουν ληφθεί μέτρα για να ελαχιστοποιηθεί ο κίνδυνος της περίπτωσης όπου η ταυτότητα του ατόμου να μην είναι η ταυτότητα που ζητήθηκε, λαμβάνοντας υπόψη, τα ενδεχόμενα και τους τον κινδύνους απώλειας, κλοπής, αναστολής, ανάκλησης ή λήξης εγγράφων.

Σε περίπτωση Εσθονών πολιτών, η αρχική απόδειξη ταυτότητας γίνεται με βάση το πιστοποιητικό γέννησης, τη συγγένεια στο μητρώο πληθυσμού της Εσθονίας και σύμφωνα με τον νόμο περί ιθαγένειας. Σε περίπτωση ανανέωσης ταυτότητας, η ταυτοποίηση γίνεται με βάση την προηγούμενη ταυτότητα και το μητρώο πληθυσμού της Εσθονίας. Σε περίπτωση πολιτών της Ε.Ε., η απόδειξη της ταυτότητας διενεργείται με βάση έγκυρο έγγραφο ταυτότητας που περιλαμβάνει βιομετρικά δεδομένα, όπως φωτογραφία.

Όταν οι διαδικασίες που χρησιμοποιήθηκαν προηγουμένως από δημόσιο ή ιδιωτικό φορέα στο ίδιο κράτος-μέλος, για σκοπό διαφορετικό από την έκδοση μέσων ηλεκτρονικής ταυτοποίησης, παρέχουν ισοδύναμη διασφάλιση με εκείνες που ορίζονται για το ουσιαστικό επίπεδο διασφάλισης, τότε η οντότητα που είναι υπεύθυνη για την καταχώριση, δεν χρειάζεται να επαναλάβει τις συγκεκριμένες προηγούμενες διαδικασίες, υπό την προϋπόθεση ότι η ισοδύναμη αυτή διασφάλιση, επιβεβαιώνεται από φορέα αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 2 παράγραφος 13 του Κανονισμού (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ή από ισοδύναμο φορέα.

Όταν τα ηλεκτρονικά μέσα αναγνώρισης εκδίδονται βάσει έγκυρων κοινοποιημένων μέσων ηλεκτρονικής ταυτοποίησης με ουσιαστικό ή υψηλό το επίπεδο ασφάλειας, λαμβανομένων υπόψη των κινδύνων αλλαγής στα δεδομένα αναγνώρισης προσώπου, τότε δεν απαιτείται επανάληψη απόδειξης ταυτότητας και διαδικασίες επαλήθευσης. Όταν τα μέσα ηλεκτρονικής αναγνώρισης που χρησιμεύουν ως βάση, δεν έχουν κοινοποιηθεί, το σημαντικό ή υψηλό επίπεδο ασφάλειας πρέπει να επιβεβαιώνεται από φορέα αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 2 παράγραφος 13 του Κανονισμού (ΕΚ) αριθ. 765/2008 ή από ισότιμο φορέα.

Αυθεντικοποίηση: Ο **μηχανισμός ελέγχου ταυτότητας της εσθονικής ταυτότητας περιγράφεται στην παρακάτω εικόνα**.



Εικόνα 3: Αυθεντικοποίηση της εσθονικής ID κάρτας

Στην **Εσθονία**[19] χρησιμοποιούνται **διάφορα ψηφιακά έγγραφα** - το πιο συνηθισμένο από τα οποία είναι, φυσικά, η υποχρεωτική ταυτότητα για τους Εσθονούς πολίτες. **Εκτός**

[19] Republic of Estonia, Police and Boarder Guard Board. Estonian eID scheme: ID card. Technical specifications and procedures for assurance level high for electronic identification, 27/02/2018.
"eIDAS Regulation," http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
"Internal Safety Development Plan 2015–2020," (in Estonian only), https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/taiendatud_siseturvalisuse_arengukava_2015-2020.pdf.
"Identity Documents Act," https://www.riigiteataja.ee/en/eli/521062017003/consolide.
"EstEID v. 3.5 Estonian electronic ID card application specification," http://id.ee/public/TB-SPEC-EstEID-Chip-App-v3.5-20170314.pdf
"GDPR," http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 "Electronic Identification and Trust Services for Electronic Transactions Act," https://www.riigiteataja.ee/en/eli/527102016001/consolide
"Certificate policy for the ID card," https://sk.ee/upload/files/SK-CP-ID%20CARD-EN-v6_0_20161101.pdf
"Certificate, CRL and OCSP Profile for Personal Identification Documents of the Republic of Estonia," https://sk.ee/upload/files/SK-CPR-ESTEID-EN_v8_1_20171104.pdf
"The safe use of an identity card (ID card), residence card, and Digi-ID," https://www.politsei.ee/en/nouanded/isikut-toendavad-dokumendid/index.dot
"Terms and conditions for the use of certificates of personal identification documents of the Republic of Estonia," https://www.sk.ee/upload/files/SK-TCU-ESTEID-EN-CURRENT.pdf
"Regulation 77 of the Minister of the Interior," (in Estonian only), https://www.riigiteataja.ee/akt/102022018002
"Consular Act," https://www.riigiteataja.ee/en/eli/527012016004/consolide
"Regulation 62 of the Minister of the Interior, as of 01/12/2015," (in Estonian only), https://www.riigiteataja.ee/akt/118112016005
"Citizenship Act," https://www.riigiteataja.ee/en/eli/513012017001/consolide
"Police and Border Guard Act," https://www.riigiteataja.ee/en/eli/515092017001/consolide
"Statutes of the Police and Border Guard Board," (in Estonian only), https://www.riigiteataja.ee/akt/128062017043
"International Civil Aviation Organization," https://www.icao.int/
"Statutes of the IT and Development Centre, Ministry of the Interior," (in Estonian only), https://www.smit.ee/pdf/pohimaarus.pdf
"ISKE," https://www.ria.ee/en/iske-en.html
"Statutes of the Information System Authority," (in Estonian only), https://www.riigiteataja.ee/akt/129122016014
"Estonian Trusted List," https://sr.riik.ee/en/tl.html
"Statutes of the Technical Regulatory Authority," (in Estonian only), https://www.riigiteataja.ee/akt/106012017003
"ESTEID-SK qualified certificates for electronic signatures," https://www.sk.ee/upload/files/9734UE_s_2017.pdf
"SK insurance certificate," https://www.sk.ee/upload/files/PI%20Certificate%20-%20SK%20ID%20Solutions%20AS%20-%20signed_nimega.pdf
"Emergency Act," https://www.riigiteataja.ee/en/eli/505012018004/consolide
"General Part of the Economic Activities Code Act," https://www.riigiteataja.ee/en/eli/504012018003/consolide
"Trust Services Practice Statement," https://sk.ee/upload/files/SK-PS-EN-v3_0_20170101.pdf
"State Fees Act," https://www.riigiteataja.ee/en/eli/502012018002/consolide
"Personal Data Protection Act," https://www.riigiteataja.ee/en/eli/507032016001/consolide
"Statutes of the Identity Documents Database," (in Estonian only), https://www.riigiteataja.ee/akt/102022018003

από το δελτίο ταυτότητας, υπάρχει επίσης ψηφιακή ταυτότητα, κάρτα άδειας διαμονής, ψηφιακή ταυτότητα e-Resident και διπλωματική κάρτα.

Τα ψηφιακά έγγραφα διακρίνονται με βάση κυρίως από ποιες αρχές εκδίδονται και σε ποιον πολίτη αφορούν. Ενδεικτικό στοιχείο χρήσης κάθε κάρτας αποτελεί καταρχάς το όνομά της. Η **ψηφιακή ταυτότητα** αποσκοπεί στην αναγνώριση της ταυτότητας ατόμου, ώστε να είναι κατάλληλη για τη χρήση παράλληλα με την φυσική ταυτότητα. Η **κάρτα άδειας διαμονής** αφορά πολίτες που δεν ζουν μόνιμα στην Εσθονία, αλλά διατηρούν την ιδιότητα του αλλοδαπού, ενώ η **ψηφιακή ταυτότητα του e-Resident** επιτρέπει σε αλλοδαπούς που δεν ζουν στην Εσθονία να χρησιμοποιούν εσθονικές ηλεκτρονικές υπηρεσίες, όπως σύνδεση σε τραπεζικούς λογαριασμούς, εγγραφή και διαχείριση εταιρειών κ.λπ.

Το σύνολο δε των καρτών αυτών λειτουργούν με τον ίδιο τρόπο σε επίπεδο ηλεκτρονικό, ήτοι α) για να αναγνωστεί μία κάρτα απαιτείται συσκευή ανάγνωσης ταυτότητας (ID-card reader)[20], β) για τη χρήση της κάρτας είναι απαραίτητο να εγκατασταθεί το λογισμικό ID (ID-software) στον υπολογιστή του πολίτη και γ) οι οδηγίες για την ταυτότητα είναι ίδιες για το σύνολο των ψηφιακών εγγράφων.

Στην Εσθονία η **ταυτότητα**, ως υποχρεωτικό νομιμοποιητικό έγγραφο, **μπορεί να έχει τη μορφή της ψηφιακής ταυτότητας**, ενώ παρέχεται και η δυνατότητα εγγραφής στο **mobile-ID** καθώς και η δυνατότητα εγκατάστασης στην έξυπνη συσκευή, ακόμα και σε **tablet**, υπό μορφή **Smart-ID**. Τα δελτία ταυτότητας ισχύουν έως και πέντε (5) χρόνια .

Οι **χρήσεις της ταυτότητας στην Εσθονία** αποτυπώνονται ως εξής: α) ως **φυσικό έγγραφο ταυτότητας**, β) **ως έγγραφο ψηφιακής αναγνώρισης του ατόμου**, γ) **ως μέσο πρόσβασης σε ηλεκτρονικές υπηρεσίες** (λ.χ. Internet Bank, e-Tax και ηλεκτρονικά τιμολόγια), δ) **ως κάρτα επιβράβευσης σε αρκετά μέρη**, ε) αξιοποιείται για την **ψηφιακή υπογραφή** καθώς **και την κρυπτογράφηση εγγράφων**, στ) χρησιμοποιείται **κατά τη διενέργεια ηλεκτρονικής ψηφοφορίας**, ζ) μπορεί να χρησιμοποιηθεί **ως ταξιδιωτικό έγγραφο στην Ε.Ε. και τον Ευρωπαϊκό Οικονομικό Χώρο** και η) **αξιοποιείται με μία διεύθυνση ηλεκτρονικού ταχυδρομείου μορφής @eesti.ee, που παρέχεται από τη Δημοκρατία της Εσθονίας.**

"Public Information Act," https://www.riigiteataja.ee/en/eli/516102017007/consolide
"Archives Act," https://www.riigiteataja.ee/en/eli/504032016002/consolide
"Regulation 78 of the Minister of the Interior," (in Estonian only), https://www.riigiteataja.ee/akt/114012017016
"Regulation 181 of the Government of the Republic as of 22/12/2011," (in Estonian only), https://www.riigiteataja.ee/akt/113012015021?leiaKehtiv
"Civil Service Act," https://www.riigiteataja.ee/en/eli/502012018003/consolide
"ESTEID-SK Certification Practice," https://sk.ee/upload/files/SK-CPS-ESTEID-EN-v3_0_20171101.pdf
"Government of the Republic Act," https://www.riigiteataja.ee/en/eli/516102017008/consolide
"Certificate Policy for Mobile ID of the Republic of Estonia," https://sk.ee/upload/files/SK-CP-MOBILE%20ID-EN-v6_0-20171024.pdf

[20] Δύο κινητά εργαλεία ηλεκτρονικής αναγνώρισης: α) Mobile-ID που βασίζεται σε SIM και β) Έξυπνη εφαρμογή Smart-ID.

Εικόνα 4: Δελτίο Ταυτότητας Εσθονίας (εμπρόσθια όψη)

Εικόνα 5: Ψηφιακή ταυτότητα Εσθονίας (οπίσθια όψη)

Σημειώνεται παράλληλα οι οδηγίεστης Εσθονικής Κυβέρνησης ότι, σε περίπτωση καθημερινής χρήσης της ταυτότητας, συνιστάται η παραγγελία μίας ψηφιακής ταυτότητας, ώστε το φυσικό δελτίο ταυτότητας να αποθηκεύεται σε ασφαλές μέρος, χωρίς φόβο απώλειας ή καταστροφής του τσιπ, λόγω της συνεχούς χρήσης. Εξάλλου, η ψηφιακή ταυτότητα, που εκδίδεται κατόπιν αίτησης στο Συμβούλιο Αστυνομίας και Συνοριακής Φύλαξης της Εσθονίας, επιτρέπει τη χρήση των ιδίων ηλεκτρονικών υπηρεσιών με το φυσικό δελτίο ταυτότητας, αλλά δεν μπορεί να χρησιμοποιηθεί ως έγγραφο ταυτότητας. Επομένως, η ψηφιακή ταυτότητα, ως ψηφιακό έγγραφο, **μπορεί να χρησιμοποιηθεί παράλληλα με το φυσικό δελτίο ταυτότητας**. Επίσης, δεδομένου ότι μία **ψηφιακή ταυτότητα έχει ισχύ για πέντε (5) έτη και δεν διαθέτει φωτογραφία του ατόμου, μπορεί να χρησιμοποιείται μόνο ηλεκτρονικά.**

Οι ομοιότητες της ψηφιακής ταυτότητας με τα φυσικά δελτία ταυτότητας αναφέρονται στην ψηφιακή ταυτοποίηση, την ψηφιακή υπογραφή, την κρυπτογράφηση εγγράφων, τη χρήση ηλεκτρονικών υπηρεσιών, την ηλεκτρονική ψηφοφορία, τη χρήση του ιδίου λογισμικού ID καθώς και την παροχή πρόσβασης σε μία διεύθυνση ηλεκτρονικού ταχυδρομείου μορφής @eesti.ee.

Αντίθετα, **οι διαφορές των δύο αυτών εγγράφων συνίστανται στο ότι οι ψηφιακές ταυτότητες δεν δύναται να χρησιμοποιηθούν για τη φυσική ταυτοποίηση του ατόμου καθώς και ως ταξιδιωτικά έγγραφα.**

Το **δελτίο άδειας διαμονής** είναι υποχρεωτικό (για αλλοδαπούς πολίτες) εθνικό έγγραφο ταυτότητας. Εκδίδεται σε αλλοδαπούς που υποβάλλουν αίτηση ή έχουν άδεια διαμονής ή δικαίωμα διαμονής στην Εσθονία και που δεν είναι πολίτες της Ευρωπαϊκής Ένωσης. Η κάρτα περιλαμβάνει προσωπικά δεδομένα του χρήστη, δεδομένα άδειας διαμονής, φωτογραφίες και εικόνες δακτυλικών αποτυπωμάτων. Οι κάρτες άδειας διαμονής ισχύουν έως και πέντε (5) χρόνια, αλλά όχι περισσότερο από τη χορήγηση άδειας διαμονής ή δικαιώματος διαμονής στον χρήστη. Η **ομοιότητα με τα δελτία ταυτότητας** έγκειται στη δυνατότητα χρήσης ηλεκτρονικών υπηρεσιών, της ψηφιακής ταυτοποίησης και της ψηφιακής υπογραφής. Από την άλλη πλευρά, οι **διαφορές μεταξύ των αδειών διαμονής και των δελτίων ταυτότητας** αφορούν στο ότι, οι κάρτες άδειες διαμονής δεν μπορούν να χρησιμοποιηθούν ως ταξιδιωτικά έγγραφα εκτός Εσθονίας καθώς και ότι περιλαμβάνουν ένα τσιπ χωρίς επαφή με δακτυλικό αποτύπωμα και τη φωτογραφία του χρήστη, ενώ τα δελτία ταυτότητας δεν έχουν τσιπ χωρίς επαφή.

Η **ψηφιακή ταυτότητα e-Resident** (κάρτα ηλεκτρονικού κατοίκου) είναι ένα ψηφιακό έγγραφο που εκδίδεται σε αλλοδαπούς πολίτες, το οποίο μπορεί να χρησιμοποιηθεί μόνο ηλεκτρονικά. Η διάρκεια ισχύος της κάρτας είναι πέντε (5) χρόνια. Οι Εσθονοί ηλεκτρονικοί κάτοικοι μπορεί να είναι αλλοδαποί που θέλουν να χρησιμοποιούν εσθονικές ηλεκτρονικές υπηρεσίες, όπως για παράδειγμα να ανοίξουν τραπεζικό λογαριασμό ή να εγγράψουν την εταιρεία τους στην Εσθονία, να εξασφαλίσουν πρόσβαση σε ηλεκτρονικό φόρο, τραπεζικούς λογαριασμούς, Εμπορικό Μητρώο κ.λπ. Το e-residency δεν παρέχει στον χρήστη του άλλα δικαιώματα πέραν της δυνατότητας χρήσης ψηφιακών υπηρεσιών. Δεν συνεπάγεται εσθονική υπηκοότητα ή φορολογική διαμονή, δεν χορηγεί σε αλλοδαπό άδεια παραμονής ή άδεια εισόδου στην Ευρωπαϊκή Ένωση.. Η **ομοιότητα με τα δελτία ταυτότητας** είναι η παροχή δυνατότητας ψηφιακής υπογραφής και χρήσης ηλεκτρονικών υπηρεσιών της Εσθονίας (πρόσβαση στο Εμπορικό Μητρώο, Τράπεζες Διαδικτύου, Φορολογικό Συμβούλιο κ.λπ.). Αντίθετα, **οι κύριες διαφορές μεταξύ των ψηφιακών ταυτοτήτων και των δελτίων ταυτότητας του e-Resident** έγκειται στο ότι οι ψηφιακές ταυτότητες του E-Resident δεν είναι φυσικά έγγραφα ταυτότητας, δεν μπορεί να χρησιμοποιηθούν ως ταξιδιωτικά έγγραφα και το δικαίωμα ενός ηλεκτρονικού κατοίκου να εισέλθει στην Εσθονία/Ευρωπαϊκή Ένωση εξαρτάται από τη χώρα καταγωγής του, αφού η κάρτα ηλεκτρονικού κατοίκου δεν παρέχει ούτε επιβεβαιώνει αυτό το δικαίωμα. Συνεπώς, η ψηφιακή ταυτότητα e-Resident επιτρέπει σε αλλοδαπούς να εγγραφούν και να ασκήσουν επιχειρηματική δραστηριότητα στην Εσθονία και, επομένως, στην Ε.Ε., χωρίς να εγκαταλείπουν τη χώρα διαμονής τους.

Οι ηλεκτρονικές ευκαιρίες που παρέχει η Εσθονία την καθιστούν μοναδική στον κόσμο. Εκτός από τη δυνατότητα εκτέλεσης όλων σχεδόν των λειτουργιών ηλεκτρονικά, ένα σημαντικό μέρος των (επιχειρηματικών) πληροφοριών είναι δημόσια διαθέσιμο σε όλους όσους ενδιαφέρονται. Αυτό εξασφαλίζει ένα ευνοϊκό, διαφανές και αξιόπιστο επιχειρηματικό περιβάλλον και υποστηρίζει νεοφυείς και μικρές επιχειρήσεις.

Τα ψηφιακά έγγραφα (συμπεριλαμβανομένων των ταυτοτήτων, των ψηφιακών ταυτοτήτων, των δελτίων αδειών παραμονής και των ψηφιακών ταυτοτήτων ηλεκτρονικού κατοίκου) εκδίδονται από την Αστυνομία και το Συμβούλιο Συνοριακής Φύλαξης. Οι αιτήσεις μπορεί να υποβληθούν τόσο σε σημεία εξυπηρέτησης όσο και σε σημεία αυτοεξυπηρέτησης. Τα ψηφιακά αναγνωριστικά του ηλεκτρονικού κατοίκου μπορεί, επίσης, να υποβληθούν εύκολα μέσω του ιστότοπου e-residency. Όλα τα έγγραφα ψηφιακής ταυτότητας υπόκεινται σε κρατικά τέλη, δηλαδή τέλη έκδοσης. Επίσης, αν κάποιος βρίσκεται στο εξωτερικό, μπορεί, επίσης, να υποβάλει αίτηση για την έκδοσή τους και να γίνει παραλαβή από τις διπλωματικές αρχές της Δημοκρατίας της Εσθονίας.

Ως πιστοποιητικό νοούνται τα ηλεκτρονικά αποδεικτικά στοιχεία που συνδέουν ένα άτομο, και είναι απαραίτητο για την παροχή της διαβεβαίωσης ότι μια δραστηριότητα ή συναλλαγή πραγματοποιήθηκε ή δόθηκε μια υπογραφή κ.λπ. από το κατάλληλο άτομο. Το άτομο του οποίου η ταυτότητα βρίσκεται στον αναγνώστη αναγνωρίζεται αμέσως, όταν πραγματοποιείται μία δραστηριότητα, ενώ κάθε πιστοποιητικό που μπορεί να έχει έννομες συνέπειες προϋποθέτει για λόγους ασφαλείας, την ύπαρξη πιστοποιητικού.

Όπως και στο Βέλγιο, η ψηφιακή ταυτότητα περιλαμβάνει ένα τσιπάκι ασφαλείας εντός του οποίου είναι ενταγμένα δύο πιστοποιητικά, το ένα για την ηλεκτρονική αυθεντικοποίηση και το άλλο για την ψηφιακή υπογραφή. Σημαντικό είναι το γεγονός ότιαπό το 2007 αναπτύχθηκε μια λύση για το κινητό.

Από τη στιγμή δημιουργίας της ψηφιακής ταυτότητας, ο χρήστης μπορεί να πληροφορηθεί για τα προσωπικά δεδομένα που τον αφορούν, όπως τη διεύθυνση του και να αποφασίσει αν θέλει να δημιουργήσει την ψηφιακή ταυτότητά του. Οι χρήστες αποφασίζουν ποιες υπηρεσίες θα έχουν πρόσβαση στα δεδομένα τους.

Η λύση της Εσθονίας (Mobile ID) επιτρέπει στο χρήστη να έχει πρόσβαση σε υπηρεσίες τόσο του δημόσιου όσο και του ιδιωτικού τομέα, χρησιμοποιώντας ένα αναγνωριστικό και δύο κωδικούς PIN, υπό όρους δηλαδή αυξημένης ασφάλειας για την προστασία των δεδομένων προσωπικού χαρακτήρα και την αποτροπή τυχόν πλαστοπροσωπίας.

Η Εσθονία έχει αναπτύξει στρατηγική σχετικά με τη δυνατότητα των πολιτών να έχουν πρόσβαση σε λίστα πληροφοριών που διαθέτει η Δημόσια Διοίκηση για αυτούς, με την ανάπτυξη συστήματος ειδοποιήσεων. Επίσης, έχει αναπτύξει έναν πίνακα όπου οι πολίτες μπορούν να βλέπουν τα δεδομένα που ανταλλάσσουν οι διοικητικές υπηρεσίες μεταξύ τους, στο πλαίσιο της αρχής μόνον άπαξ (ψηφιακό ντοσιέ του πολίτη).

Όταν ένας Εσθονός πολίτης κάνει αίτηση για την έκδοση ψηφιακής ταυτότητας, τα δεδομένα σχετικά με την αίτηση της ταυτότητας παραμένουν σε βάση δεδομένων. Τα έγγραφα της ταυτότητας φέρουν ένα προσωπικό αριθμό ταυτοποίησης και καταγράφονται

κεντρικά στο **Εσθονικό Μητρώο Πολιτών**. Ο **προσωπικός αριθμός ταυτοποίησης** είναι μοναδικός κωδικός ταυτοποίησης. Η βάση δεδομένων επιβεβαιώνει αν μια ταυτότητα είναι έγκυρη, αλλά, παρέχει επίσης, πληροφορίες σχετικά με τα προσωπικά δεδομένα του κατόχου του εγγράφου, καθώς και για την κατάσταση της προηγούμενης εκδοθείσας ταυτότητας.

Η ηλεκτρονική ταυτοποίηση σημαίνει ότι χρησιμοποιούνται τουλάχιστον δύο παράγοντες αυθεντικοποίησης: ένα τσιπάκι και κωδικοί PIN. Ο δεύτερος παράγοντας αυθεντικοποίησης είναι οι κωδικοί PIN, οι οποίοι εκδίδονται μαζί με την ταυτότητα. Ο πολίτης λαμβάνει 3 ασφαλείς κωδικούς, το πρώτο PIN για λόγους αυθεντικοποίησης, PIN 2 για μια πιστοποιημένη ηλεκτρονική υπογραφή και PUK για το ξεμπλοκάρισμα του PIN, μετά την καταχώρηση εσφαλμένου PIN τρεις φορές. Ο χρήστης κατέχει ένα μοναδικό ιδιωτικό κλειδί, το οποίο χρησιμοποιείται για αυθεντικοποίηση. Το ιδιωτικό κλειδί είναι αποθηκευμένο σε μια ασφαλή μονάδα ενός μικροτσίπ στην έξυπνη κάρτα. Η έξυπνη κάρτα είναι μια φυσική συσκευή κάτω από τον έλεγχο του χρήστη. Η ηλεκτρονική ταυτοποίηση προστατεύει από την αντιγραφή, την παραποίηση, καθώς και από κακόβουλες ενέργειες τρίτων όπως hackers.

5.2. Δανία

Στη Δανία χρησιμοποιείται κάρτα που αποτελείται από μια σειρά αριθμών μιας χρήσης. Πρόκειται για την ψηφιακή ταυτότητα NemID, της οποίας η λειτουργία είναι διακριτή όσον αφορά το δημόσιο και τον ιδιωτικό τομέα.

5.3. Γερμανία

Στη Γερμανία η αυθεντικοποίηση είναι εφικτή ηλεκτρονικά με μία κάρτα ψηφιακής ταυτότητας, η οποία δημιουργήθηκε το 2010. Η ενεργοποίηση της ψηφιακής ταυτότητας ήταν προαιρετική και χορηγείται, κατόπιν αίτησης του πολίτη. Είναι πλέον υποχρεωτική, πλην των ανηλίκων κάτω των 17 ετών, οι οποίοι είναι δυνατό να επωφεληθούν από έναν αριθμό, που δεν έχει αυτή τη λειτουργία.

Η γερμανική ψηφιακή ταυτότητα αποτελεί μέσο ηλεκτρονικής απόδειξης της ταυτότητας ενός προσώπου στο Διαδίκτυο. Σύμφωνα με τη γερμανική προσέγγιση του ζητήματος, που διακρίνεται από αυτή άλλων κρατών-μελών της Ε.Ε., όπου διαχωρίζεται με αυστηρό τρόπο η ηλεκτρονική ταυτοποίηση του προσώπου από την ηλεκτρονική υπογραφή, η νέα γερμανική ψηφιακή ταυτότητα παρέχει τη δυνατότητα να χρησιμοποιείται και ως συσκευή ασφαλούς υπογραφής.

Τα κύρια χαρακτηριστικά της γερμανικής ηλεκτρονικής ταυτότητας είναι τα εξής:

α) είναι εξοπλισμένη με ένα ανέπαφο RFIP chip, στο οποίο αποθηκεύονται βιομετρικά δεδομένα του προσώπου, όπως δακτυλικά αποτυπώματα, κατόπιν αιτήματος του πολίτη,

β) χρησιμοποιείται και ως συσκευή ασφαλούς υπογραφής προαιρετικά,

γ) οι πάροχοι υπηρεσιών πιστοποίησης είναι ιδιώτες,

δ) η προσέγγιση είναι πολιτοκεντρική.

Στη Γερμανία η ταυτότητα δεν ανανεώνεται αποκλειστικά από επίσημους φορείς, αλλά μέσω έρευνας του Μητρώου Πολιτών, είτε από άλλους δημόσιους οργανισμούς είτε από ιδιώτες-αναδόχους.

Στη συνέχεια παρουσιάζονται **οι λειτουργίες του συστήματος ταυτοποίησης**. Συγκεκριμένα, οι ταυτότητες δεν απαιτούνται για τη διαδικασία ταυτοποίησης, αλλά, έχει δημιουργηθεί κυβερνητικό σύστημα ταυτοποίησης, όπου παράγεται επίσημη ταυτότητα, η οποία μπορεί να αναπαραχθεί σε μεταγενέστερες διαδικασίες ταυτοποίησης για κάθε πολίτη. Το κράτος είναι αυτό που αποφασίζει για τη χρήση των εργαλείων για υποχρεωτική εγγραφή και ταυτοποίηση των πολιτών καιγια την θεσμική κατοχύρωση της ταυτότητας .

Επομένως, **η ηλεκτρονική ταυτότητα δεν αποτελεί μόνο επίσημη απόδειξη της ταυτότητας ενός ατόμου, αλλά και προσωπική ταυτότητα**, στο πλαίσιο της έκφρασης του δικαιώματος του πληροφοριακού αυτοπροσδιορισμού του προσώπου. Ασφαλώς το δικαίωμα πληροφοριακού του αυτοπροσδιορισμού συναρτάται άμεσα με την προστασία των δεδομένων προσωπικού χαρακτήρα του ατόμου, σε συνδυασμό με τις θεμελιώδεις αρχές και δικαιώματα του ατόμου, με τη προστασία της δημοκρατίας και του δημόσιου συμφέροντος, επιφέροντας δυνητικές συνέπειες οριζόντια.

Έχει καταστεί δε απόλυτα κατανοητή η ανάγκη για ασφαλή ταυτοποίηση. Μάλιστα, στην ψηφιακή κοινότητα υπάρχει μία πληθώρα διαφορετικών διαδικασιών αυθεντικοποίησης, όπως το PIN/TAN, η διαδικασία του HBCI στην περιοχή της ηλεκτρονικής τραπεζικής, η διαδικασία απαντήσεων για την αυθεντικοποίηση, και η «μέθοδος PostIdent» που προσφέρεται από το γερμανικό ταχυδρομείο (Deutsche Post AG). Ωστόσο, αυτές οι μέθοδοι καλύπτουν μόνο μια περιορισμένη ομάδα ανθρώπων και είναι αποτελεσματικές σε καθορισμένες σχέσεις που διέπονται από διαφορετικούς κανόνες. Ακολούθως, δεν διαμορφώνουν μια βάση για δομές ταυτότητας γενικής χρήσεως.

Στο **πλαίσιο της ηλεκτρονικής ταυτοποίησης**, για την ταυτοποίηση των κατόχων, πραγματοποιείται **συλλογή και μεταφορά δεδομένων**, παρέχοντας τη δυνατότητα άρσης της συλλογής και μεταφοράς των δεδομένων αυτών.

Επιπρόσθετα οι κάτοχοι μπορούν να αποφασίζουν σχετικά με τη χρήση σε συγκεκριμένες περιπτώσεις. Για το σκοπό αυτό, η καταχώριση του κωδικού αυτού είναι υποχρεωτική. Η ίδια πρόβλεψη ορίζει ότι η μεταφορά δεδομένων λαμβάνει χώρα μόνο, εάν ο πάροχος της υπηρεσίας, για παράδειγμα ο εταίρος της επικοινωνίας, έχει μεταφέρει ένα έγκυρο πιστοποιητικό στον κάτοχο της ταυτότητας. Αυτά τα πιστοποιητικά, εκδίδονται μόνο από παρόχους, των οποίων η επεξεργασία των μεθόδων έχει περάσει από διαδικασίες αξιολόγησης για την προστασία δεδομένων προσωπικού χαρακτήρα. **Τα πιστοποιητικά της**

αυθεντικοποίησης περιέχουν, κυρίως, πληροφορίες σχετικά με τον πάροχο, τις κατηγορίες των μεταφερόμενων δεδομένων και τους σκοπούς του, καθώς και πληροφορίες επικοινωνίας αναφορικά με την Αρχή Προστασίας Προσωπικών Δεδομένων που υπάγεται ο εκτελών την επεξεργασία.

Η Αρχή Προστασίας δύναται να ανακαλέσει τα πιστοποιητικά αυθεντικοποίησης, σε περίπτωση μη ορθής χρήσης των προσωπικών δεδομένων. Ακόμη, τα πιστοποιητικά είναι περιορισμένα ως προς το εύρος της εγκυρότητάς τους. Το σύστημα αυτό λαμβάνει μια θετική αξιολόγηση από τη σκοπιά της προστασίας προσωπικών δεδομένων. Τελικά, το πιστοποιητικό αυθεντικοποίησης δίνει στον κάτοχο της ηλεκτρονικής ταυτότητας τη δυνατότητα να επικυρώσει την ταυτότητα του άλλου μέρους. Αυτό καθιστά τον νομικό έλεγχο ευκολότερο, εάν ανακύψει νομική έριδα.

Η γερμανική ηλεκτρονική ταυτότητα έχει **δύο επιπλέον φιλικές,** για την προστασία δεδομένων, λειτουργίες. Είναι δυνατό να χρησιμοποιηθεί μια υπηρεσία και μία κάρτα με συγκεκριμένο αριθμό (ψευδώνυμο), η οποία χαρακτηρίζεται από ξεχωριστή ηλεκτρονική αναγνώριση της ταυτότητας από τον πάροχο για τον οποίο παρήχθη το ψευδώνυμο αυτό, χωρίς την διαβίβαση επιπρόσθετων προσωπικών δεδομένων. Έπίσης ενα πιστοποιητικό αυθεντικοποίησης μπορεί να περιοριστεί σε συγκεκριμένους τομείς δεδομένων, για παράδειγμα στον τομέα της ηλικίας, ή μιας συγκεκριμένης τοποθεσίας.

Συμπερασματικά, η διπλή δυνατότητα επιλογής που έχει ο πολίτης με τη χρήση ψευδωνύμου και την επιλεκτική δυνατότητα μεταφοράς δεδομένων με την υποχρεωτική καταχώριση του PIN, συνηγορούν στο συμπέρασμα ότι αυτό το μοντέλο είναι πιο κοντά στο στόχο της βέλτιστης προστασίας δεδομένων προσωπικού χαρακτήρα.

Το γερμανικό μοντέλο της ηλεκτρονικής ταυτότητας ακολουθεί μια συγκεκριμένη διαδικασία, π.χ. ταυτοποίηση μέσω του ψηφιακού ελέγχου της ηλεκτρονικής ταυτότητας (identification through visual control of the ID card). Ωστόσο, δεν ισοδυναμεί με την παραδοσιακή ταυτότητα, όσον αφορά την ταυτότητα και την υπογραφή του κατόχου.Οι πάροχοι των εφαρμογών ηλεκτρονικής ταυτοποίησης επομένως πρέπει να βρίσκονται σε επαγρύπνηση σχετικά με το γεγονός αυτό και τους περιορισμούς που συνεπάγονται.

Επειδή η λειτουργία αυτή αντιστοιχεί με την παρουσίαση, αλλά όχι με την αντιγραφή της ταυτότητας, εάν ο πάροχος μιας υπηρεσίας θέλει ή πρέπει να αποδείξει (την εγκυρότητα της ταυτότητας), πρέπει να το κάνει με έμμεσους τρόπους απόδειξης. Τα προβλήματα της απόδειξης που συνεπάγονται σε αυτή την περίπτωση είναι ξεκάθαρα: η καταγραφή πραγματοποιείται από τον πάροχο, όπου σε μια ενδεχόμενη δικαστική διαμάχη, υπάρχει ειδικό ενδιαφέρον για το ένα μέρος της καταγραφής του περιεχομένου, το οποίο χωρίς τα κατάλληλα μέτρα ασφαλείας, θα μπορούσε να τροποποιηθεί και να μην μπορεί να εντοπισθεί.Το ζήτημα αυτό μένει να επιλυθεί από τα γερμανικά δικαστήρια. Σε κάθε περίπτωση, στην περίπτωση κατά την οποία υπάρξουν δικαστικές διενέξεις μεταξύ των τηλεπικοινωνιακών παρόχων και των πελατών τους, έχει ήδη κριθεί ότι η απόδειξη της προσωπικής σύνδεσης λαμβάνεται υπόψη από τα δικαστήρια ως αποδεικτικό μέσο.

Γενικά είναι αναμενόμενο, ότι η ηλεκτρονική απόδειξη της ταυτότητας πρόκειται να έχει διπλές επιπτώσεις στα ζητήματα απόδειξης, όπως για παράδειγμα στις Γερμανικές

υποθέσεις «e-bay», στην οποία η ταυτότητα ή αυθεντικοποίηση ενός χρήστη επιβεβαιώνεται μέσω ενός PIN και TAN, user name και άλλων μηχανισμών.

Το ζήτημα της ασφαλούς ταυτοποίησης με την αρχική επαφή (initial contact), μπορεί να λυθεί, μέσω της ηλεκτρονικής απόδειξης της ταυτότητας, όπως λ.χ. ηλεκτρονικές διαδικασίες αδειοδότησης (πιστοποίησης), ηλεκτρονική παρακολούθηση καταγραφών, εκτέλεση του δικαιώματος πρόσβασης του υποκειμένου στα προσωπικά του δεδομένα.

Η ηλεκτρονική απόδειξη της ταυτότητας βελτιώνει τις λειτουργίες της παραδοσιακής ταυτότητας στη Γερμανία και σε άλλες χώρες και αναβαθμίζει το επίπεδο της ηλεκτρονικής διακυβέρνησης. Συνολικά αναδεικνύεται μια πρόκληση για το σύστημα ταυτοποίησης. Υπάρχουν νέα διοικητικά καθήκοντα, νέες διαδικασίες και νέες συνδέσεις για επικοινωνία και διάδραση, τα οποία απαιτούν ένα νέο ρυθμιστικό πλαίσιο που θα εξασφαλίζει το απαιτούμενο υψηλό επίπεδο προστασίας. Για παράδειγμα, η γερμανική νομοθεσία αναφορικά με την ηλεκτρονική υπογραφή, αφήνει ανοιχτό το ενδεχόμενο της συνεργασίας μεταξύ των αρχών που είναι αρμόδιες για την ταυτοποίηση και των παρόχων υπηρεσιών ταυτοποίησης. Μέσα από αυτή τη συνεργασία, θα ανακύψουν εκτεταμένα ζητήματα προς διασαφήνιση σχετικά με τον ορισμό καθηκόντων, την αστική ευθύνη και τη διαδικασία προσφυγών.

Επιπλέον, είναι χρήσιμο η ηλεκτρονική απόδειξη της ταυτότητας να αξιολογηθεί συνδυαστικά με άλλες δομές ταυτοποίησης, όπως για παράδειγμα της κάρτας υγείας, της απόδειξης της ταυτότητας, το portal της κυβέρνησης. Η τελική εικόνα της «επίσημης ταυτότητας» μεταβάλλεται μαζί με τους μηχανισμούς αλληλεπίδρασης μεταξύ των πολιτών και της διοίκησης. Αυτές οι διαδικασίες είναι εν εξελίξει τόσο στη Γερμανία και σε όλη την Ευρώπη.

5.4. Βέλγιο - Belgian Electronic Identity Card

Η βέλγικη ηλεκτρονική ταυτότητα (Belgian Electronic Identity Card) επιτρέπει στους πολίτες να ταυτοποιηθούν ηλεκτρονικά και να υπογράφουν ηλεκτρονικά έγγραφα. Στο Βέλγιο γίνεται χρήση τεχνολογιών e-ID, για σκοπούς αυθεντικοποίησης. Ωστόσο, το γεγονός αυτό εγείρει ζητήματα προστασίας δεδομένων προσωπικού χαρακτήρα και ασφάλειας, τόσο από την ηλεκτρονική ταυτότητα όσο και από το ενδιάμεσο λογισμικό (Middleware).

Η βελγική ηλεκτρονική ταυτότητα αποτελεί μία έξυπνη κάρτα (αστυνομική ταυτότητα), που επιτρέπει στους Βέλγους πολίτες την ταυτοποίησή τους.

Ιδιωτικές πληροφορίες, όπως το όνομα του ιδιοκτήτη, η διεύθυνσή, η ψηφιακή φωτογραφία του ιδιοκτήτη και ο αριθμός του εθνικού του Μητρώου αποθηκεύονται σε τρία διαφορετικά αρχεία, ένα αρχείο ταυτότητας, όλα υπογεγραμμένα από την κυβέρνηση. Ο μοναδικός αριθμός (ή αλλιώς RRN) αφορά κάθε ένα πολίτη χωριστά. Συνολικά, μια βέλγικη ηλεκτρονική κάρτα εμπεριέχει τρία διαφορετικά 1024-bit RSA ιδιωτικά κλειδιά: ένα για την αυθεντικοποίηση του πολίτη, ένα για τη μη απόρριψη της

ταυτότητας και ένα για την ταυτοποίηση της κάρτας αυτής καθεαυτής, η οποία γίνεται έναντι του Δημοσίου και με τα 3 ιδιωτικά κλειδιά.

Τα δύο PIN κλειδιά επιτρέπουν την ψηφιακή αυθεντικοποίηση και την ψηφιακή υπογραφή. Τα δημόσια κλειδιά βρίσκονται εντός πιστοποιητικού που περιέχει το μοναδικό εθνικό αριθμό και το όνομα του κατόχου της κάρτας, υπογεγραμμένη από κυβερνητική υπηρεσία που εντάσσεται στη δομή PKI. Τα ιδιωτικά κλειδιά αποθηκεύονται σε απαραβίαστο μέρος του τσιπ και μπορεί να διαβαστεί μόνο με ένα κωδικό PIN.

Οι κρυπτογραφικές λειτουργίες της βέλγικης ταυτότητας είναι διαθέσιμες, μέσω ενός ενδιάμεσου λογισμικού, το οποίο περνάει από ένα εργαλείο κλειδώματος και λειτουργεί ως ενδιάμεσος κόμβος για την είσοδο από άλλες εφαρμογές στην ηλεκτρονική ταυτότητα,

Οι εφαρμογές τυπικά, αλληλεπιδρούν με μια κάρτα μέσω ενός απλού API που προσφέρεται από το ενδιάμεσο λογισμικό. Αν ένα έγγραφο πρέπει να υπογραφεί, το ενδιάμεσο λογισμικό περνάει μέσα από ένα εργαλείο κλειδώματος του εγγράφου, στην κάρτα. Ομοίως, το εργαλείο κλειδώματος περνάει στην κάρτα για λόγους ταυτοποίησης. Όταν η εφαρμογή επιθυμεί να αυθεντικοποιήσει ή να υπογράψει ένα έγγραφο με την ηλεκτρονική ταυτότητα, το ενδιάμεσο λογισμικό προσκαλεί τον χρήστη να πληκτρολογήσει τον προσωπικό του κωδικό προκειμένου να επιβεβαιώσει την εγκυρότητα των πιστοποιητικών. Η υπηρεσία της ιδιωτικότητας, μέρος του ενδιάμεσου λογισμικού, αποτρέπει άλλες εφαρμογές να έχουν άμεση είσοδο στην κάρτα. Συνεπώς, ζητείται η συγκατάθεση του χρήστη, όταν μια εφαρμογή προσπαθεί να διαβάσει την ταυτότητα ή να απευθύνει πληροφορία.

Λαμβανομένων υπόψη των παραπάνω, **εξετάζονται διάφορες λύσεις ασφαλείας για τα προσωπικά δεδομένα**. Κάποιες απλές τεχνικές μπορεί να εφαρμοστούν σχετικά με την προστασία προσωπικών δεδομένων στην ηλεκτρονική ταυτότητα.

Μια **πρώτη λύση**, είναι ο **διαχωρισμός των πληροφοριών που περιλαμβάνονται στην ταυτότητα σε περισσότερα αρχεία**. Η είσοδος ορισμένων αρχών, ιδίως στον εθνικό αριθμό, μπορεί να γίνεται μόνο μετά αυθεντικοποίηση.

Μια **δεύτερη λύση** είναι ότι κάθε χαρακτηριστικό-πληροφορία-δεδομένο πρέπει να **κρυπτογραφείται**. Άρα, ο χρήστης μπορεί να επιλέξει μια ομάδα κλειδιών αποκρυπτογράφησης και, ακολούθως, το μέρος των πληροφοριών τα οποία είναι προσβάσιμα στην εφαρμογή.

Μια πιο ευέλικτη τεχνική είναι η **ανωνυμοποίηση των διαπιστευτηρίων**.

Με στόχο να δοθεί περισσότερος έλεγχος στους πολίτες αναφορικά με το χρήστη, πρέπει να υπάρχει **διαφορετικό pin για αυθεντικοποίηση, για υπογραφή και για ανάγνωση.**

Πιστοποιημένοι αναγνώστες μπορεί να έχουν ένα πληκτρολόγιο αναγνώστη και μια μικρή οθόνη. Με τον τρόπο αυτό, οι χρήστες μπορούν να πληκτρολογήσουν με ασφάλεια το Pin τους, χωρίς να χρειάζεται να εμπιστευτούν ενδιάμεσο λογισμικό. Η οθόνη στον

αναγνώστη της κάρτας μπορεί να εμφανίσει την τιμή κατακερματισμού του εγγράφου προς υπογραφή ή των προσωπικών δεδομένων, τα οποία πρόκειται να γνωστοποιηθούν.

Για την επαλήθευση, μόνο πιστοποιημένες κάρτες χρησιμοποιούνται, επομένωσοι κάρτες που αναγιγνώσκονται πρέπει να πιστοποιούνται στην ηλεκτρονική ταυτότητα.

Στην ηλεκτρονική ταυτότητα του Βελγίου και τα **κρυπτογραφικά της χαρακτηριστικά**, εστιάζουμε στην εθνική υποδομή δημοσίου κλειδιού (PKI) και στα πιστοποιητικά ανάκλησης (CRL).

Η ηλεκτρονική κάρτα διαθέτει επιπρόσθετα των πιστοποιητικών, 3 εξειδικευμένα πιστοποιητικά: The Belgium Root CA certificate, the Citizen CA Certificate και το Πιστοποιητικό του Εθνικού Μητρώου.

5.5. Ηνωμένο Βασίλειο - The UK National Identity Card

Το Ηνωμένο Βασίλειο ανέπτυξε ένα σύστημα που μοιάζει με αυτό της Γαλλίας (France Connect). Πρόκειται για Ηλεκτρονική Ταυτότητα (National Identity Card), για την απόκτηση της οποίας οι πολίτες εγγράφονται στην πλατφόρμα GOV.UK Verify. Η εισαγωγή της ηλεκτρονικής ταυτότητας συνδέθηκε με ζητήματα που άπτονται της προστασίας δεδομένων προσωπικού χαρακτήρα.

Παρακάτω παρατίθενται τα κύρια χαρακτηριστικά των συστημάτων ταυτοποίησης που έχουν αξιολογηθεί ως ορθά, με τα εξής κριτήρια:

- **Καθολικότητα της κάλυψης**: ένα άτομο πρέπει να έχει ένα αναγνωριστικό για κάθε τομέα.

- **Μοναδικότητα**: κάθε άτομο πρέπει να έχει ένα αναγνωριστικό που δεν το έχει κανένας άλλος.

- **Μονιμότητα**: το αναγνωριστικό δεν πρέπει να αλλάζει, ούτε να μπορεί να αλλάξει, χωρίς έγκριση. Αυτό σημαίνει ότι το αναγνωριστικό πρέπει να μην μπορεί να τύχει απομνημόνευσης, εκτός εάν κάποια ουσιώδης σύνδεση έχει οικοδομηθεί πάνω στο αναγνωριστικό. Σε αυτήν την περίπτωση, η σύνδεση αυτή πρέπει να αλλάζει συν τω χρόνω.

- **Αναγκαιότητα**: το αναγνωριστικό πρέπει να μπορεί να χρησιμοποιηθεί ανά πάσα στιγμή.

- **Αποκλειστικότητα**: καμία άλλη μορφή ταυτοποίησης δεν πρέπει να χρειάζεται ή να χρησιμοποιείται.

Η εισαγωγή εθνικού αναγνωριστικού είναι προαπαιτούμενο για τη θέσπιση τεχνολογίας όπως αυτής του smartcard. Εξάλλου, πέραν κάθε αμφιβολίας, ένα κοινό και σταθερό αναγνωριστικό συμβάλλει στην εφαρμογή της συνεκτικής διακυβέρνησης και στην εισαγωγή της διαλειτουργικότητας στις ηλεκτρονικές υπηρεσίες.

Ένα εθνικό αναγνωριστικό μπορεί να είναι ένα κωδικός ή ένα βιομετρικό στοιχείο. Μια έξυπνη κάρτα, είναι ένα τόκεν, που ενσωματώνει τον αναγνωριστικό κωδικό. Με όρους πρόσβασης στην έκδοση της κάρτας, μπορούμε να διακρίνουμε μεταξύ των παρακάτω τρόπων:

- **Πρόσωπο με πρόσωπο**
- **Με κινητό τηλέφωνο.** Ο πολίτης είναι πιθανό να του ζητηθεί να διαβάσει το νούμερο της ταυτοποίησης και πιθανόν άλλες μορφές αυθεντικοποίησης, όπως την τοποθεσία από την οποία συνδέεται.
- **PC/PIAP.** Η μόνιμη μορφή πρόσβασης μέσω της συσκευής είναι πιθανό να περιλαμβάνει την πληκτρολόγηση του αναγνωριστικού και το password.

Ως προς την εφαρμογή ενός συστήματος ταυτότητας, κάποιοι ειδικοί έχουν υποστηρίξει ότι η συγκεκριμένη βάση δεδομένων είναι πολύ περίπλοκη και ότι η βιομετρική τεχνολογία βασίζεται σε πυλώνες που στηρίζονται σε ένα επαρκή αριθμό χρηστών.

Υπάρχει, επίσης, απόδειξη ότι αντί των υποδομών που λειτουργούν ως καταλύτης για την ενσωμάτωση των δεδομένων της κυβέρνησης, 19 διαφορετικά σχέδια για την ενσωμάτωση βρίσκονται στο Ηνωμένο Βασίλειο.

Ένα στοιχείο- κλειδί είναι το περίφημο **delivery service**. Αυτό το σημείο κλειδί απαιτεί **πληροφοριακά συστήματα της Κυβέρνησης** γεγονός που συνεπάγεταιμεγαλύτερη ενσωμάτωση και διαλειτουργικότητα συστημάτων. Ένα κοινό αναγνωριστικό θα διευκόλυνε την ενσωμάτωση των συστημάτων και θα βελτίωνε τη διαλειτουργικότητα. Υπάρχει δε συζήτηση σχετικά με την ανάγκη να αποθηκευτούν τα δεδομένα της ταυτότητας σε ένα κεντρικό μητρώο.

Υποστηρίζεται ότι η πολλαπλάσια διαχείριση της ταυτότητας καθιστά απαραίτητη τη διασφάλιση της ιδιωτικότητας. Συνέπεια αυτού, είναι ότι **τα αναγνωριστικά πρέπει να είναι σαφώς διαφορετικά για κάθε ξεχωριστό σύστημα ανθρώπινων δραστηριοτήτων.** Επίσης, αναφέρεται ότι η αυθεντικοποίηση μπορεί να επιτευχθεί, μέσω μιας έξυπνης κάρτας που θα εμπεριέχει αποθηκευμένα τα δεδομένα ταυτότητας. Το αποθετήριο των δεδομένων αυτών δεν απαιτείται για αυθεντικοποίηση. Αυτή είναι μια ακόμη πιο πρακτική προσέγγιση για να χτιστεί η δομή της ταυτότητας προκειμένου να είναι λιγότερο περίπλοκη και λιγότερο δαπανηρή.

Στο παράδειγμα της Γερμανίας[21] οι πολίτες υποχρεωτικά πρέπει να θυμούνται ένα Pin για την πρόσβασή τους σε δημόσιες τοπικές ηλεκτρονικές υπηρεσίες. Στις Η.Π.Α. ο αριθμός Κοινωνικής Ασφάλισης είναι απαραίτητος για τις περισσότερες συναλλαγές, ενώ οι άδειες οδήγησης είναι ψηφιακές και λειτουργούν ως ανεπίσημες ταυτότητες.

Δημιουργώντας μια ενσωματωμένη back-end Information and Communication δομή: Η διαχείριση των λειτουργικών δεδομένων είναι κρίσιμης σημασίας στην back-end δομή. Για παράδειγμα, όταν ένας πελάτης εισάγει προσωπικές πληροφορίες, όπως το όνομα και τη διεύθυνσή του, σε ένα σύστημα, πρέπει ιδανικά αυτά να είναι διαθέσιμα σε όλα τα συστήματα, που «χρειάζονται» τα συγκεκριμένα δεδομένα.

[21] Personnal Identification in the Information Age: The Case of the in the UK.

II. Ενωσιακό Δίκαιο για την ψηφιακή ταυτοποίηση

1. Ο Κανονισμός (ΕΕ) αριθ. 910/2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά (eIDAS)

Στην παρούσα ενότητα, επιχειρείται η παρουσίαση του Κανονισμού (ΕΕ) **αριθ. 910/2014** σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά (εφεξής Κανονισμός eIDAS), καθώς και η αξιολόγηση της εφαρμογής του στην πράξη μέχρι σήμερα, σύμφωνα με αξιολόγηση της Ευρωπαϊκής Επιτροπής.

1.1. Η παρουσίαση του Κανονισμού (ΕΕ) αριθ. 910/2014

Ο Κανονισμός (ΕΕ) αριθ. 910/2014/ Κανονισμός eIDAS εκδόθηκε το 2014 και η Ε.Ε. πρωτοπόρησε, θεσπίζοντας παγκοσμίως το πρώτο διασυνοριακό πλαίσιο για την επίτευξη αξιόπιστων ψηφιακών ταυτοτήτων και υπηρεσιών εμπιστοσύνης.

Κύριος στόχος του Κανονισμού eIDAS ήταν **η παροχή πρόσβασης στο σύνολο των πολιτών της Ε.Ε. σε δημόσιες υπηρεσίες σε όλη την ευρωπαική Επικράτεια,** με αξιοποίηση μέσων ηλεκτρονικής ταυτοποίησης, όπως αυτά εκδίδονται στη χώρα καταγωγής τους, ήτοι σε κάποιο κράτος-μέλος της Ε.Ε. Παράλληλα, στόχος του Κανονισμού ήταν **η ενίσχυση της εμπιστοσύνης στις ηλεκτρονικές συναλλαγές, στο πλαίσιο της εσωτερικής αγοράς**, μέσω της παροχής κοινού πλαισίου που θα διασφαλίζει τις ασφαλείς και εύχρηστες ηλεκτρονικές αλληλεπιδράσεις των πολιτών, των επιχειρήσεων και των δημοσίων φορέων, για την ενδυνάμωση της αποτελεσματικότητας των δημόσιων και ιδιωτικών επιγραμμικών[22] υπηρεσιών, του ηλεκτρονικού επιχειρείν, του ηλεκτρονικού εμπορίου και των ιδιωτικών επιγραμμικών υπηρεσιών.

Είναι χαρακτηριστικό ότι ο Κανονισμός eIDAS κατήργησε την Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.[23]ΗΟδηγία αφενός αφορούσε περιορισμένα μόνο το πεδίο των ηλεκτρονικών υπογραφών αφετέρου, δεν διασφάλιζε την ομοιόμορφη εφαρμογή των κανόνων στα κράτη-μέλη, συγκριτικά με τον Κανονισμό άμεσης εφαρμογής.

Νομική βάση του Κανονισμού eIDAS αποτέλεσε το άρθρο 114 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης[24], το οποίο **αποβλέπει** στην άρση των υφιστάμενων

[22] Όπου γίνεται χρήση του όρου «επιγραμμικός», εννοούμε on-line. Θα μπορούσε ο όρος ορθότερα να αποτυπωθεί ως διαδικτυακός, αφού η μετάφραση που ακολουθείται δεν είναι δόκιμη στην ελληνική γλώσσα για τον απλό πολίτη.

[23] Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:01999L0093-20081211&from=EN

[24] 1. Εκτός αν ορίζουν άλλως οι Συνθήκες, εφαρμόζονται οι ακόλουθες διατάξεις για την πραγματοποίηση των στόχων του άρθρου 26. Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο,

φραγμών στη λειτουργία της εσωτερικής αγοράς, μέσω της προώθησης της προσέγγισης των θεσμικών πλαισίων των κρατών-μελών, ιδίως στο πεδίο της αμοιβαίας αναγνώρισης και αποδοχής της ηλεκτρονικής ταυτοποίησης, της επαλήθευσης ταυτότητας, της ηλεκτρονικής υπογραφής και των σχετικών υπηρεσιών εμπιστοσύνης **σε διασυνοριακό επίπεδο,** για τη διασφάλιση της πρόσβασης σε ηλεκτρονικές διαδικασίες και συναλλαγές καθώς και για την ολοκλήρωση αυτών.

Σημειώνεται ότι, πριν την έναρξη ισχύος του Κανονισμού eIDAS **απουσίαζε ένα ολοκληρωμένο διασυνοριακό και διατομεακό πλαίσιο στην Ε.Ε. για ασφαλείς, αξιόπιστες**

αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία και μετά από διαβούλευση με την Οικονομική και Κοινωνική Επιτροπή, **εκδίδουν τα μέτρα, σχετικά με την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που έχουν ως αντικείμενο την εγκαθίδρυση και τη λειτουργία της εσωτερικής αγοράς.**

2. Η παράγραφος 1 δεν εφαρμόζεται στις φορολογικές διατάξεις, στις διατάξεις για την ελεύθερη κυκλοφορία των προσώπων και στις διατάξεις για τα δικαιώματα και τα συμφέροντα των μισθωτών.

3. Η Επιτροπή, στις προτάσεις της που προβλέπονται στην παράγραφο 1, σχετικά με την υγεία, την ασφάλεια, την προστασία του περιβάλλοντος και την προστασία των καταναλωτών, λαμβάνει ως βάση ένα υψηλό επίπεδο προστασίας, λαμβάνοντας ιδίως υπόψη όσες νέες εξελίξεις βασίζονται σε επιστημονικά δεδομένα. Στο πλαίσιο των αντίστοιχων αρμοδιοτήτων τους, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο επιδιώκουν επίσης την επίτευξη αυτού του στόχου.

4. Όταν, μετά τη θέσπιση μέτρου εναρμόνισης από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, από το Συμβούλιο ή από την Επιτροπή, ένα κράτος μέλος θεωρεί αναγκαίο να διατηρήσει εθνικές διατάξεις που δικαιολογούνται από τις επιτακτικές ανάγκες που προβλέπονται στο άρθρο 36 ή διατάξεις σχετικές με την προστασία του περιβάλλοντος ή του χώρου εργασίας, τις κοινοποιεί στην Επιτροπή, καθώς και τους λόγους διατήρησής τους.

5. Επίσης, υπό την επιφύλαξη της παραγράφου 4, εάν, μετά τη θέσπιση μέτρου εναρμόνισης από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, από το Συμβούλιο ή από την Επιτροπή, ένα κράτος μέλος θεωρεί αναγκαία τη θέσπιση εθνικών διατάξεων επί τη βάσει νέων επιστημονικών στοιχείων σχετικών με την προστασία του περιβάλλοντος ή του χώρου εργασίας, για λόγους οι οποίοι συντρέχουν μόνον στην περίπτωσή του και οι οποίοι έχουν ανακύψει μετά τη θέσπιση του μέτρου εναρμόνισης, κοινοποιεί στην Επιτροπή τις μελετώμενες διατάξεις και τους λόγους που υπαγορεύουν τη θέσπισή τους.

6. Η Επιτροπή, εντός έξι μηνών από τις κοινοποιήσεις που αναφέρονται στις παραγράφους 4 και 5, εγκρίνει ή απορρίπτει τις εν λόγω εθνικές διατάξεις, αφού εξακριβώσει εάν αποτελούν ή όχι μέσο αυθαιρέτων διακρίσεων ή συγκεκαλυμμένο περιορισμό του εμπορίου μεταξύ των κρατών μελών, και εάν συνιστούν ή όχι εμπόδιο στη λειτουργία της εσωτερικής αγοράς. Εάν η Επιτροπή δεν αποφασίσει εντός αυτής της περιόδου, οι εθνικές διατάξεις, περί των οποίων οι παράγραφοι 4 και 5, λογίζονται ότι έχουν εγκριθεί. Εάν η πολυπλοκότητα του αντικειμένου το δικαιολογεί, και δεν υπάρχει κίνδυνος για την υγεία του ανθρώπου, η Επιτροπή μπορεί να κοινοποιήσει στο συγκεκριμένο κράτος μέλος ότι η περίοδος η αναφερόμενη στην παρούσα παράγραφο μπορεί να παραταθεί μέχρι ένα εξάμηνο.

7. Οσάκις, σύμφωνα με την παράγραφο 6, επιτρέπεται σε ένα κράτος μέλος να διατηρήσει ή να εισαγάγει εθνικές διατάξεις παρεκκλίνουσες από το μέτρο εναρμόνισης, η Επιτροπή εξετάζει πάραυτα μήπως πρέπει να προτείνει αναπροσαρμογή του εν λόγω μέτρου.

8. Όταν ένα κράτος μέλος επικαλείται συγκεκριμένο πρόβλημα δημόσιας υγείας σε τομέα στον οποίο έχουν ήδη ληφθεί μέτρα εναρμόνισης, το θέτει υπόψη της Επιτροπής η οποία αμέσως εξετάζει αν πρέπει να προτείνει κατάλληλα μέτρα στο Συμβούλιο.

9. Κατά παρέκκλιση από τη διαδικασία των άρθρων 258 και 259 η Επιτροπή ή κάθε κράτος μέλος δύναται να προσφύγει απευθείας στο Δικαστήριο της Ευρωπαϊκή Ένωσης, για το θέμα αυτό, εάν κρίνει ότι ένα άλλο κράτος μέλος ασκεί καταχρηστικώς τις εξουσίες που προβλέπονται στο παρόν άρθρο.

10. Τα προαναφερόμενα μέτρα εναρμόνισης περιλαμβάνουν, στις ενδεδειγμένες περιπτώσεις, ρήτρα διασφάλισης που επιτρέπει στα κράτη μέλη να λαμβάνουν, για έναν ή περισσότερους από τους μη οικονομικούς λόγους που προβλέπονται στο άρθρο 36, προσωρινά μέτρα υποκείμενα σε διαδικασία ελέγχου της Ένωσης.

και εύχρηστες ηλεκτρονικές συναλλαγές, το οποίο μάλιστα να περιλαμβάνει την ηλεκτρονική ταυτοποίηση, την επαλήθευση ταυτότητας και τις υπηρεσίες εμπιστοσύνης. Η θεσμοθέτησή του εκκίνησε με την πρόταση της Επιτροπής [COM(2012) 238 final] της 4ης Ιουνίου 2012, η οποία συνοδεύτηκε από εκτίμηση των επιπτώσεων, και έθεσε τέσσερις γενικούς στόχους: α) διασφάλιση της ανάπτυξης της ψηφιακής ενιαίας αγοράς, β) προώθηση της ανάπτυξης βασικών διασυνοριακών δημόσιων υπηρεσιών, γ) τόνωση και ενίσχυση του ανταγωνισμού στην ενιαία αγορά και δ) ενίσχυση του φιλικού για τον χρήστη (πολίτες και επιχειρήσεις) χαρακτήρα.

Παρά το στρατηγικό πλεονέκτημα της Ε.Ε. και το θετικό πρόσημο του Κανονισμού eIDAS στην επίτευξη των στόχων που τέθηκαν και τη διευκόλυνση της ενιαίας αγοράς σε επιμέρους τομείς, όπως λ.χ. στις χρηματοπιστωτικές υπηρεσίες, τις διοικητικές διαδικασίες με επαναχρησιμοποίηση δεδομένων, κ.λπ., ο Κανονισμός eIDAS **υπόκειται σε ορισμένους περιορισμούς**. Ειδικότερα, απουσιάζει η υποχρέωση κοινοποίησης των εθνικών συστημάτων ηλεκτρονικής ταυτοποίησης, περιλαμβάνει περιορισμένα χαρακτηριστικά (στοιχεία προσωπικών πληροφοριών) που μπορεί να γνωστοποιηθούν αξιόπιστα σε τρίτους, εστιάζει στην πράξη στο δημόσιο τομέα και απουσιάζουν σαφή κίνητρα για τη χρήση των εθνικών ηλεκτρονικών ταυτοτήτων από τους ιδιώτες.

Ο Κανονισμός eIDAS καθιστά δυνατή τη διασυνοριακή αναγνώριση των δημόσιων ηλεκτρονικών ταυτοτήτων για την πρόσβαση σε δημόσιες υπηρεσίες, υπό την προϋπόθεση ότι η ηλεκτρονική ταυτότητα έχει κοινοποιηθεί στο πλαίσιο του Κανονισμού eIDAS. Επιπλέον, το ευρωπαϊκό οικοσύστημα ηλεκτρονικής ταυτότητας είναι κατακερματισμένο μεταξύ των διαφόρων εθνικών κανονιστικών πλαισίων, επιπέδων ψηφιακής διακυβέρνησης, πολιτισμικών χαρακτηριστικών, καθώς και των διαφορετικών επιπέδων εμπιστοσύνης στους δημόσιους θεσμούς.

Περαιτέρω, **έχει μεταβληθεί άρδην το ψηφιακό περιβάλλον**, το οποίο διακρίνεται από **μεγάλο αριθμό παραγόντων** που το επηρεάζουν, **όπως οντότητες** (τράπεζες, πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών, εταιρείες κοινής ωφέλειας), **που συχνά ενεργούν ως εγκεκριμένοι πάροχοι ταυτότητας των προσώπων.** Παράλληλα, δραστηριοποιούνται διαδικτυακοί ενδιάμεσοι, όπως μεγάλες πλατφόρμες μέσων κοινωνικής δικτύωσης και φυλλομετρητών του Διαδικτύου, που δρουν ως ρυθμιστές της ψηφιακής ταυτότητας και προσφέρουν λύσεις τύπου BYOI (‘‘bring your own identity’’/ «φέρτε τη δική σας ταυτότητα»), ώστε να επιτρέπεται στους χρήστες να επαληθεύουν την ταυτότητά τους σε ιστοτόπους και υπηρεσίες τρίτων που χρησιμοποιούν τα προφίλ χρήστη. Με τον τρόπο αυτό, όμως, αν και διευκολύνεται η επαλήθευση της ταυτότητας, επέρχεται απώλεια του ελέγχου επί των δεδομένων προσωπικού χαρακτήρα που διακινούνται και γνωστοποιούνται, καθώς δεν διασφαλίζεται η επαληθευμένη φυσική ταυτότητα του χρήστη, με αποτέλεσμα να επιτρέπεται η ηλεκτρονική απάτη και να δημιουργούνται εν γένει κίνδυνοι για την κυβερνοασφάλεια.

Υπό τις διαπιστώσεις αυτές, καθίσταται σαφές ότι αφενός οι πολίτες της Ε.Ε. θα επιθυμούσαν να έχουν απρόσκοπτη πρόσβαση σε ασφαλή ψηφιακή ταυτότητα τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα, λαμβάνοντας υπόψη ότι αυξάνεται ο αριθμός των ευαίσθητων και εξατομικευμένων παρεχόμενων υπηρεσιών, αφετέρου τα κράτη-μέλη

πρέπει να διαδραματίσουν σημαντικό ρόλο για την ανάπτυξη οικοσυστήματος ψηφιακής ταυτοποίησης, ώστε η ηλεκτρονική ταυτοποίηση να γίνεται με αξιόπιστο τρόπο και να παρέχονται υπηρεσίες εμπιστοσύνης, με έμφαση στην ασφάλεια, την ευχέρεια και την αποτελεσματικότητα των επιγραμμικών συναλλαγών.

1.2. Η αξιολόγηση του Κανονισμού (ΕΕ) αριθ. 910/2014

Η παρούσα ενότητα αξιολόγησης του Κανονισμού (ΕΕ) αριθ. 910/2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά (eIDAS) βασίζεται στην «**Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο όσον αφορά την αξιολόγηση του Κανονισμού (ΕΕ) αριθ. 910/2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά (eIDAS)** (**COM/2021/290 final/3.6.2021)**», σύμφωνα με το άρθρο 49 του Κανονισμού[25] που απαιτεί επανεξέταση του Κανονισμού από την Επιτροπή καθώς και αξιολόγηση, ιδίως αν είναι σκόπιμο να τροποποιηθεί το πεδίο εφαρμογής του ή συγκεκριμένες διατάξεις του, βάσει των τεχνολογικών, εμπορικών και νομικών εξελίξεων αλλά και το βαθμού εφαρμογής του.[26]

Επί της ουσίας του Κανονισμού eIDAS, η Επιτροπή κατέληξε σε ορισμένα **συμπεράσματα ως προς την αξιολόγησή του**. Αναλυτικότερα, συνοψίζονται τα ακόλουθα:

1. Με βάση το κριτήριο της αποτελεσματικότητας, οι διατάξεις του Κανονισμού οδήγησαν στη δημιουργία του δικτύου eIDAS, που αποσκοπεί στην παροχή δυνατότητας πρόσβασης σε επιγραμμικές δημόσιες υπηρεσίες σε διασυνοριακό επίπεδο, ωστόσο στην Ε.Ε. η **διαλειτουργικότητα αποτυπώνεται σε χαμηλό βαθμό ως προς τα συστήματα ηλεκτρονικής ταυτοποίησης**. Έτσι, ναι μεν ο Κανονισμός διασφάλισε την ασφάλεια δικαίου ως προς την ευθύνη, το βάρος της απόδειξης, τη νομική ισχύ και τις διεθνείς πτυχές των υπηρεσιών εμπιστοσύνης, αλλά παρατηρείται διαφοροποίηση μεταξύ των κρατών-μελών και των επιμέρους υπηρεσιών εμπιστοσύνης.

Επομένως, από τη μία πλευρά έχουν επιτευχθεί ορισμένοι στόχοι του Κανονισμού, αλλά ο τελευταίος δεν έχει καταφέρει να αξιοποιήσει πλήρως τη δυναμική του στο πεδίο της αποτελεσματικότητας, αφού, όπως προαναφέρθηκε, είναι περιορισμένος ο αριθμός των ηλεκτρονικών ταυτοτήτων που έχει κοινοποιηθεί. Έτσι, καλύπτεται **περιορισμένος αριθμός**

[25] «Η Επιτροπή προβαίνει σε επανεξέταση της εφαρμογής του παρόντος κανονισμού και υποβάλλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο το αργότερο την 1η Ιουλίου 2020. Η Επιτροπή αξιολογεί ιδίως αν είναι σκόπιμο να τροποποιηθεί το πεδίο εφαρμογής του παρόντος κανονισμού ή συγκεκριμένων διατάξεών του, συμπεριλαμβανομένου του άρθρου 6, του άρθρου 7 στοιχείο στ) και των άρθρων 34, 43, 44 και 45, λαμβανομένης υπόψη της πείρας από την εφαρμογή του παρόντος κανονισμού, καθώς και των τεχνολογικών, εμπορικών και νομικών εξελίξεων».

[26] Ευρωπαική Επιτροπή, Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο όσον αφορά την αξιολόγηση του Κανονισμού (ΕΕ) αριθ. 910/2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά (eIDAS) (COM/2021/290 final/3.6.2021).
Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:52021DC0290

πολιτών της Ε.Ε., δεν έχουν τεθεί σε λειτουργία όλοι οι κόμβοι eIDAS, λίγες δημόσιες υπηρεσίες προσφέρουν την κοινοποίηση eIDAS, ενώ λόγω τεχνικών σφαλμάτων παρατηρείται και μη αποτελεσματική επαλήθευση της ταυτότητας χρηστών. Επίσης, παρατηρείται απουσία κοινών τεχνικών απαιτήσεων μεταξύ των κρατών-μελών, λόγω της μη έκδοσης πρόσθετων εκτελεστικών πράξεων της Ε.Ε.., με αποτέλεσμα να μη διασφαλίζονται ισότιμοι όροι ανταγωνισμού σε ευρωπαϊκό επίπεδο. Παρόλα αυτά, πρέπει να αναγνωριστεί ότι ο Κανονισμός έχει αποτελέσει μία ισχυρή θεσμική βάση, η οποία μπορεί να επικαιροποιηθεί και να συμπληρωθεί με τα αναγκαία πρότυπα και τις απαιτήσεις, για τη μείωση του κατακερματισμού της αγοράς και των αποκλίσεων μεταξύ των εποπτικών φορέων και των οργανισμών αξιολόγησης της συμμόρφωσης, καθώς και να επιτευχθεί η ενίσχυση της συνεργασίας μεταξύ των εποπτικών φορέων.

2. Στο πεδίο της αποδοτικότητας, διαπιστώνεται εκ μέρους της Επιτροπής ότι το **κόστος που είναι εφικτό να ποσοτικοποιηθεί είναι υψηλότερο από τα οφέλη, λόγω του χαμηλού βαθμού υιοθέτησης της ηλεκτρονικής ταυτοποίησης**. Οι βασικές ομάδες ενδιαφερομένων για τις οποίες το μέρος του Κανονισμού eIDAS που αφορά στην ηλεκτρονική ταυτοποίηση έχει δημιουργήσει κόστος και οφέλη, είναι οι εθνικές αρχές, οι φορείς εκμετάλλευσης κόμβων eIDAS, οι πάροχοι υπηρεσιών ηλεκτρονικής ταυτοποίησης και οι πάροχοι υπηρεσιών.

Επίσης, αναφορικά με τις υπηρεσίες εμπιστοσύνης, οι βασικές ομάδες ενδιαφερομένων που επιβαρύνθηκαν με τις βασικές δαπάνες και έλαβαν τα κυριότερα οφέλη είναι οι φορείς διαπίστευσης, οι οργανισμοί αξιολόγησης της συμμόρφωσης, οι εποπτικοί φορείς και οι εγκεκριμένοι και μη εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης. Σημειώνεται ακόμη, ότι οι πάροχοι υπηρεσιών εμπιστοσύνης καταγράφουν οφέλη με τη μορφή εσόδων, λόγω της παροχής υπηρεσιών εμπιστοσύνης σε άλλες χώρες της Ε.Ε. και της επέκτασης της βάσης της αγοράς.

3. Με βάση το κριτήριο της συνάφειας, παρατηρείται ότι, σε σχέση με την περίοδο θέσπισης του Κανονισμού eIDAS, έχει αλλάξει δραματικά το παγκόσμιο οικοσύστημα ηλεκτρονικής ταυτοποίησης, ιδίως λόγω της αυξημένης συμμετοχής των ιδιωτικών παρόχων ταυτότητας, της υπέρογκης αύξησης των ψηφιακών συναλλαγών και των κινδύνων που απορρέουν αναφορικά με την ασφαλή και διαλειτουργική ψηφιακή ταυτότητα των χρηστών. Ωστόσο, δεν θεωρείται ότι οι στόχοι του Κανονισμού eIDAS είναι απαρχαιωμένοι, αφού εξακολουθεί να **αποτελεί ζητούμενο η διασφάλιση της μείωσης του κατακερματισμού της αγοράς**, με την παροχή διασυνοριακής και διατομεακής διαλειτουργικότητας των υπηρεσιών εμπιστοσύνης, με θέσπιση κοινών προτύπων, ωστόσο φαίνεται περιορισμένη η αξιοποίηση του Κανονισμού και στο πεδίο των επιγραμμικών δημοσίων υπηρεσιών.

Ένα βασικό μειονέκτημα του Κανονισμού αποτελεί το γεγονός ότι δεν έχει καταφέρει να ανταποκριθεί στις ανάγκες ορισμένων τομέων, όπως η εκπαίδευση, ο τραπεζικός κλάδος, η αεροπορία, τα ταξίδια, κ.λπ., αφού ελλείπουν ειδικά χαρακτηριστικά και πρότυπα ανά τομέα. Επίσης, ο Κανονισμός δεν έχει καταφέρει να εναρμονίζεται με τις πρόσφατες τεχνολογικές εξελίξεις στον τομέα των υπηρεσιών εμπιστοσύνης (καθιέρωση υπηρεσίας εμπιστοσύνης για την ηλεκτρονική αρχειοθέτηση, υπηρεσίας εμπιστοσύνης που

θα υποστηρίζει φορητά διαπιστευτήρια ταυτότητας και υπηρεσίας εμπιστοσύνης για ηλεκτρονικά λογιστικά βιβλία, κ.λπ.), με αποτέλεσμα να μην ανταποκρίνεται στις ανάγκες των πολιτών της Ε.Ε..

4. **Ο Κανονισμός στο πεδίο της ηλεκτρονικής ταυτοποίησης διακρίνεται από συνεκτικό σύστημα για την αμοιβαία αναγνώριση των ηλεκτρονικών ταυτοτήτων**, με βάση αφενός την κοινοποίηση αφετέρου την αξιολόγηση από ομότιμους. Επίσης, το πεδίο των υπηρεσιών εμπιστοσύνης χαρακτηρίζεται από συνεκτικό σύστημα εποπτείας ως προς αυτές. Ωστόσο, ακόμα εντοπίζονται δυσλειτουργίες στην εσωτερική συνοχή του Κανονισμού, κυρίως γιατί ως προς τις ηλεκτρονικές ταυτότητες το σύστημα κοινοποίησης και αξιολόγησης από ομότιμους, παρότι αποβλέπει στην εξασφάλισης κοινής αντίληψης, η εξασφάλιση αυτή δεν συμβαίνεισε κάθε περίπτωση, γιατί δεν υπάρχει πάντοτε κοινή αντίληψη για το επίπεδο διασφάλισης των δικαιωμάτων των πολιτών.

Έτσι, παρότι ο Κανονισμός προωθεί την ευελιξία και την τεχνολογική ουδετερότητα ως προς τα εθνικά μέτρα των κρατών-μελών, δεν διασφαλίζεται κοινή αντίληψη στο πεδίο των διαβιβαζόμενων δεδομένων για την ταυτοποίηση του χρήστη αναφορικά με τις δημόσιες υπηρεσίες. Αποτέλεσμα η μη ομοιόμορφη εφαρμογή και η μη εναρμόνιση με τις αρχές του **Γενικού Κανονισμού Προσωπικών Δεδομένων** ως προς την ελαχιστοποίηση των δεδομένων και την προστασία της ιδιωτικής ζωής του ατόμου, μέσω του ελέγχου του καθορισμού του αριθμού και τύπου δεδομένων πρέπει να κοινοποιούνται και σε ποιον φορέα. Παράλληλα, δημιουργείται ανασφάλεια δικαίου και μη ισότιμη διασφάλιση των όρων του ελεύθερου ανταγωνισμού, εξαιτίας του γεγονότος ότι ορισμένα κράτη-μέλη διαθέτουν κανονιστικό πλαίσιο που αναγνωρίζει ορισμένες μεθόδους ταυτοποίησης, όπως η βιομετρική επαλήθευση. Επιπλέον, ως προς την αξιολόγηση των παρόχων υπηρεσιών εμπιστοσύνης έναντι των λειτουργικών απαιτήσεων του Κανονισμού για την απόκτηση έγκρισης υπάρχουν αδυναμίες, καθόσον ο ρόλος των οργανισμών αξιολόγησης της συμμόρφωσης δεν ρυθμίζεται λεπτομερώς αναφορικά με τις υποχρεώσεις, την ευθύνη ή το επίπεδο ικανότητας.

5. Δεν μπορεί να παραγνωριστεί ότι ο Κανονισμός eIDAS έθεσε τις θεσμικές βάσεις για την ανάπτυξη εθνικών λύσεων ηλεκτρονικής ταυτοποίησης, ωστόσο παρατηρούνται κάποιοι περιορισμοί ως προς την προστιθέμενη αξία του πλαισίου ηλεκτρονικής ταυτοποίησης, λόγω της χαμηλής υιοθέτησής τους και χρήσης τους στην πράξη. Ωστόσο, αναφορικά με τις υπηρεσίες εμπιστοσύνης παρατηρείται ότι υπάρχει επαρκές κοινό πλαίσιο για τη χρήση τους, περιορίζοντας τον κατακερματισμό της αγοράς και την ενίσχυση της υιοθέτησής τους. Το γεγονός αυτό είναι ιδιαίτερα σημαντικό, αφού έτσι οι δημόσιες διοικήσεις μπορεί να ψηφιοποιήσουν επαρκώς τις υπηρεσίες τους, παράγοντας ψηφιακά αποδεικτικά στοιχεία και μειώνοντας το αντίστοιχο διοικητικό βάρος. Αναφορικά με την ηλεκτρονική ταυτοποίηση προκρίνεται η υιοθέτηση προσαρμογών του **θεσμικού πλαισίου του Κανονισμού, όπως η διευκόλυνση της χρήσης αξιόπιστων δημόσιων ηλεκτρονικών ταυτοτήτων** από τον ιδιωτικό τομέα και για την ανταλλαγή ειδικών χαρακτηριστικών και διαπιστευτηρίων που παρέχονται από το δημόσιο και τον ιδιωτικό τομέα. Επίσης, πρέπει να αρθούν ορισμένες διαφοροποιημένες εθνικές ερμηνείες αναφορικά με τις υπηρεσίες εμπιστοσύνης, για την απόκτηση μιας πλήρους κοινής αντίληψης.

1.3. Η αναθεώρηση του Κανονισμού (ΕΕ) αριθ. 910/2014

Από τα ανωτέρω, **καθίσταται προφανές ότι ο Κανονισμός eIDAS αποτελεί ακρογωνιαίο λίθο για τη διασφάλιση ενιαίας αγοράς σε επιμέρους τομείς**, **όπως** στον **τραπεζικό,** για την παροχή ορισμένων δεδομένων ταυτότητας, και τη διευκόλυνση συμμόρφωσης με τους κανόνες που αφορούν στην καταπολέμηση της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες[27]. Παράλληλα ο **Κανονισμός eIDAS** αποτελεί καταλυτικό παράγοντα για την εφαρμογή και το αντικείμενο της **Οδηγίας για τις υπηρεσίες πληρωμών** (PSD2)[28] που στηρίζεται σε υπηρεσίες εμπιστοσύνης του συστήματος eIDAS, όπως οι ηλεκτρονικές σφραγίδες και τα εγκεκριμένα πιστοποιητικά για επαλήθευση της ταυτότητας ιστοτόπων (Qualified Website Authentication Certificate, QWAC) για την εξακρίβωση της γνησιότητας ιστοτόπων από τρίτους παρόχους πληρωμών, κ.ά.

Επίσης, η **ηλεκτρονική ταυτοποίηση μέσω του eIDAS συνιστά προϋπόθεση για τη διασυνοριακή ανταλλαγή διοικητικών πιστοποιητικών** και το πλαίσιο eIDAS είναι απαραίτητο για την **επιτυχή εφαρμογή και λειτουργία της αρχής «μόνον άπαξ»** (Once-only principle, OOP) από το 2023.[29]

Σε κάθε περίπτωση, **το θεσμικό πλαίσιο του eIDAS ως προς τις υπηρεσίες εμπιστοσύνης έχει τύχει διεθνούς αναγνώρισης και συνιστά το πρότυπο** στο οποίο βασίζεται το υπόδειγμα νόμου του Οργανισμού Ηνωμένων Εθνών για τις υπηρεσίες εμπιστοσύνης στο ηλεκτρονικό εμπόριο (2021)[30] και τις σε εξέλιξη ηλεκτρονικές εμπορικές διαπραγματεύσεις στο πλαίσιο του Παγκόσμιου Οργανισμού Εμπορίου (Π.Ο.Ε.)[31].

---

[27] Οδηγία (ΕΕ) 2015/849 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2015, σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, και την κατάργηση της οδηγίας 2005/60/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και της οδηγίας 2006/70/ΕΚ της Επιτροπής.
Διαθέσιμο σε:
https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32015L0849&from=DA

[28] Οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2015, σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 2002/65/ΕΚ, 2009/110/ΕΚ και 2013/36/ΕΕ και του κανονισμού (ΕΕ) αριθ. 1093/2010 και την κατάργηση της οδηγίας 2007/64/ΕΚ.
Διαθέσιμο σε: https://eur-lex.europa.eu/legal-content/EL/LSU/?uri=celex:32015L2366

[29] Η αρχή «μόνον άπαξ» θα παράσχει τη δυνατότητα, από το 2023, στις δημόσιες διοικήσεις να επαναχρησιμοποιούν και να ανταλλάσσουν με διαφανή και ασφαλή τρόπο δεδομένα και έγγραφα που έχουν ήδη υποβληθεί από πολίτες. [Άρθρο 14 του κανονισμού (ΕΕ) αριθ. 2018/1724 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 2ας Οκτωβρίου 2018, για τη δημιουργία ενιαίας ψηφιακής θύρας με σκοπό την παροχή πρόσβασης σε πληροφορίες, σε διαδικασίες και σε υπηρεσίες υποστήριξης και επίλυσης προβλημάτων. ΕΕ L 295 της 21.11.2018].

[30] https://undocs.org/en/A/CN.9/WG.IV/WP.167

[31] 10 Βλ. π.χ. έγγραφα συνεδριάσεων της ομάδας εργασίας IV της UNCITRAL/Ηλεκτρονικό εμπόριο, συνεδρίαση 6-9 Απριλίου 2021:
https://uncitral.un.org/en/working_groups/4/electronic_commerce

Ωστόσο, όπως αναφέρθηκε ανωτέρω, από το 2014, έχουν επέλθει αρκετές αλλαγές, ενώ δεν μπορεί να συνεχιστεί η διατήρηση του θεσμικού αυτού πλαισίου, το οποίο βασίζεται σε εθνικά συστήματα ηλεκτρονικής ταυτοποίησης με διαφορετικά πρότυπα που αφορούν μάλιστα περιορισμένο πεδίο δραστηριοτήτων και ικανοποίησης αναγκών των πολιτών και των επιχειρήσεων της Ε.Ε.. Ο εκσυχγρονισμός του πλαισίου αυτού κρίνεται ακόμα πιο απαραίτητος αν λάβουμε υπόψη την ραγδαία ψηφιοποίηση του ιδιωτικού και δημόσιου τομέα, λόγω και της πανδημίας του κορωνοϊού COVID-19 που επιτάχυνε τις σχετικές διαδικασίες ψηφιοποίησης.

Κύρια ζητούμενα των πολιτών είναι η παροχή όρων υψηλής ασφάλειας και ευκολίας για τις επιγραμμικές τους δραστηριότητες, ώστε να **αυξάνεται η ζήτηση για μέσα ταυτοποίησης και επαλήθευσης της ταυτότητας διαδικτυακά, για ψηφιακή ανταλλαγή πληροφοριών ως προς την ταυτότητα των προσώπων καθώς και για υψηλό επίπεδο προστασίας των** προσωπικών δεδομένων.

Αυτό είχε ως συνέπεια τη στροφή σε νέες προηγμένες λύσεις που μπορούν να ενσωματώσουν επαληθεύσιμα δεδομένα και πιστοποιητικά του χρήστη. Επομένως, δεν αρκούν τα μέσα ηλεκτρονικής ταυτοποίησης και οι υπηρεσίες εμπιστοσύνης, όπως ρυθμίζονται στην παρούσα φάση από τον Κανονισμό eIDAS, λόγω των περιορισμών που αναφέρθηκαν ανωτέρω. Εξάλλου, και τα μέσα ταυτοποίησης ή επαλήθευσης ταυτότητας που αναπτύχθηκαν από τον ιδιωτικό τομέα εκτός πλαισίου του eIDAS, όπως μέσω Facebook ή Google, δηλαδή μέσω φιλικών προς τον χρήστη μέσων, δεν ανταποκρίνονται και πάλι ικανοποιητικά στα νέα δεδομένα και τις προκλήσεις της εποχής, αφού δεν παρέχουν ικανοποιητικό και υψηλό επίπεδο ασφαλείας και προστασίας των προσωπικών δεδομένων,και μπορούν να χαρακτηριστούν, ως μη συνδεόμενα σε αξιόπιστα και ασφαλή δημόσια ηλεκτρονική ταυτοποίηση.

Έτσι, ήδη από τον Φεβρουάριο του 2020[32], η Ευρωπαική Επιτροπή, διαμόρφωσε στρατηγική για το ψηφιακό μέλλον της Ευρώπης, με δέσμευση αναθεώρησης του Κανονισμού eIDAS, αποβλέποντας στη βελτίωση της αποτελεσματικότητάς του, την επέκταση εφαρμογής του στον ιδιωτικό τομέα και την προώθηση αξιόπιστων ψηφιακών ταυτοτήτων για τους πολίτες και τις επιχειρήσεις της Ε.Ε..

Εξάλλου, η αναθεώρηση του Κανονισμού eIDAS επιταχύνθηκε και από τις **έκτακτες ανάγκες που επέφερε η πανδημία του κορωνοϊού,** επιβάλλοντας άμεσες ψηφιακές υπηρεσίες και λύσεις σε σειρά ζητημάτων, όπως τις διακοπές στις μη επιγραμμικές δημόσιες και ιδιωτικές υπηρεσίες καθώς και την ανάγκη για πρόσβαση σε δημόσιες και ιδιωτικές υπηρεσίες διαδικτυακά.

Κατά συνέπεια, προκύπτει ότι, ναι μεν ο **Κανονισμός eIDAS** έχει συμβάλει, με αξιόλογο τρόπο, στη διαμόρφωση μίας ενιαίας ψηφιακής αγοράς υπηρεσιών ταυτότητας και εμπιστοσύνης στην Ε.Ε., τονίζοντας την ανάγκη για ασφαλείς ψηφιακές συναλλαγές, αλλά **χρήζει βελτίωσης ως προς την αποτελεσματικότητα, την αποδοτικότητα, τη συνοχή και τη**

[32] Ευρωπαϊκή Επιτροπή. (2020). Στρατηγική για τη διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης. Διαθέσιμο σε: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_el

συνάφειά του, για την κάλυψη των σύγχρονων και αυξημένων ψηφιακών αναγκών της αγοράς.

Πλέον, απαιτείται ένα υψηλό επίπεδο ηλεκτρονικής ταυτοποίησης και εμπιστοσύνης στις παρεχόμενες υπηρεσίες στο πλαίσιο της Ε.Ε., τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα, με ιδιαίτερη έμφαση στην προστασία των δεδομένων προσωπικού χαρακτήρα.

2. Η ευρωπαική ψηφιακή ταυτότητα

Η Ευρωπαϊκή Επιτροπή πρότεινε ένα πλαίσιο για την ευρωπαϊκή ψηφιακή ταυτότητα[33], η οποία θα είναι διαθέσιμη σε όλους τους πολίτες, τους κατοίκους και τις επιχειρήσεις της Ε.Ε.. Με τον τρόπο αυτό, οι πολίτες θα μπορούν να αποδείξουν την ταυτότητά τους και να κοινοποιήσουν ηλεκτρονικά έγγραφα από τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητάς τους με ένα απλό κλικ στο τηλέφωνό τους. Επίσης, θα μπορούν να έχουν **πρόσβαση σε διαδικτυακές υπηρεσίες με την εθνική τους ψηφιακή ταυτοποίηση, η οποία θα αναγνωρίζεται σε όλη την Ευρώπη**. Οι πολύ μεγάλες πλατφόρμες θα υποχρεούνται να δέχονται τη χρήση των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας, κατόπιν αιτήματος του χρήστη, για παράδειγμα για την απόδειξη της ηλικίας του. Η χρήση του ευρωπαϊκού πορτοφολιού ψηφιακής ταυτότητας θα γίνεται πάντα με επιλογή του χρήστη.

Η κ. **Μαργκρέιτε Βέστεϊγιερ**, εκτελεστική αντιπρόεδρος για μια Ευρώπη Έτοιμη για την Ψηφιακή Εποχή, δήλωσε τα εξής: «Η ευρωπαϊκή ψηφιακή ταυτότητα **θα μας δώσει τη δυνατότητα να κάνουμε τις ίδιες ενέργειες σε οποιοδήποτε κράτος μέλος με αυτές που κάνουμε στη χώρα μας, χωρίς επιπλέον κόστος και με λιγότερα εμπόδια, είτε πρόκειται για την ενοικίαση διαμερίσματος είτε για το άνοιγμα τραπεζικού λογαριασμού εκτός της χώρας μας. Και να το πράττουμε αυτό με ασφαλή και διαφανή τρόπο. Έτσι, θα αποφασίζουμε πόσες πληροφορίες που μας αφορούν επιθυμούμε να μοιραστούμε, με ποιον και για ποιο σκοπό**. Πρόκειται για μια μοναδική ευκαιρία που θα επιτρέψει σε όλους μας να βιώσουμε ακόμα περισσότερο τι σημαίνει να ζούμε στην Ευρώπη και να είμαστε Ευρωπαίοι.». Στο ίδιο πνεύμα, ο Επίτροπος Εσωτερικής Αγοράς, κ. Τιερί Μπρετόν δήλωσε: «Οι πολίτες της Ε.Ε., πέρα από το **υψηλό επίπεδο ασφάλειας, αναμένουν επίσης και ευκολία, είτε κατά τις επαφές τους με τις εθνικές διοικήσεις**, για παράδειγμα, για να υποβάλουν τη φορολογική τους δήλωση, είτε όταν γράφονται σε ένα ευρωπαϊκό πανεπιστήμιο όπου απαιτείται επίσημη ταυτοποίηση. **Τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας τούς προσφέρουν τη νέα δυνατότητα να αποθηκεύουν και να χρησιμοποιούν δεδομένα για κάθε είδους υπηρεσία**, από τον έλεγχο εισιτηρίων στο αεροδρόμιο έως την ενοικίαση αυτοκινήτου. Σκοπός τους είναι να δώσουν μια επιλογή στους καταναλωτές, μια ευρωπαϊκή επιλογή. Οι ευρωπαϊκές εταιρείες μας, μεγάλες και

[33] https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
Η Επιτροπή προτείνει την έκδοση αξιόπιστης και ασφαλούς ψηφιακής ταυτότητας για όλους τους Ευρωπαίους. https://ec.europa.eu/commission/presscorner/detail/el/ip_21_2663

μικρές, θα επωφεληθούν κι αυτές από την ψηφιακή ταυτότητα. **Θα μπορούν να προσφέρουν ευρύ φάσμα νέων υπηρεσιών, δεδομένου ότι η πρόταση δίνει τη λύση για ασφαλείς και αξιόπιστες υπηρεσίες ταυτοποίησης.**».

Ειδικότερα, το πλαίσιο του νέου Κανονισμού, τα κράτη-μέλη της Ε.Ε. θα έχουν τη δυνατότητα να προσφέρουν στους πολίτες και τις επιχειρήσεις τους **ψηφιακά πορτοφόλια**, **στα οποία θα είναι εφικτή η διασύνδεση με την εθνική τους ψηφιακή ταυτότητα**, με αποδεικτικά έγγραφα άλλων προσωπικών τους ιδιοχαρακτηριστικών (λ.χ. άδεια οδήγησης, πτυχία, τραπεζικός λογαριασμός, κ.ο.κ.).

Μάλιστα, **τα ευρωπαϊκά ψηφιακά πορτοφόλια θα μπορεί να παρέχονται είτε από δημόσιες αρχές των κρατών-μελών είτε από ιδιωτικούς φορείς, υπό τον όρο ότι αναγνωρίζονται από τα κράτη-μέλη**.

Έτσι, μέσω των ευρωπαϊκών ψηφιακών πορτοφολιών, θα δίνεται η δυνατότητα στους πολίτες να έχουν πρόσβαση ψηφιακά σε υπηρεσίες, χωρίς τη χρήση ιδιωτικών μεθόδων ταυτοποίησης και χωρίς να κοινοποιούν προσωπικά δεδομένα τους χωρίς λόγο. Αντίθετα, οι πολίτες θα έχουν πλήρη έλεγχο των δεδομένων που διαμοιράζονται κάθε φορά για την ψηφιακή τους συναλλαγή.

Ορισμένα βασικά χαρακτηριστικά της ευρωπαϊκής ψηφιακής ταυτότητας θα είναι τα ακόλουθα:

- Η ευρωπαική ψηφιακή ταυτότητα θα είναι **διαθέσιμη σε όποιον πολίτη**, **κάτοικο της Ε.Ε. ή επιχείρηση επιθυμεί να την χρησιμοποιεί**.
- Τα ευρωπαϊκά ψηφιακά πορτοφόλια θα μπορεί να χρησιμοποιούνται με διακριτούς τρόπους, ήτοι **είτε ως τρόπος ταυτοποίησης των χρηστών είτε ως μέσο απόδειξης συγκεκριμένων προσωπικών χαρακτηριστικών**, με σκοπό την πρόσβαση σε δημόσιες και ιδιωτικές ψηφιακές υπηρεσίες στην Ε.Ε.
- Ο χρήστης θα έχει τον **πλήρη έλεγχο των δεδομένων του ως προς τα στοιχεία** (πτυχές της ταυτότητάς τους, δεδομένα, πιστοποιητικά) κοινοποιούνται σε τρίτα μέρη καθώς και να παρακολουθούν τις σχετικές αυτές κοινοποιήσεις. Επίσης, στο πλαίσιο της αρχής της αναγκαιότητας, θα διασφαλίζεται ότι θα κοινοποιούνται μόνο πληροφορίες και στοιχεία που είναι απαραίτητο να κοινοποιηθούν.

Στόχος της Ευρωπαϊκής Επιτροπής είναι **η άμεση εφαρμογή της ευρωπαϊκής ψηφιακής ταυτότητας, με αποτέλεσμα να έχει εκδοθεί σύσταση**, η οποία καλεί τα κράτη-μέλη να καθορίσουν κοινή εργαλειοθήκη έως τον Σεπτέμβριο του 2022, για την έναρξη των προπαρασκευαστικών εργασιών. Στην εργαλειοθήκη θα συμπεριλαμβάνεται η τεχνική αρχιτεκτονική, τα πρότυπα και οι κατευθυντήριες γραμμές με βέλτιστες πρακτικές για την υιοθέτηση της ευρωπαϊκής ψηφιακής ταυτότητας.

Εκτός των θεσμικών ενεργειών, **η Επιτροπή αποβλέπει στην έναρξη συνεργασίας με τα κράτη-μέλη και τον ιδιωτικό τομέα αναφορικά με τις τεχνικές πτυχές της ευρωπαϊκής ψηφιακής ταυτότητας, ενώ, μέσω του Προγράμματος «Ψηφιακή Ευρώπη», θα προωθήσει την εφαρμογή του ευρωπαϊκού πλαισίου για την ψηφιακή ταυτότητα.**

Περαιτέρω, η **«Ψηφιακή Πυξίδα» της Ευρωπαϊκής Επιτροπής για το 2030 ορίζει στόχους και ορόσημα στην επίτευξη των οποίων θα συντελέσει η ευρωπαϊκή ψηφιακή ταυτότητα.** Επί παραδείγματι, έως το 2030, όλες οι βασικές δημόσιες υπηρεσίες πρέπει να είναι διαθέσιμες διαδικτυακά, όλοι οι πολίτες να έχουν πρόσβαση σε ηλεκτρονικά ιατρικά αρχεία και το 80% των πολιτών πρέπει να χρησιμοποιεί μια λύση ηλεκτρονικής ταυτοποίησης (eID).

Ασφαλώς, η Επιτροπή στηρίζεται στο ισχύον διασυνοριακό θεσμικό πλαίσιο για τις **αξιόπιστες ψηφιακές ταυτότητες, την ευρωπαική πρωτοβουλία για την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης** (Κανονισμός eIDAS, 2014), που παρέχει τη νομική βάση για τη διασυνοριακή ηλεκτρονική ταυτοποίηση, την επαλήθευση της ταυτότητας προσώπων και την πιστοποίηση ιστοτόπων εντός της Ε.Ε.. Μάλιστα, ήδη υπολογίζεται ότι το 60% των ευρωπαίων πολιτών μπορεί να επωφεληθεί από τον Κανονισμό eIDAS.

3. Η πρόταση της Ευρωπαϊκής Επιτροπής για μία ευρωπαϊκή ψηφιακή ταυτότητα (2021)

Από την πλευρά της η Ευρωπαϊκή Επιτροπή από το 2021 έχει προτείνει μία **ευρωπαϊκή ψηφιακή ταυτότητα, στην οποία θα έχουν πρόσβαση όλοι οι πολίτες, οι κάτοικοι και οι επιχειρήσεις της Ευρωπαϊκής Ένωσης**, και μάλιστα μία αξιόπιστη και ασφαλή ψηφιακή ταυτότητα για όλους τους Ευρωπαίους πολίτες[34]. Με τον τρόπο αυτό, **οι πολίτες θα είναι εφικτό να αποδεικνύουν την ταυτότητά τους και να μοιράζονται ηλεκτρονικά έγγραφα από το ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητάς τους**, κάνοντας κλικ σε ένα κουμπί στο smartphone τους. Παράλληλα, θα είναι δυνατό να **έχουν πρόσβαση σε διαδικτυακές υπηρεσίες, χρησιμοποιώντας την εθνική ψηφιακή τους ταυτότητα, η οποία θα αναγνωρίζεται σε όλη την Ευρώπη**. Μάλιστα, οι πολύ μεγάλες πλατφόρμες, όπως για αγορές, ανάγνωση του Τύπου, κ.λπ., θα πρέπει να αποδέχονται τη χρήση ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας, κατόπιν αιτήματος του χρήστη, για παράδειγμα, για να τους επιτρέψουν να αποδείξουν την ηλικία τους. Σε κάθε περίπτωση, **η χρήση του χαρτοφυλακίου ευρωπαϊκής ψηφιακής ταυτότητας θα επαφίεται πάντοτε στη διακριτική ευχέρεια του χρήστη**.

Η Ευρωπαϊκή Επιτροπή αναγνωρίζει ότι η ταυτοποίηση των πολιτών επιτρέπει να αποδεικνύουμε ποιοι είμαστε, όπως γίνεται σήμερα στο φυσικό κόσμο με τα διαβατήρια και τις ταυτότητες στην καθημερινότητά μας. Ωστόσο, **η ψηφιακή ταυτοποίηση αναγνωρίζεται από την Ε.Ε. ότι αφενός απλοποιεί τις αλληλεπιδράσεις μας στο νέο ψηφιακό περιβάλλον αφετέρου εξοικονομεί χρόνο**.

[34] La Commission propose une identité numérique fiable et sécurisée pour tous les Européens, Bruxelles, le 3 juin 2021.
Διαθέσιμο σε: https://digital-strategy.ec.europa.eu/fr/news/commission-proposes-trusted-and-secure-digital-identity-all-europeans

Βασική έννοια είναι αυτή της ψηφιακής ταυτότητας (Digital ID), η **οποία επιτρέπει σε διάφορους ιδιωτικούς παρόχους και δημόσιους φορείς να προσφέρουν μέσα ψηφιακής ταυτοποίησης που επιτρέπουν στους χρήστες να έχουν πρόσβαση σε διάφορες διαδικτυακές δημόσιες υπηρεσίες** ή άλλες ιδιωτικές διαδικτυακές συναλλαγές, όπως οι τραπεζικές.

Το **πρόβλημα** εκκινεί από το γεγονός ότι **οι υφιστάμενες ψηφιακές ταυτότητες παρέχουν διαφοροποιημένο βαθμό αξιοπιστίας και ασφάλειας, ενώ ακόμα και μεγάλες πλατφόρμες δεν επιτρέπουν στους χρήστες τους, να έχουν πλήρη έλεγχο των δεδομένων τους που διακινούνται στο ηλεκτρονικό περιβάλλον**, όταν λ.χ. συνδέονται για να κάνουν χρήση μίας διαδικτυακής υπηρεσίας.

Έτερη έννοια που εισάγεται από την Ευρωπαϊκή Επιτροπή είναι αυτή του Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας. Η έννοια αυτή συναρτάται με το γεγονός ότι αρκετοί ευρωπαίοι πολίτες κάνουν ήδη χρήση ψηφιακών πορτοφολιών (Wallets) στα smartphone τους, για την αποθήκευση καρτών επιβίβασης όταν ταξιδεύουν ή εικονικών τραπεζικών καρτών για σκοπούς πληρωμής. Σύμφωνα με τους νέους κανόνες που εισηγείται η Ευρωπαϊκή Επιτροπή, τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας θα είναι προσβάσιμα σε όλους. Άλλωστε, αποτελούν προσωπικές ψηφιακές συσκευές που επιτρέπουν στους πολίτες να αναγνωρίζουν ψηφιακά, να αποθηκεύουν και να διαχειρίζονται τα στοιχεία της ταυτότητάς τους ή άλλα επίσημα έγγραφά τους σε ηλεκτρονική μορφή (λ.χ. πιστοποιητικό εμβολιασμού κατά του κορωνοϊού COVID-19). Επομένως, οι δυνατότητες που παρέχουν τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας επιτρέπουν τη συμπερίληψη και άλλων επίσημων πληροφοριών των πολιτών, όπως η άδεια οδήγησης, ιατρικές συνταγές, απολυτήρια σχολείου, πτυχία πανεπιστημιακών φορέων, κ.ά.

Σκοπός της Ε.Ε. είναι, μέσω του πορτοφολιού ψηφιακής ταυτότητας, **οι πολίτες να είναι εφικτό να αποδεικνύουν την ταυτότητά τους**, εφόσον τούτο είναι απαραίτητο **για την πρόσβασή τους σε διαδικτυακές υπηρεσίες, να κοινοποιούν ψηφιακά έγγραφα** ή **απλώς να αποδεικνύουν** ένα συγκεκριμένο προσωπικό τους χαρακτηριστικό, όπως η ηλικία, χωρίς να αποκαλύπτουν συγχρόνως και την ταυτότητά τους ή άλλα προσωπικά δεδομένα. Παράλληλα, στόχος της θεσμικής αυτής πρωτοβουλίας είναι οι πολίτες **να διαθέτουν ανά πάσα στιγμή πλήρη έλεγχο των δεδομένων που μοιράζονται κατά τις συναλλαγές τους με τρίτα πρόσωπα ή φορείς.**

Η θεσμική παρέμβαση της Ευρωπαϊκής Επιτροπής επιτρέπει στους πολίτες, με τους νέους κανόνες που εισάγονται, να έχουν όλοι τη δυνατότητα να διαθέτουν ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας κοινά αποδεκτό από το σύνολο των κρατών-μελών της Ε.Ε., χωρίς ωστόσο να υποχρεούνται στην απόκτηση του είδους αυτού ψηφιακής ταυτότητας.

Τίθεται, επίσης, το ζήτημα εάν οι δημόσιες και ορισμένες ιδιωτικές υπηρεσίες, θα υποχρεωθούν να αποδέχονται την ψηφιακή ταυτότητα της Ε.Ε. Σε κάθε περίπτωση, καθίσταται αντιληπτό ότι τυχόν ευρεία αξιοποίηση του ευρωπαϊκού πορτοφολιού ψηφιακής ταυτότητας θα διαμορφώσει τους όρους για βελτιωμένες επιχειρηματικές ευκαιρίες, αφού διασφαλίζεται μεγαλύτερος βαθμός ασφάλειας και ισχυρός έλεγχος ταυτότητας των προσώπων.

Η προστιθέμενη αξία του νέου Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας συνίσταται στο γεγονός ότι παρέχει δυνατότητα πρόσβασης τόσο σε δημόσιες όσο και σε ιδιωτικές διαδικτυακές υπηρεσίες στο πλαίσιο της Ε.Ε., ιδίως όταν απαιτείται ισχυρός έλεγχος ταυτοποίησης του χρήστη (λ.χ. πρόσβαση σε τραπεζικό λογαριασμό, υποβολή αίτησης χορήγησης δανείου, υποβολή δήλωσης φορολογίας, εγγραφή σε πανεπιστήμιο στην Ελλάδα ή το εξωτερικό, κ.λπ.).

Επομένως, μπορεί να αξιοποιηθεί πρακτικά, ως **ψηφιακό πορτοφόλι ταυτότητας στο κινητό του πολίτη**, επιτρέποντας:

α) να αποθηκεύει και να έχει πρόσβαση στα προσωπικά του δεδομένα, ως μέσο αποθήκευσης της άδειας οδήγησης, του διπλώματος οδήγησης, των τραπεζικών καρτών αντί φυσικής κάρτας στο φυσικό του πορτοφόλι.

β) να συνιστά αποδεικτικό στοιχείο της ηλικίας του χρήστη, όπου αυτό είναι απαραίτητο, λ.χ. για την είσοδο σε νυχτερινό κέντρο διασκέδασης κατά τον έλεγχο από την ασφάλεια αυτού, χωρίς την αποκάλυψη λοιπών προσωπικών δεδομένων. Εξασφαλίζοντας έτσι την αρχή της ελαχιστοποίησης των δεδομένων προσωπικού χαρακτήρα.

γ) για την ενοικίαση αυτοκινήτου σε ένα αεροδρόμιο, χωρίς αναμονή και χωρίς έλεγχο της ταυτότητας/ διαβατηρίου, της άδειας οδήγησης και της πιστωτικής κάρτας του πολίτη, πριν την έλευση του ατόμου στο αεροδρόμιο και τη σύναψη της σύμβασης ενοικίασης.

δ) για την απόδειξη της ταυτότητας του προσώπου, ώστε να μπορεί να αξιοποιήσει μία διαδικτυακή υπηρεσία, λ.χ. για την αγορά μίας κάρτας SIM, την εγγραφή στους αρμόδιους φορείς ενός εργαζόμενου στη χώρα υποδοχής του, κ.ο.κ.

Επομένως, η χρήση των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας παράγουν προστιθέμενη αξία για την Ε.Ε. συγκριτικά με το ισχύον σύστημα, δεδομένου ότι θα δημιουργηθούν αξιόπιστες υπηρεσίες που θα παρέχονται από τα κράτη-μέλη, βελτιώνοντας την **αποτελεσματικότητα**, παράγοντας οφέλη για τις ιδιωτικές επιχειρήσεις και διασφαλίζοντας την προστασία των προσωπικών δεδομένων και **την απρόσκοπτη διενέργεια συναλλαγών** με δωρεάν, εύχρηστο και ασφαλή τρόπο για τους πολίτες των κρατών-μελών.

Μέχρι πρόσφατα υφίστανται 19 κοινοποιημένα συστήματα ηλεκτρονικής αναγνώρισης που χρησιμοποιούνται από 14 κράτη-μέλη, καλύπτοντας περίπου το 60% του πληθυσμού της Ε.Ε. (27 κράτη-μέλη)[35]. Εξάλλου, σε κάποια κράτη-μέλη γίνεται περιορισμένη χρήση των συστημάτων αυτών, σε άλλα η χρήση τους είναι υποχρεωτική και, σε κάθε περίπτωση, αποτυπώνεται περιορισμένη εμπορική χρήση.

Εκτιμάται δε ότι η πανδημία του κορωνοϊού και η διαρκώς αυξανόμενη τάση χρήσης των ψηφιακών υπηρεσιών θα συμβάλουν στην πιο ευχερή μετάβαση στο νέο θεσμικό πλαίσιο. Εξάλλου, **η θέσπιση του ευρωπαϊκού πορτοφολιού ευρωπαϊκής ταυτότητας δεν αναιρεί την τυχόν υπάρχουσα ηλεκτρονική ταυτοποίηση**, αφού τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας **θα βασιστούν στα εθνικά συστήματα ψηφιακής ταυτότητας**.Τα

[35] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview

κράτη-μέλη επομένως, θα πρέπει να προσφέρουν τη δυνατότητα στους πολίτες και τους κατοίκους τους να αποκτήσουν ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας σε εθνικό επίπεδο.

Επισημαίνεται δε ότι η ασφάλεια, **το απόρρητο και η προστασία των δεδομένων προσωπικού χαρακτήρα** θα είναι διασφαλισμένα, αφού η πρόταση της Ευρωπαϊκής Επιτροπής αποβλέπει στην επίτευξη υψηλού επιπέδου ασφαλείας, ενώ θα προτείνει, σε συνεργασία και συμφωνία με τα επιμέρους κράτη-μέλη, τα πρότυπα, τις τεχνικές προδιαγραφές και τις επιχειρησιακές πτυχές, πιστοποιώντας τα αντίστοιχα χαρτοφυλάκιά τους και διασφαλίζοντας τη διαλειτουργικότητα των εθνικών συστημάτων ψηφιακής ταυτότητας, μέσω σχετικής εκτελεστικής πράξης της Ε.Ε.. Μάλιστα, επισημαίνεται ότι η διαδικτυακή κοινή χρήση προσωπικών δεδομένων θα επιτρέπεται, μόνο εφόσον ο πολίτης το επιθυμεί.

Υπογραμμίζεται ότι η πρόταση της Ευρωπαϊκής Επιτροπής για μία ενιαία ευρωπαϊκή ψηφιακή ταυτότητα δεν έχει σκοπό την αντικατάσταση των εθνικών ψηφιακών ταυτοτήτων, αλλά θα εξακολουθούν να παρέχονται ψηφιακές ταυτότητες από τα κράτη-μέλη. Η προστιθέμενη αξία με τη θεσμική παρέμβαση της Ευρωπαϊκής Επιτροπής έγκειται στην επέκταση της λειτουργικότητας και της χρηστικότητας των εθνικών ηλεκτρονικών ταυτοτήτων, δημιουργώντας ένα προσωπικό ψηφιακό πορτοφόλι. Μάλιστα, **τα κράτη-μέλη θα μπορεί να δημιουργήσουν προσωπικό ψηφιακό πορτοφόλι για τους πολίτες και τους κατοίκους του, ένα έτος μετά την έναρξη ισχύος του νέου Κανονισμού**. Προς την κατεύθυνση αυτή, εκ μέρους της Ευρωπαϊκής Επιτροπής προτείνεται και κοινή εργαλειοθήκη μαζί με το πλαίσιο για το ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας, ώστε να επιταχυνθεί η διαδικασία διαμόρφωσης εύχρηστων και φιλικών προς τον χρήστη ψηφιακών υπηρεσιών σε όλη την Ε.Ε. με ομοιόμορφο τρόπο, σε στενή συνεργασία με τον ιδιωτικό τομέα.

Έτσι, το χρονοδιάγραμμα για την ανάπτυξη, υιοθέτηση και εφαρμογή της κοινής εργαλειοθήκης προβλέπει, να έχει ολοκληρωθεί η συμφωνία των κρατών-μελών με την Ευρωπαϊκή Επιτροπή έως τον Σεπτέμβριο 2022, και τη δημοσίευσή του τον Οκτώβριο του 2022.

III. Ελληνική Πραγματικότητα

1. Γενικό Μέρος

Οι τεχνολογίες Πληροφορικής και Επικοινωνιών έχουν συμβάλλει στην βελτίωση της σχέσης κράτους-πολίτη, μέσω της ανάπτυξης της ηλεκτρονικής διακυβέρνησης, με στόχο την παροχή υπηρεσιών, με στοιχεία όπως η διαφάνεια, η συμμετοχή των πολιτών στις δημοκρατικές διαδικασίες και στον έλεγχο του κυβερνητικού έργου. Για το σκοπό αυτό, συστάθηκε το Υπουργείο Ψηφιακής Διακυβέρνησης με το **π.δ 40/2020, ενώ το Σεπτέμβριο του 2020 ψηφίστηκε ο νόμος 4727, «Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) -**

Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις».

1.1. Ηλεκτρονική ταυτοποίηση

Η διαδικασία της ταυτοποίησης με ψηφιακά μέσα, διευκολύνει τις ηλεκτρονικές συναλλαγές με το Δημόσιο, ενώ η ανάπτυξη συστημάτων ηλεκτρονικής ταυτοποίησης υπόσχεται πολλά οφέλη για τον πολίτη και τις επιχειρήσεις, καθώς δίνεται η δυνατότητα στον πολίτη να χρησιμοποιεί ολοένα και περισσότερες υπηρεσίες με περισσότερη ασφάλεια, σε σύγκριση με το υπάρχον σύστημα ταυτοποίησης (κωδικοί taxisnet, χρήση για φορολογικούς σκοπούς). Παράδειγμα ηλεκτρονικής ταυτοποίησης είναι η χρήση ενός username και ενός κωδικού πρόσβασης. Η διαδικασία για την έκδοση των διαπιστευτηρίων περιγράφεται στο άρθρο 25 του ν. 4727/2021, ταυτοποίηση για την έκδοση διαπιστευτηρίων.

1. Για την έκδοση διαπιστευτηρίων της περ. α΄ της παρ. 1 του άρθρου 24, η **Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης** είναι αποκλειστικά υπεύθυνη για την ταυτοποίηση και την αυθεντικοποίηση των φυσικών ή νομικών προσώπων ή νομικών οντοτήτων για σκοπούς παροχής και χρήσης των ψηφιακών δημόσιων υπηρεσιών. Η ταυτοποίηση φυσικών προσώπων είναι απαραίτητη προϋπόθεση για την έκδοση διαπιστευτηρίων, με σκοπό την αυθεντικοποίησή τους.

2. Η ταυτοποίηση διενεργείται με έναν από τους ακόλουθους τρόπους:

α) Μέσω της Ανεξάρτητης Αρχής Δημοσίων Εσόδων, σύμφωνα με τα οριζόμενα στην υπ' αρ. 1178/2010 απόφαση του Υπουργού Οικονομικών «Εγγραφή νέων χρηστών στις ηλεκτρονικές υπηρεσίες TaxisNet» (Β΄ 1916).

β) Με φυσική παρουσία του φυσικού προσώπου στα Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ).

γ) Με τη χρήση εξ αποστάσεως ταυτοποίησης που παρέχει διασφάλιση ισοδύναμη με τη φυσική παρουσία. Η ταυτοποίηση αυτή μπορεί να διενεργείται μέσω του Εθνικού Μητρώου Επικοινωνίας Πολιτών του άρθρου 17 του ν. 4704/2020 (Α΄ 133).

1.2. Διαλειτουργικότητα

Η διαλειτουργικότητα των πληροφοριακών συστημάτων της ελληνικής δημόσιας δίοικησης ορίζεται στο άρθρο 84 του ν. 4727/2020, σύμφωνα με το οποίο:

1**. Η Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης (Γ.Γ.Π.Σ.Δ.Δ.) του Υπουργείου Ψηφιακής Διακυβέρνησης είναι υπεύθυνη για την ηλεκτρονική ταυτοποίηση και την επιβεβαίωση ταυτότητας (αυθεντικοποίηση) των**

φυσικών προσώπων σύμφωνα με τα άρθρα 24 και 25, με σκοπό την παροχή ψηφιακών δημόσιων υπηρεσιών. Αποτελεί τον μοναδικό αρμόδιο φορέα για την υλοποίηση διατομεακής διαλειτουργικότητας και διαλειτουργικότητας των επιμέρους μητρώων των φορέων του δημόσιου τομέα, σε συνεργασία με την Γενική Γραμματεία Ψηφιακής Διακυβέρνησης και Απλούστευσης Διαδικασιών, τον μοναδικό αρμόδιο φορέα για την ταυτοποίηση των φυσικών προσώπων μεταξύ των μητρώων των φορέων αυτών αξιοποιώντας τα επιμέρους αναγνωριστικά, που είναι αποκλειστικά υπεύθυνη για τη λειτουργία του Κέντρου Διαλειτουργικότητας (ΚΕΔ) και για την υλοποίηση όλων των σχετικών δράσεων σε συνεργασία με τους ως άνω φορείς.

2. Στο πλαίσιο της αυτεπάγγελτης αναζήτησης δικαιολογητικών, πιστοποιητικών ή εγγράφων των φυσικών ή νομικών προσώπων ή νομικών οντοτήτων για την άσκηση των αρμοδιοτήτων των φορέων του δημοσίου τομέα, **οι φορείς υποχρεούνται έως την 1η.7.2022 να διαθέτουν μέσω διαδικτυακής υπηρεσίας στο Κέντρο Διαλειτουργικότητας (ΚΕΔ) το σύνολο των δεδομένων που περιλαμβάνονται στα ανωτέρω δικαιολογητικά, πιστοποιητικά και έγγραφα.**

3. Η Γ.Γ.Π.Σ.Δ.Δ. είναι αρμόδια και το Εθνικό Δίκτυο Υποδομών Τεχνολογίας και Έρευνας (Ε.Δ.Υ.Τ.Ε. Α.Ε.) μεριμνά για τη συνδυαστική ανάλυση των διατομεακών δεδομένων, στο πλαίσιο της διαλειτουργικότητας, αξιοποιώντας τεχνικές ανάλυσης μεγάλου όγκου δεδομένων (data analytics).

2. Η Υπάρχουσα κατάσταση στην Ελλάδα

Σύμφωνα με τη διεθνή βιβλιογραφία[36] **οι υπηρεσίες ταυτοποίησης πολιτών (eID Services) είναι βασικές υπηρεσίες για την παροχή ολοκληρωμένων υπηρεσιών ηλεκτρονικής διακυβέρνησης**. Οι χώρες που βρίσκονται στην κορυφή στους δείκτες παρακολούθησης της ηλεκτρονικής διακυβέρνησης (DESI, UN) έχουν ολοκληρωμένα και λειτουργικά συστήματα ηλεκτρονικής ταυτοποίησης πολιτών εδώ και πολλά χρόνια.

Παρά την διαπιστωμένη ανάγκη για την ύπαρξη ενός συστήματος παροχής υπηρεσιών ηλεκτρονικής ταυτοποίησης, στην Ελλάδα δεν υπήρξε μια σύγχρονη και ασφαλής υποδομή που θα επέτρεπε την παροχή σύγχρονων και ασφαλών υπηρεσιών ηλεκτρονικής ταυτοποίησης.

Τι γίνεται μέχρι σήμερα στην Ελλάδα;

[36] https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/EGovernment%20Survey%202018_FINAL%20for%20web.pdf
https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-akey-to-inclusive-growth
https://www.undp.org/content/undp/en/home/blog/2017/6/1/Moving-towards-digital-technologyfor-legal-identity.html
https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-idcan-unlock-opportunities-for-the-worlds-most-vulnerable

Υπάρχουν **4 βασικά αναγνωριστικά** στους βασικούς τομείς διακυβέρνησης:

- ΑΦΜ (Φορολογία)
- ΑΜΚΑ (Κοινωνική Ασφάλιση)
- Αριθμός Πολίτη (Δημοτολόγιο – Ληξιαρχείο)
- Αριθμός Δελτίου Ταυτότητας (Αστυνομία)
- Πολλαπλά "legacy" IDs στα διάφορα επί μέρους Μητρώα

Ένα από τα βασικά προβλήματα για την παροχή υπηρεσιών ταυτοποίησης προς τους πολίτες είναι **η έλλειψη ενός προσωπικού αριθμού ταυτοποίησης των φυσικών προσώπων.** Στην χώρα μας το μοντέλο που κυριαρχεί σε ότι αφορά την αυθεντικοποίηση είναι εκείνο της αποκεντροποιημένης ταυτοποίησης. Δηλαδή, ένα φυσικό πρόσωπο συνάπτει σχέσεις εμπιστοσύνης απευθείας με τον πάροχο υπηρεσιών και ταυτοποιείται απευθείας σε αυτόν (π.χ. Φορολογική Διοίκηση και ΑΦΜ, Υπηρεσίες Κοινωνικής Ασφάλισης και ΑΜΚΑ, Υπηρεσίες Ασφάλειας και ΑΔΤ, κ.ο.κ). Το αποτέλεσμα είναι η δημιουργία πολλών και ανεπαρκώς συνδεδεμένων μητρώων, στα οποία πολλές φορές τηρούνται στοιχεία για τις ίδιες οντότητες, ενώ σε αρκετές περιπτώσεις τα στοιχεία αυτά δεν συμπίπτουν είτε λόγω μη επικαιροποίησης τους είτε λόγω μη σωστής διαδικασίας αρχικής εισαγωγής τους.

Η σημερινή κατάσταση, όπως περιγράφεται, έχει ως συνέπειες, μεταξύ άλλων, **ένα φυσικό πρόσωπο να «εμφανίζεται με πολλά πρόσωπα» έναντι του Δημοσίου και το Δημόσιο να «εμφανίζεται με πολλά πρόσωπα» έναντι του φυσικού προσώπου.** Με τη χρήση του Προσωπικού Αριθμού απλουστεύεται η ζωή του πολίτη, ο οποίος δεν θα έχει πλέον την υποχρέωση απομνημόνευσης πολλών αριθμών ταυτοποίησης και διατήρησης αντίστοιχων πιστοποιητικών. Επιπλέον, **περιορίζεται σημαντικά η ύπαρξη διπλοεγγραφών στα διάφορα μητρώα του Δημοσίου.** Απώτερος στόχος είναι η **πλήρης εξάλειψη των διπλοεγγραφών και η διόρθωση σφαλμάτων στις εγγραφές** (αναγραμματισμοί, ορθογραφικά λάθη σε ονοματεπώνυμα), που πλήττουν το κύρος της ακρίβειας των δεδομένων των φυσικών προσώπων.

Χαρακτηριστικό παράδειγμα για τα πλεονεκτήματα του Προσωπικού Αριθμού είναι το ακόλουθο: Στην παρούσα κατάσταση χρησιμοποιούνται οι **κωδικοί taxisnet** για τη σύνδεση στις ηλεκτρονικές υπηρεσίες ΕΦΚΑ. Το αποτέλεσμα είναι ο ήδη υφιστάμενος αυτόματος συσχετισμός **ΑΦΜ** και **ΑΜΚΑ** στον Φορέα να διαιωνίζει τις εσφαλμένες εγγραφές (ορθογραφικά, διπλοεγγραφές λάθος πατρώνυμο ή μητρώνυμο) στα επιμέρους μητρώα, για το ίδιο πρόσωπο. Αυτό συμβαίνει διότι διασυνδέονται διαφορετικοί αριθμοί, για να επιτευχθεί η επαλήθευση της ταυτότητας του φυσικού προσώπου. Με την χρήση του Προσωπικού Αριθμού αυτό δεν θα είναι, πλέον, απαραίτητο, αφού αυτήν την υπηρεσία θα παρέχει με ασφαλή - μη φανερό - τρόπο το **Μητρώο Προσωπικού Αριθμού**. Ακόμη, λοιπόν, και αν τα στοιχεία του φυσικού προσώπου στο σώμα ενός εγγράφου είναι εσφαλμένα σε σχέση με τα στοιχεία στο σώμα άλλου εγγράφου (πχ ορθογραφικό λάθος σε επώνυμο), η αναφορά θα γίνεται σε σχέση με τα δεδομένα της ΓΓΠΣΔΔ. Υπ' αυτή την έννοια, κάθε νέο έργο του δημοσίου, θα μπορεί να πληροί τις αρχές της ακρίβειας, της ελαχιστοποίησης και του ορθού σκοπού της επεξεργασίας των προσωπικών δεδομένων που είναι απαραίτητα για την επαλήθευση της ταυτότητας ενός φυσικού προσώπου. Με τον τρόπο αυτό

αποφεύγεται η μαζική – παράλληλη επεξεργασία δεδομένων που πιθανώς να μην είναι ορθά και ανακριβή.

3.Τρέχουσα Κατάσταση σε άλλες χώρες της Ε.Ε. σχετικά με τη χρήση εθνικού αριθμού ταυτότητας και το παράδειγμα της Ολλανδίας.

Η κατάσταση σε άλλες χώρες παρουσιάζεται κατωτερω:

Τρέχουσα κατάσταση σε άλλες χώρες μέλη της ΕΕ σε σχέση με ενιαία ταυτοποίηση

Χώρα – Αριθμός	Μοναδικός και ενιαίος	Καθολική αποδοχή	Ύπαρξη δεδομένων προσωπικού χαρακτήρα
Ολλανδία – Burgerservicenummmer	ΝΑΙ	ΝΑΙ	ΟΧΙ
Αυστρία – Source Identification Number (SourcePIN)	ΝΑΙ	ΝΑΙ	ΟΧΙ
Ισπανία – Documento Nacional de Identidad (DNI)	ΝΑΙ	ΝΑΙ	ΟΧΙ
Βέλγιο – National Register Number (NN)	ΝΑΙ	ΝΑΙ	ΝΑΙ (φύλο και ημερομηνία γέννησης)
Βουλγαρία – Uniform Civil Number (ΕΓΗ)	ΝΑΙ	ΝΑΙ	ΝΑΙ (φύλο και ημερομηνία γέννησης)
Δανία – CPR-nummer	ΝΑΙ	ΝΑΙ	ΝΑΙ (φύλο και ημερομηνία γέννησης)
Εσθονία – Isikukood (IK)	ΝΑΙ	ΝΑΙ	ΝΑΙ (φύλο και ημερομηνία γέννησης)
Φινλανδία – Henkilötunnus (HETU)	ΝΑΙ	ΝΑΙ	ΝΑΙ (φύλο και ημερομηνία γέννησης)
Λιθουανία – Asmens Kodas (AS)	ΝΑΙ	ΝΑΙ	ΝΑΙ (φύλο και ημερομηνία γέννησης)
Πολωνία – Powszechny Elektroniczny System Ewidencji Ludności (PESEL)	ΝΑΙ	ΝΑΙ	ΝΑΙ (φύλο και ημερομηνία γέννησης)
Σουηδία – Personnummer	ΝΑΙ	ΝΑΙ	ΝΑΙ (φύλο και ημερομηνία γέννησης)

Τρέχουσα κατάσταση σε άλλες χώρες μέλη της ΕΕ σε σχέση με ενιαία ταυτοποίηση

Χώρα – Αριθμός	Μοναδικός και ενιαίος	Καθολική αποδοχή	Ύπαρξη δεδομένων προσωπικού χαρακτήρα
Κροατία – Osobni Identifikacijski Broj (OIB)	ΟΧΙ	ΝΑΙ	ΟΧΙ
Ιρλανδία – Personal Public Service Number (PPS No.)	ΝΑΙ	ΟΧΙ	ΝΑΙ (φύλο)
Λετονία – Personas Kods (PK)	ΟΧΙ	ΝΑΙ	ΝΑΙ (ημερομηνία γέννησης)
Λουξεμβούργο – Tax Identification Number (TIN)	ΝΑΙ	ΝΑΙ	ΝΑΙ (ημερομηνία γέννησης)
Τσεχία & Σλοβακία – Rodné Číslo (RČ)	ΟΧΙ	ΝΑΙ	ΝΑΙ (φύλο και ημερομηνία γέννησης)
Γαλλία – Code Insee (INSEE)	ΝΑΙ	ΝΑΙ	ΝΑΙ (φύλο, τόπος και ημερομηνία γέννησης)
Ρουμανία – Cod Numeric Personal (CNP)	ΝΑΙ	ΝΑΙ	ΝΑΙ (φύλο, τόπος και ημερομηνία γέννησης)
Ιταλία – Codice Fiscale	ΟΧΙ	ΝΑΙ	ΝΑΙ (όνομα, φύλο, τόπος και ημερομηνία γέννησης)
Γερμάνια / Μ. Βρετανία / Πορτογαλία / Ουγγαρία: Κανένας ενιαίος αριθμός με καθολική αποδοχή			

4

Ειδικότερα, στην **Ολλανδία** έχει θεσμοθετηθεί ο **ενιαίος αριθμός BSN** (burgerservicenummer - **αριθμός «υπηρεσιών» πολίτη**), ο οποίος εκδίδεται **από το Υπουργείο Εσωτερικών** (Ministry of the Interior and Kingdom Relations) και αποτελεί το «πεδίο-κλειδί» του Μητρώου «Πληθυσμού» (Basisregistratie Personen).

Σημειώνεται ότι **στην Ολλανδία η έκδοση του ενιαίου αριθμού BSN είναι υποχρεωτική, εφόσον κάποιος**: α) ζήσει στην Ολλανδία για πάνω από 4 μήνες (resident), β) μείνει στην Ολλανδία για κάτω από 4 μήνες (non-resident) αλλά επιθυμεί τη διεξαγωγή συναλλαγής με τις δημόσιες υπηρεσίες στην Ολλανδία **ή με μη-δημόσιες που τον απαιτούν**, όπως π.χ. τράπεζες. Για την έκδοση του, **προϋπόθεση αποτελεί το νόμιμο δικαίωμα παραμονής** που **ελέγχεται από την Υπηρεσία Μεταναστευτικής Πολιτικής** (Ministry of Justice and Security - Immigration and Naturalization Service).

Ο ενιαίος αριθμός BSN δεν περιέχει πληροφορίες προσωπικού χαρακτήρα. Ο ενιαίος αριθμός BSN αντικατέστησε τον αριθμό sofinummer (SOcial FIscal) που εκδίδονταν από το Υπουργείο Οικονομικών (Tax and Customs Administration), με αυτόματη μετάβαση το 2007 (ένα παλαιό νούμερο sofinummer π.χ. 269740533 έμεινε το ίδιο). Το δε 2014 το Υπουργείο Οικονομικών σταμάτησε να εκδίδει sofinummer

4. Νέος Προσωπικός Αριθμός

Στο πλαίσιο χάραξης μιας ενιαίας πολιτικής ψηφιακής διακυβέρνησης, με στόχο την **παροχή προηγμένων ηλεκτρονικών υπηρεσιών με ασφάλεια και προστασία της ιδιωτικότητας σε πολίτες αλλά και επιχειρήσεις**, κρίνεται απαραίτητος ο προσδιορισμός και η εφαρμογή ενός μοναδικού **Προσωπικού Αριθμού που θα ακολουθεί τον Έλληνα Πολίτη** καθ' όλη τη διάρκεια της ζωής του σύμφωνα και με βάση τα παραδείγματα καλών και βέλτιστων πρακτικών άλλων ευρωπαϊκών κρατών[37].

Οι λόγοι, για τους οποίους είναι σημαντική η θέσπιση ενός ενιαίου εθνικού αριθμού είναι:

α) Ενοποίηση Δεδομένων: η ένταξη των δεδομένων που διατηρούνται σε back-end βάσεις δεδομένων στηρίζονται σε συνδυασμό δεδομένων που βρίσκονται σε data centers και με κοινό αναγνωριστικό, το οποίο χρησιμοποιείται εντός των συστημάτων της κυβέρνησης, και αναμένεται να βελτιώσει την αποτελεσματικότητα αυτού του ταιριάσματος-αντιστοίχισης των δεδομένων.

β) Μοίρασμα δεδομένων: σχετίζεται με το ταίριασμα δεδομένων που διατρέχει τους κυβερνητικούς οργανισμούς.

γ) Αυθεντικοποίηση: των χρηστών είναι μια σημαντική στρατηγική στη διασφάλιση των Πληροφοριακών Συστημάτων. Η χρήση βιομετρικών δεδομένων στην εθνική ταυτότητα με συσκευή πρόσβασης είναι πιθανό να βελτιώσει την αυθεντικοποίηση στα πληροφοριακά συστήματα.

δ) Ασφάλεια Δεδομένων: η σύνδεση ενός καθολικού αναγνωριστικού με τεχνολογίες ασφάλειας, όπως τα ψηφιακά πιστοποιητικά βελτιώνουν και αναβαθμίζουν το επίπεδο ασφαλείας των δεδομένων κατά την διαδικασία της αυθεντικοποίησης.

[37] Τέλος ΑΦΜ και ΑΜΚΑ - Μπαίνουν ταυτότητα και δίπλωμα στο κινητό. 18.07.2022. Διαθέσιμο σε: https://newsme.gr/telos-afm-kai-amka-mpainoyn-taytotita-kai-diploma-sto-kinito/

1. Άρθρο 11 του ν. 4727/2020 (Α' 184). Στο Κεφάλαιο Γ' (Προσωπικός Αριθμός) και στο άρθρο 11 του ν. 4727/2020 «Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) - Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις.» (ΦΕΚ 184/τ. Α'/23.09.2020) προβλέπεται ότι: «1. Καθιερώνεται προσωπικός αριθμός (Π.Α.) ως αριθμός υποχρεωτικής επαλήθευσης της ταυτότητας των φυσικών προσώπων στις συναλλαγές τους με τους φορείς του δημόσιου τομέα. Ο Π.Α. αποτελείται από δώδεκα (12) αλφαριθμητικά στοιχεία, εκ των οποίων τουλάχιστον τα εννέα (9) είναι αριθμητικά, και χορηγείται άπαξ στο φυσικό πρόσωπο. Ο Π.Α. δεν μεταβάλλεται και απενεργοποιείται με τον θάνατο ή την κήρυξη σε αφάνεια του φυσικού προσώπου.

2. Ο Π.Α. χορηγείται υποχρεωτικά σε κάθε φυσικό πρόσωπο που δικαιούται Αριθμό Φορολογικού Μητρώου (Α.Φ.Μ.) ή Αριθμό Μητρώου Κοινωνικής Ασφάλισης (Α.Μ.Κ.Α.), σύμφωνα με την εθνική νομοθεσία.

3. Η Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης (Γ.Γ.Π.Σ.Δ.Δ.) είναι αποκλειστικά αρμόδια για την **παροχή υπηρεσιών επαλήθευσης ταυτότητας των φυσικών προσώπων προς τους φορείς του δημόσιου τομέα και για την αντιστοίχιση των Π.Α. με τους αναγνωριστικούς αριθμούς των μητρώων (ειδικούς τομεακούς αριθμούς) των φορέων του δημόσιου τομέα,** ιδίως Α.Φ.Μ. και Α.Μ.Κ.Α., με σκοπό την επαλήθευση της ταυτότητας των φυσικών προσώπων και την επίτευξη διαλειτουργικότητας των πληροφοριακών συστημάτων των αρμόδιων φορέων μέσω του Κέντρου Διαλειτουργικότητας, υπό τους όρους προστασίας των δεδομένων προσωπικού χαρακτήρα, όπως προβλέπονται στον Γενικό Κανονισμό για την Προστασία Δεδομένων και την εθνική νομοθεσία.

4. Η Γ.Γ.Π.Σ.Δ.Δ. είναι υπεύθυνη επεξεργασίας για τους σκοπούς της επαλήθευσης της ταυτότητας των φυσικών προσώπων και τηρεί το Μητρώο Προσωπικού Αριθμού. Το Μητρώο Προσωπικού Αριθμού περιλαμβάνει τα στοιχεία που είναι απολύτως αναγκαία για την επαλήθευση της ταυτότητας του φυσικού προσώπου, ήτοι όνομα, επώνυμο, πατρώνυμο, μητρώνυμο, ημερομηνία γέννησης, τόπο γέννησης, Αριθμό Δελτίου Ταυτότητας, Α.Μ.Κ.Α., Α.Φ.Μ. Η τήρηση των δεδομένων του Μητρώου Π.Α. λαμβάνει χώρα, ακόμα και ύστερα από την απενεργοποίηση του Π.Α. για τους λόγους που προβλέπονται στην παρ. 1, στο πλαίσιο εκπλήρωσης καθήκοντος που εκτελείται προς το δημόσιο συμφέρον και κατά την άσκηση της ειδικής δημόσιας εξουσίας τήρησης του Μητρώου Π.Α., που έχει ανατεθεί στον Υπεύθυνο Επεξεργασίας και υπό τους όρους που προβλέπονται στον Γενικό Κανονισμό για την Προστασία Δεδομένων και την εθνική νομοθεσία.

5. Ο Π.Α. χορηγείται στα φυσικά πρόσωπα σύμφωνα με τη διαδικασία και το χρονοδιάγραμμα που ορίζεται στο προεδρικό διάταγμα που εκδίδεται σύμφωνα με την παρ. 6 του άρθρου 107. Με την διαδικασία αυτή χορηγείται ο Π.Α. και σε όσα φυσικά πρόσωπα έχει χορηγηθεί Α.Φ.Μ. ή/και Α.Μ.Κ.Α.

6. Οι φορείς του δημόσιου τομέα επεξεργάζονται τον Π.Α., μέσω του Κέντρου Διαλειτουργικότητας της Γ.Γ.Π.Σ.Δ.Δ., με μόνο και αποκλειστικό σκοπό την επαλήθευση της

ταυτότητας των φυσικών προσώπων για την παροχή δημόσιων υπηρεσιών προς φυσικά και νομικά πρόσωπα, την εν γένει διεκπεραίωση των υποθέσεων των φυσικών προσώπων και την άσκηση των αρμοδιοτήτων τους, χωρίς να τον συλλέγουν και αποθηκεύουν στα πληροφοριακά συστήματα ή στα συστήματα αρχειοθέτησης και τηρώντας τα απαραίτητα τεχνικά και οργανωτικά μέτρα που ορίζονται στο προεδρικό διάταγμα της παρ. 6 του άρθρου 107.

7. Ο Π.Α. δεν τηρείται από τους επιμέρους φορείς του δημόσιου τομέα, οι οποίοι αποδίδουν στα φυσικά πρόσωπα αναγνωριστικό αριθμό εσωτερικού τους μητρώου, για την επίτευξη της λειτουργικότητας των πληροφοριακών συστημάτων τους και των ειδικών ανεξάρτητων μητρώων τους. Όταν σύμφωνα με τη νομοθεσία απαιτείται η συλλογή και επεξεργασία του Α.Φ.Μ., ιδίως για φορολογικούς ή τελωνειακούς σκοπούς ή για σκοπούς είσπραξης δημοσίων εσόδων χρησιμοποιούνται και αποτελούν αντικείμενο επεξεργασίας μόνο τα τελευταία εννέα (9) αριθμητικά στοιχεία του Π.Α.»

Σύμφωνα με την εισηγητική έκθεση του ως άνω νόμου με την ως άνω διάταξη καθιερώνεται Προσωπικός Αριθμός (Π.Α.), ο οποίος αποτελεί στοιχείο για την επαλήθευση της ταυτότητας των φυσικών προσώπων που συναλλάσσονται με τους φορείς του δημόσιου τομέα. **Η επαλήθευση της ταυτότητας των φυσικών προσώπων πραγματοποιείται με τον συνδυασμό του Π.Α. και των στοιχείων φυσικής ή ηλεκτρονικής ταυτοποίησης.** Η χρήση αποκλειστικά και μόνο του Π.Α. δεν συνεπάγεται την ολοκλήρωση της επαλήθευσης της ταυτότητας του φυσικού προσώπου ούτε την παροχή δημοσίων υπηρεσιών προς αυτό. Ως εκ τούτου, ο Π.Α. αποτελεί στοιχείο αναγκαίο αλλά όχι επαρκές για την επαλήθευση της ταυτότητας των φυσικών προσώπων.

Με την καθιέρωση του προσωπικού αριθμού γίνεται μια μεγάλη τομή στη διαδικασία απλοποίησης και αυτοματοποίησης των διαδικασιών ταυτοποίησης του κάθε φυσικού προσώπου. Διευκολύνεται και απλοποιείται έτσι η διαλειτουργικότητα των διαφορετικών ψηφιακών συστημάτων του δημόσιου τομέα, δεδομένου ότι στο άμεσο μέλλον ο Π.Α. θα αποτελεί τον μοναδικό αριθμό που θα καλείται να χρησιμοποιεί ο κάθε πολίτης για τη συντριπτική πλειονότητα των συναλλαγών του με δημόσιους φορείς. Κατ' αυτόν τον τρόπο, εξαλείφεται το φαινόμενο ένα φυσικό πρόσωπο να εμφανίζεται «με πολλά πρόσωπα» έναντι του Δημοσίου. Ο Π.Α. αποτελείται από δώδεκα (12) αλφαριθμητικά στοιχεία, εκ των οποίων τουλάχιστον τα εννέα (9) τελευταία είναι αριθμητικά, και χορηγείται άπαξ στο φυσικό πρόσωπο, ενώ δεν μεταβάλλεται και απενεργοποιείται με τον θάνατο ή την κήρυξη σε αφάνεια του φυσικού προσώπου.

4.1. Κριτήρια για την απόδοση Προσωπικού Αριθμού

Τα κριτήρια για την απόδοση Π.Α. είναι είτε τα κριτήρια για τη λήψη Α.Φ.Μ. είτε τα κριτήρια για τη λήψη Α.Μ.Κ.Α., ο οποίος λαμβάνεται κατά τη γέννηση, σύμφωνα με την κείμενη νομοθεσία. Τα εννέα (9) τελευταία αριθμητικά στοιχεία του Π.Α. αποτελούν τον Α.Φ.Μ. του φυσικού προσώπου. Στη Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης (Γ.Γ.Π.Σ.Δ.Δ.) τηρείται το Μητρώο Π.Α., το οποίο περιλαμβάνει τα

στοιχεία που είναι απολύτως αναγκαία για την επαλήθευση της ταυτότητας του φυσικού προσώπου, ήτοι όνομα, επώνυμο, πατρώνυμο, μητρώνυμο, ημερομηνία γέννησης, τόπο γέννησης, Αριθμό Δελτίου Ταυτότητας, Α.Μ.Κ.Α. και Α.Φ.Μ. Για την ασφαλή τήρηση του Μητρώου Π.Α. λαμβάνονται από τη Γ.Γ.Π.Σ.Δ.Δ. όλα τα αναγκαία τεχνικά και οργανωτικά μέτρα και ιδίως η κρυπτογράφηση.

Η τήρηση του Π.Α. και η συγκέντρωση των σχετικών αναγνωριστικών πραγματοποιείται σε ένα κεντρικό σημείο, ήτοι στη Γ.Γ.Π.Σ.Δ.Δ., η οποία αποτελεί την αρμόδια αρχή για την επιβεβαίωση της ταυτότητας των πολιτών, σύμφωνα με το άρθρο 84 του παρόντος Κώδικα. Με τον τρόπο αυτό εξασφαλίζονται οι εγγυήσεις και τα μέτρα που μετριάζουν κατά πολύ τους κινδύνους,μέσω της κρυπτογράφησης του Μητρώου Π.Α. (βλ. σκέψη 83 του Γενικού Κανονισμού για την Προστασία Δεδομένων), της χρήσης εξυπηρετητών (servers) προηγμένης κυβερνοασφάλειαςκαι της τήρησης τεχνικών και οργανωτικών μέτρων που καλύπτουν την τήρηση των αρχών της αναλογικότητας και της αποτελεσματικότητας.

Για την επαλήθευση της ταυτότητας των συναλλασσομένων φυσικών προσώπων, οι φορείς του δημόσιου τομέα αξιοποιούν διαδικτυακή υπηρεσία της Γ.Γ.Π.Σ.Δ.Δ., με την οποία γίνεται η αντιστοίχιση του Π.Α., τον οποίο γνωστοποιεί ο πολίτης στον εκάστοτε φορέα του δημόσιου τομέα, με τα τηρούμενα στο Μητρώο Π.Α. στοιχεία. Κατά τη χρήση της ανωτέρω διαδικτυακής υπηρεσίας, δεν γίνεται διασύνδεση των αρχείων του Μητρώου Π.Α. με τα πληροφοριακά συστήματα και τα συστήματα αρχειοθέτησης των φορέων του δημόσιου τομέα που την αξιοποιούν. Οι φορείς του δημόσιου τομέα που αξιοποιούν την ανωτέρω διαδικτυακή υπηρεσία λαμβάνουν τα αναγκαία τεχνικά και οργανωτικά μέτρα, ώστε να μην τηρείται ούτε να αποθηκεύεται σε αυτούς ο Π.Α., σύμφωνα με τα οριζόμενα στην παρ. 7.

4.2. Συστηματοποίηση και οργάνωση του τρόπου λειτουργίας του Προσωπικού Αριθμού

Η ορθή και ασφαλής λειτουργία του Προσωπικού Αριθμού προϋποθέτει τον προηγούμενο **σχεδιασμό του από ειδικούς των Τεχνολογιών Πληροφορικής και Επικοινωνιών (Τ.Π.Ε.) σε σειρά ζητημάτων**:

(α) Τρόπος τήρησης του Μητρώου Προσωπικού Αριθμού και αποθήκευσης των συνοδών πληροφοριών (όνομα, επώνυμο, πατρώνυμο, ημερομηνία γέννησης, τόπος γέννησης, Α.Δ.Τ., Α.Φ.Μ., Α.Μ.Κ.Α.).

(β) Διαλειτουργικότητα με άλλα εθνικά πληροφοριακά συστήματα. Το πλαίσιο διαλειτουργικότητας απαιτείται να πληροί τα ακόλουθα κριτήρια:

- **Να έχει ως στόχο ένα τεχνολογικά ουδέτερο περιβάλλον** που δεν κάνει διακρίσεις μεταξύ συγκεκριμένων εθνικών τεχνικών λύσεων για την ηλεκτρονική ταυτοποίηση εντός του κράτους-μέλους.

- **Να ακολουθεί τα ευρωπαϊκά και διεθνή πρότυπα**, όταν αυτό είναι εφικτό.

- **Να διευκολύνει ήδη από τη φάση του σχεδιασμού, την εφαρμογή της αρχής της προστασίας της ιδιωτικής ζωής.**

- **Να διασφαλίζει την επεξεργασία των δεδομένων προσωπικού χαρακτήρα**, σύμφωνα με τον Γενικό Κανονισμό για την Προστασία των Δεδομένων Προσωπικού Χαρακτήρα[38] (βλ. άρθρο 12, παρ. 8 του Κανονισμού eIDAS).

(γ) Ενεργοποίηση των δικαιωμάτων του φυσικού προσώπου βάσει του Κανονισμού για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα, όπως το δικαίωμα διόρθωσης, της φορητότητας, και της πρόσβασης.

(δ) Χρόνος ζωής του προσωπικού αριθμού/διάρκεια διατήρησης των δεδομένων.

(ε) Σημαντική παράμετρος αποτελεί η διατήρηση των δεδομένων σύνδεσης και ιχνηλάτησης των δεδομένων.

4.2.α Αυθεντικοποίηση

Στο πεδίο της αυθεντικοποίησης, η **μέθοδος Single Sign-On (SSO)** επιτρέπει στο χρήστη να **αυθεντικοποιηθεί την ταυτότητα του φυσικού προσώπου σε περισσότερες εφαρμογές και ιστοτόπους**, χρησιμοποιώντας ένα και μόνο σετ διαπιστευτηρίων.

Πρόκειται για μέθοδο που **βασίζεται σε μία σχέση εμπιστοσύνης** που έχει εγκαθιδρυθεί **μεταξύ του παρόχου υπηρεσίας και του παρόχου ταυτότητας**.

Η **ροή του login στο Single Sign-On περιλαμβάνει μία σειρά από βήματα**, τα οποία αποτυπώνονται παρακάτω. Αρχικά, ο πάροχος της ταυτότητας αποστέλλει ένα τόκεν που περιλαμβάνει συγκεκριμένες πληροφορίες σχετικές με τον χρήστη, όπως η διεύθυνση e-mail στο σύστημα του SSO, ως μέρος του αιτήματος για αυθεντικοποίηση. Έτσι, ελέγχεται από τον πρώτο εάν και κατά πόσο ο χρήστης έχει ήδη αυθεντικοποιηθεί. Εφόσον αυτό δεν έχει πραγματοποιηθεί, η αυθεντικοποίηση μπορεί να γίνει με One Time Password. Από τη στιγμή που ο πάροχος εγκρίνει τα διαπιστευτήρια που παρέχονται, στέλνει ένα τόκεν πίσω, στον πάροχο υπηρεσίας, επιβεβαιώνοντας την επιτυχή αυθεντικοποίηση. Εφόσον εγκρίνονται τα διαπιστευτήρια, ο πάροχος υπηρεσίας επιβεβαιώνει την αυθεντικοποίηση. Το τόκεν που παρελήφθη από τον πάροχο υπηρεσίας εγκρίνεται κατά τη συμφωνία που ιδρύθηκε μεταξύ του παρόχου υπηρεσίας και του παρόχου ταυτότητας, κατά τη διάρκεια της αρχικής διαμόρφωσης.

[38] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)

Το **Single sign-on (SSO)**[39] **συνιστά ένα σχήμα ελέγχου ταυτότητας που επιτρέπει σε έναν χρήστη να συνδεθεί με ένα μόνο αναγνωριστικό σε οποιοδήποτε από τα πολλά σχετικά, αλλά ανεξάρτητα, συστήματα λογισμικού**. Περαιτέρω, η True single sign-on επιτρέπει στο χρήστη να συνδέεται μία φορά και να έχει πρόσβαση σε υπηρεσίες, χωρίς να εισάγει ξανά παράγοντες ελέγχου ταυτότητας. Ωστόσο, δεν πρέπει να συγχέεται με την ταυτόχρονη σύνδεση (Επαλήθευση διακομιστή καταλόγου), που συχνά επιτυγχάνεται με τη χρήση του Lightweight Directory Access Protocol (LDAP) και τις αποθηκευμένες βάσεις δεδομένων LDAP σε διακομιστές (καταλόγου)[40]. Μια απλή έκδοση της απλής σύνδεσης μπορεί να επιτευχθεί, μέσω δικτύων IP, χρησιμοποιώντας cookies, αλλά μόνο εάν οι ιστότοποι μοιράζονται έναν κοινό γονικό τομέα DNS[41].

Για λόγους σαφήνειας, γίνεται διάκριση μεταξύ ελέγχου ταυτότητας διακομιστή καταλόγου (ίδια σύνδεση) και απλής σύνδεσης. Ο έλεγχος ταυτότητας διακομιστή καταλόγου αναφέρεται σε συστήματα που απαιτούν έλεγχο ταυτότητας για κάθε εφαρμογή, αλλά χρησιμοποιούν τα ίδια διαπιστευτήρια από έναν διακομιστή καταλόγου, ενώ η απλή σύνδεση αναφέρεται σε συστήματα όπου ένας μεμονωμένος έλεγχος ταυτότητας παρέχει πρόσβαση σε πολλαπλές εφαρμογές, περνώντας το διακριτικό ελέγχου ταυτότητας, χωρίς προβλήματα σε διαμορφωμένες εφαρμογές. Αντίθετα, η απλή αποσύνδεση (SLO) είναι η ιδιότητα με την οποία μια μεμονωμένη ενέργεια αποσύνδεσης τερματίζει την πρόσβαση σε πολλαπλά συστήματα λογισμικού.

Καθώς διαφορετικές εφαρμογές και πόροι υποστηρίζουν διαφορετικούς μηχανισμούς ελέγχου ταυτότητας, η απλή σύνδεση πρέπει να αποθηκεύει εσωτερικά τα διαπιστευτήρια που χρησιμοποιούνται για τον αρχικό έλεγχο ταυτότητας και να τα μεταφράζει στα διαπιστευτήρια που απαιτούνται για τους διαφορετικούς μηχανισμούς.

Άλλα κοινόχρηστα σχήματα ελέγχου ταυτότητας, όπως το OpenID και το OpenID Connect, προσφέρουν υπηρεσίες, που ενδέχεται να απαιτούνται από τους χρήστες, ώστε να κάνουν επιλογές κατά τη διάρκεια της σύνδεσης σε έναν πόρο. Τα κοινόχρηστα αυτά σχήματα ελέγχου ταυτότητας, μπορούν να διαμορφωθούν και για απλή σύνδεση, εάν αυτές οι άλλες υπηρεσίες (όπως η συναίνεση του χρήστη) είναι απενεργοποιημένες[42]. Ένας αυξανόμενος αριθμός ομόσπονδων συνδέσεων κοινωνικής δικτύωσης, όπως το Facebook Connect, απαιτεί από τον χρήστη να εισαγάγει επιλογές συναίνεσης κατά την πρώτη εγγραφή σε έναν νέο πόρο και, επομένως, δεν πρόκειται, πάντα για απλή σύνδεση με την αυστηρή έννοια.

Τα **οφέλη από τη χρήση σύνδεσης Single sign-on περιλαμβάνουν**[43]:

[39] https://en.wikipedia.org/wiki/Single_sign-on
[40] "What's the Difference b/w SSO (Single Sign On) & LDAP?". JumpCloud. 14-05-2019.
"SSO and LDAP Authentication". Authenticationworld.com. 23-05-2014.
[41] "OpenID versus Single-Sign-On Server". alleged.org.uk. 13-08-2007.
[42] "OpenID Connect Provider - OpenID Connect Single Sign-On (SSO) - OIDC OAuth Authentication". OneLogin.
[43] "Benefits of SSO". University of Guelph.

- **Μετριασμό του κινδύνου πρόσβασης σε ιστοτόπους τρίτων**, επειδή οι κωδικοί πρόσβασης του χρήστη δεν αποθηκεύονται ή αποτελούν αντικείμενο διαχείρισης εξωτερικά.
- **Περιορισμό της χρήσης κωδικών πρόσβασης με διαφορετικούς συνδυασμούς ονομάτων χρήστη και κωδικών πρόσβασης**.
- **Μείωση του χρόνου που απαιτείται για την εκ νέου εισαγωγή κωδικών πρόσβασης για την ίδια ταυτότητα**.
- **Μείωση του κόστους των ψηφιακών υπηρεσιών**, λόγω του μικρότερου αριθμού κλήσεων αναφορικά με τους κωδικούς πρόσβασης.
- **Απλούστευση της χορήγησης των κωδικών πρόσβασης**, με παράλληλη **μείωση των εργασιών που σχετίζονται με το SSO** που καθίστανται πιο διαφανείς και εκτελούνται στο πλαίσιο της κανονικής συντήρησης του συστήματος, ώστε να χρησιμοποιούνται τα ίδια εργαλεία που χρησιμοποιούνται και για άλλες διοικητικές εργασίες.
- **Βέλτιστος διοικητικός έλεγχος**, αφού όλες οι πληροφορίες διαχείρισης δικτύου αποθηκεύονται σε έναν ενιαίο χώρο αποθήκευσης. Τούτο σημαίνει ότι υπάρχει μία ενιαία, έγκυρη λίστα με τα δικαιώματα και τα προνόμια κάθε χρήστη. Επίσης, επιτρέπει στον διαχειριστή να αλλάζει τα προνόμια ενός χρήστη και γνωρίζει ότι τα αποτελέσματα θα διαδοθούν σε όλο το δίκτυο.
- **Βελτιωμένη παραγωγικότητα του χρήστη**, αφού οι χρήστες δεν εμπλέκονται σε πολλαπλές συνδέσεις, ούτε απαιτείται να απομνημονεύουν και να χρησιμοποιούν πολλούς κωδικούς πρόσβασης για την είσοδό τους στους πόρους του δικτύου. Τούτο είναι θετικό και για το προσωπικό του Help Desk, το οποίο δεν απαιτείται να επεξεργάζεται πολλά αιτήματα για κωδικούς πρόσβασης που έχουν ξεχαστεί.
- **Βελτιωμένη ασφάλεια δικτύου,** από το γεγονός ότι η αποφυγή πολλών κωδικών πρόσβασης περιορίζει αντίστοιχα τις πηγές παραβίασης ασφαλείας, αφού οι χρήστες καταγράφουν τους κωδικούς πρόσβασής τους. Επίσης, όταν ο διαχειριστής απενεργοποιεί ένα λογαριασμό αυτός απενεργοποιείται πλήρως.
- **Επιτυγχάνεται ενοποίηση ετερογενών δικτύων**, αφού με τη συμμετοχή σε διαφορετικά δίκτυα, ενοποιούνται αντίστοιχα οι διοικητικές προσπάθειες, ώστε να βελτιώνονται οι διοικητικές διαδικασίες, με αξιοποίηση βέλτιστων διοικητικών πρακτικών και εταιρικών πολιτικών ασφαλείας.

Το SSO μοιράζεται κεντρικούς διακομιστές ελέγχου ταυτότητας που χρησιμοποιούν όλες οι άλλες εφαρμογές και συστήματα για σκοπούς ελέγχου ταυτότητας και το συνδυάζει με τεχνικές για να διασφαλίσει ότι οι χρήστες δεν χρειάζεται να εισάγουν ενεργά τα διαπιστευτήριά τους περισσότερες από μία φορές.

Ως προς το σκέλος της ασφάλειας του Single Sign-On, καταρχάς, θεωρείται ότι διαθέτει υψηλό επίπεδο ασφαλείας. **Ωστόσο, για την ενίσχυση της ασφάλειας αυτής της μεθόδου αυθεντικοποίησης, θα ήταν χρήσιμο να ζητείται ένας επιπλέον παράγοντας αυθεντικοποίησης που να δίνει τη δυνατότητα κάποιος να συνδέεται σε μία συγκεκριμένη εφαρμογή**, με την προϋπόθεση ότι οι χρήστες έχουν ασφαλή σύνδεση. Περαιτέρω, υπάρχει και η λύση της διάφορης αυθεντικοποίησης από Εφαρμογή σε Εφαρμογή (App-App), η οποία όμως δεν είναι ακόμα διαθέσιμη.

4.3. Προσωπικός Αριθμός & Προστασία Δεδομένων Προσωπικού Χαρακτήρα

α. Η έννοια της διασύνδεσης Αρχείων και η προϊσχύσασα νομοθεσία

Η υιοθέτηση προσωπικού αριθμού δεν είναι νέα ιδέα. Αξιοσημείωτη είναι η παλαιότερη ρύθμιση του **άρθρου 2 του ν.1599/1986**[44] (αργότερα καταργήθηκε με το άρθρο 6 του Ν. 1988/1991) που προέβλεπε τη θέσπιση «Ενιαίου Κωδικού Αριθμού Μητρώου (Ε.Κ.Α.Μ.) για κάθε έλληνα πολίτη». Στην παράγραφο 4 του συγκεκριμένου άρθρου, ρητά οριζόταν στο τελευταίο εδάφιο ότι «Για αρχεία πληροφοριών στα οποία χρησιμοποιείται ο Ε.Κ.Α.Μ. εφαρμόζονται όλες οι διατάξεις της νομοθεσίας για την προστασία του ατόμου από την επεξεργασία των προσωπικών πληροφοριών και έως ότου τεθεί σε ισχύ σχετικός νόμος δεν επιτρέπεται η διασύνδεση των αρχείων αυτών είτε μεταξύ τους, είτε με άλλα αρχεία, ούτε η χρησιμοποίηση του Ε.Κ.Α.Μ., ως κωδικού αριθμού σε άλλα αρχεία προσωπικών πληροφοριών. Η παράβαση της διάταξης αυτής τιμωρείται με φυλάκιση τουλάχιστον 6 μηνών.»

Υπό το καθεστώς της προϊσχύσασας νομοθεσίας περί προσωπικών δεδομένων η «διασύνδεση αρχείων με ενιαίο αριθμό» τέθηκε υπό το αυστηρό καθεστώς της χορήγησης αδείας εκ μέρους της ΑΠΔΠΧ. Ήδη, η Οδηγία 95/46/ΕΚ45, στο άρθρο 8§7, είχε προβλέψει ότι «Τα κράτη μέλη καθορίζουν τους όρους υπό τους οποίους επιτρέπεται η επεξεργασία του εθνικού αναγνωριστικού αριθμού ταυτότητας ή άλλων γενικότερων αναγνωριστικών της ταυτότητας στοιχείων».

Με βάση αυτή την διάταξη, στο **άρθρο 8§3 του Ν.2472/1997**, οριζόταν ότι: «Εάν ένα τουλάχιστον από τα αρχεία που πρόκειται να διασυνδεθούν περιέχει ευαίσθητα δεδομένα ή εάν η διασύνδεση έχει ως συνέπεια την αποκάλυψη ευαίσθητων δεδομένων ή εάν για την πραγματοποίηση της διασύνδεσης πρόκειται να γίνει χρήση ενιαίου κωδικού αριθμού, η διασύνδεση επιτρέπεται μόνο με προηγούμενη άδεια της Αρχής (άδεια διασύνδεσης)».

Από τα ανωτέρω προκύπτει σαφώς, ότι για το κρίσιμο ζήτημα της διασύνδεσης δεδομένων, καθιερωνόταν, κατ' αρχάς, σύστημα γνωστοποίησης για κάθε διασύνδεση και σύστημα προηγούμενης άδειας της ΑΠΔΠΧ. εάν ένα τουλάχιστον από τα αρχεία ή τις επεξεργασίες που πρόκειται να διασυνδεθούν περιείχε ευαίσθητα δεδομένα (υπό την ορολογία της τότε νομοθεσίας) ή εάν, για την πραγματοποίηση της διασύνδεσης, επρόκειτο να γίνει χρήση ίδιου κωδικού αριθμού[46].

β. Ο ΓΚΠΔ και ο ν. 4624/2019

---

[44] Ν. 1599/1986 Σχέσεις κράτους - πολίτη, καθιέρωση νέου τύπου δελτίου ταυτότητας και άλλες διατάξεις. (Α΄ 75/11.6.1986).

[45] Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

[46] Επί τη βάσει αυτών εκδόθηκε π.χ. η Αποφάση της ΑΠΔΠΧ 92/2002 «Διασύνδεση αρχείων Υπουργείων Μεταφορών και Επικοινωνιών, Δημόσιας Τάξης και Οικονομικών», ενώ με την Άδεια της ΑΠΔΠΧ 21/2007 επετράπη η διασύνδεση αρχείων της ΤΕΙΡΕΣΙΑΣ ΑΕ με την ΓΓΠΣ με χρήση ενιαίου κωδικού αριθμού σύμφωνα με το άρθρο 8 παρ.3 και 4 του ν.2472/1997.

Στον **Κανονισμό (ΕΕ) 2016/679, (ΓΚΠΔ) στο άρθρο 87, εδάφιο δεύτερο,** ορίζεται ότι «[...] **ο εθνικός αριθμός ταυτότητας ή οποιοδήποτε άλλο αναγνωριστικό στοιχείο ταυτότητας γενικής εφαρμογής χρησιμοποιείται μόνο με τις δέουσες εγγυήσεις για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων δυνάμει του παρόντος κανονισμού».** Περαιτέρω, στον ν.4624/2019[47], που εισήγαγε μέτρα εφαρμογής του ΓΚΠΔ, δεν απαντάται, πλέον, η ειδική απαγόρευση του άρθρου 8§3 του ν. 2472/1997. Ωστόσο, αυτή ορθότερο είναι να θεωρείται ότι καλύπτεται ουσιαστικά από τις γενικές διατάξεις και τη διαφορετική νομική αρχιτεκτονική του ΓΚΠΔ και του ν.4624/2019.

Επισημαίνουμε στο σημείο αυτό ότι στο Case C-439/19, Latvijas Republikas Saeima Στις 17 Δεκεμβρίου 2020, ο γενικός εισαγγελέας Szpunar εξέδωσε τη γνώμη του στην Latvijas Republikas Saeima και μεταξύ άλλων, η γνωμοδότηση ερμηνεύει το υλικό πεδίο εφαρμογής του GDPR υπό το φως του άρθρου 2 παράγραφος 2 στοιχείο α), το οποίο αποκλείει την εφαρμογή του GDPR στα δεδομένα επεξεργασίας «κατά τη διάρκεια μιας δραστηριότητας που δεν εμπίπτει στο πεδίο εφαρμογής του δικαίου της Ένωσης».Στο πλαίσιο αυτό, ο γενικός εισαγγελέας τόνισε ότι «ο ίδιος ο σκοπός του GDPR είναι να τον κάνει να εφαρμόζεται σε οποιαδήποτε μορφή επεξεργασίας προσωπικών δεδομένων, ανεξάρτητα από το αντικείμενο»,και ότι, ως εξαίρεση από έναν γενικό κανόνα, το άρθρο 2 παράγραφος 2 στοιχείο α) του GDPR πρέπει να ερμηνεύεται αυστηρά. Επομένως, ο Γενικός Εισαγγελέας θεωρεί το άρθρο 87 GDPR ως επιβεβαίωση αυτού, καθώς προβλέπει τη δυνατότητα εφαρμογής του GDPR στην επεξεργασία των εθνικών αριθμών αναγνώρισης, ως ένα θέμα που ρυθμίζεται τυπικά από το εσωτερικό δίκαιο και όχι από την ΕΕ.48.

Επίσης σύμφωνα με το άρθρο 47 του ν.4623/2019 ορίζεται :

«2. Όταν πρόκειται για δεδομένα προσωπικού χαρακτήρα το Υπουργείο Ψηφιακής Διακυβέρνησης ορίζεται υπεύθυνος επεξεργασίας, κατά την έννοια του άρθρου 26 του Κανονισμού (ΕΕ) 2016/ 679 (Γενικός Κανονισμός Προστασίας Δεδομένων) όλων των δεδομένων των Φορέων του Δημόσιου Τομέα και του ευρύτερου Δημόσιου Τομέα κατά την έννοια του άρθρου 3 του ν. 3979/2011 (Α΄ 138) με αντικείμενο τον στρατηγικό σχεδιασμό, την επεξεργασία και τη διασύνδεση όλων των δεδομένων των ως άνω φορέων μέσω της χρήσης νέων τεχνολογιών, με σκοπό τη διαλειτουργικότητα των πληροφοριακών συστημάτων και εφαρμογών, τη διαβίβαση των δεδομένων μεταξύ των Φορέων είτε για την άσκηση της αρμοδιότητας των Φορέων είτε σύμφωνα με την κείμενη νομοθεσία είτε μετά από τη ρητή έγγραφη ή ηλεκτρονική συγκατάθεση του υποκειμένου των δεδομένων, τη χρήση υπηρεσιών νέφους, την αυτεπάγγελτη αναζήτηση δικαιολογητικών ή πιστοποιητικών ή εγγράφων των πολιτών είτε για την άσκηση της αρμοδιότητας των Φορέων είτε σύμφωνα με την κείμενη νομοθεσία είτε μετά από τη ρητή έγγραφη ή ηλεκτρονική συγκατάθεση του

[47] Ν. 4624/2019 (ΦΕΚ Α' 137/29.8.2019) Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

[48] Case C-439/19, Latvijas Republikas Saeima (AG Opinion), para. 52.
The EU General Data Protection Regulation: A Commentary Update of Selected Articles edited by Christopher Kuner Lee A. Bygrave Christopher Docksey

υποκειμένου των δεδομένων, την ανταλλαγή μεταξύ των ως άνω Φορέων δικαιολογητικών και δεδομένων των πολιτών είτε για την άσκηση της αρμοδιότητας των Φορέων είτε σύμφωνα με την κείμενη νομοθεσία είτε μετά από τη ρητή έγγραφη ή ηλεκτρονική συγκατάθεση του υποκειμένου των δεδομένων, και την παροχή ηλεκτρονικών υπηρεσιών εξυπηρέτησης των πολιτών, και μόνο ως προς τους ανωτέρω σκοπούς. Κάθε φορέας που επιθυμεί ο ίδιος να διασυνδέσει ή να διαλειτουργήσει αρχεία δεδομένων ή μητρώων με άλλο φορέα ή να κάνει χρήση υπηρεσιών νέφους ή να προβεί σε οποιαδήποτε ενέργεια που περιγράφεται στο προηγούμενο εδάφιο της παρούσας παραγράφου οφείλει προηγουμένως να λάβει την έγκριση του Γενικού Γραμματέα Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης με σκοπό να διασφαλιστεί η εναρμόνιση με τον στρατηγικό σχεδιασμό.

3. Με απόφαση του Υπουργού Ψηφιακής Διακυβέρνησης μπορούν να ρυθμίζονται όλες οι λεπτομέρειες για την υλοποίηση των σκοπών των παραγράφων 1 και 2 του παρόντος άρθρου καθώς και τα απαιτούμενα τεχνικά και οργανωτικά μέτρα και οι σχετικές διαδικασίες που πρέπει να τηρούνται κατά την επεξεργασία των δεδομένων με σκοπό την ασφάλεια και την προστασία τους, μετά από την διενέργεια εκτίμησης αντικτύπου, όπου αυτή απαιτείται, αλλά και τις σχετικές διαδικασίες για την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων και διαχείριση των αιτημάτων αυτών. Οι Φορείς του Δημόσιου Τομέα και του ευρύτερου Δημόσιου Τομέα κατά την έννοια του άρθρου 3 του ν. 3979/2011 (Α΄ 138) υποχρεούνται άμεσα και χωρίς υπαίτια καθυστέρηση να προβαίνουν σε όλες τις απαραίτητες ενέργειες για την υλοποίηση των σκοπών των παραγράφων 1 και 2 του παρόντος άρθρου αλλά και για την εφαρμογή της ως άνω Υπουργικής Απόφασης**. Με απόφαση του Υπουργού Ψηφιακής Διακυβέρνησης ορίζονται οι ομάδες εργασίας και τα αρμόδια συλλογικά όργανα για την υλοποίηση των ως άνω σκοπών**, μετά από εισήγηση των εμπλεκόμενων κατά περίπτωση φορέων.»

Ως κρίσιμο στοιχείο αναδεικνύεται η πρόδηλη διαφοροποίηση του Π.Α. ως μίας υπηρεσίας παροχής ταυτοποίησης / αυθεντικοποίησης «Identity as a Service (IdaaS) | Authentication as a Service (AaaS)» και όχι ως μίας μορφής διασύνδεσης αρχείων και μητρώων διαφορετικών φορέων του δημοσίου, με προδήλως διαφορετικές νομικές βάσεις και σκοπούς επεξεργασίας ανά κατηγορία ειδικών ή μη δεδομένων των φυσικών προσώπων. Η εφαρμογή των γενικών αρχών του ΓΚΠΔ (άρθρο 5) σε συνδυασμό με τη νομιμότητα της επεξεργασίας (άρθρο 6) οφείλει να μην εστιάσει στη λειτουργία του Π.Α. αυτή καθεαυτή, αφού είναι σαφές ότι δεν διασυνδέει προσωπικά ή ειδικά δεδομένα φυσικών προσώπων, παρά μόνο συμβάλει στην ταυτοποίηση τους και μάλιστα με τρόπο ακριβή, ασφαλή και ενιαίο.

Ωστόσο, δεν υπάρχει αμφιβολία ότι ο Π.Α., όπως και ο ΑΦΜ, αποτελούν προσωπικά δεδομένα των φυσικών προσώπων. Συνεπώς, κατά την γνώμη μας, αρκεί η γενική επισκόπηση των τεχνικών και οργανωτικών μέτρων, του μηχανισμού υλοποίησης της απόδοσης και μετάπτωσης στο καθεστώς χρήσης του Π.Α. Στόχος είναι να εξασφαλίζεται ότι η λειτουργία του θα περιορίζεται κατά τον σχεδιασμό με τέτοια (τεχνικά) μέτρα, ώστε να μην επιδέχεται οποιαδήποτε άλλη προσέγγιση ή χρήση πλην της παροχής υπηρεσιών ταυτοποίησης / αυθεντικοποίησης «Identity as a Service (IdaaS) | Authentication as a Service (AaaS)». Ακόμη δηλαδή και η τυχόν εκπόνηση Μελέτης Εκτίμησης Αντικτύπου στα Προσωπικά Δεδομένα (ΕΑΠΔ) κατ' άρ. 35 ΓΚΠΔ πρέπει να περιοριστεί σε αυτόν τον έλεγχο.

Πέραν αυτού, δεν διαπιστώνονται άλλα σημεία στάθμισης ή μελέτης πιθανού κινδύνου για τα προσωπικά δεδομένα των φυσικών προσώπων.

γ. Ζητήματα ως προς την τήρηση/αποθήκευση του προσωπικού αριθμού

Σε κάθε περίπτωση αποσαφηνίζουμε ότι δεν τίθεται ζήτημα μετάπτωσης των πληροφοριακών συστημάτων του Δημοσίου και ενημέρωσής τους με τον Προσωπικό Αριθμό. Όπως διαφαίνεται από την προτεινόμενη διάταξη, ο Προσωπικός Αριθμός θα τηρείται μόνο σε ένα κεντρικό σημείο (ΓΓΠΣΔΔ). Ο Προσωπικός Αριθμός δεν θα τηρείται από τους επιμέρους φορείς του δημοσίου, όπως ρητά αναφέρεται στην παρ. 8 της προτεινόμενης διάταξης, παρά μόνο από τη ΓΓΠΣΔΔ και δεν θα αποτελεί κλειδί για τη διασύνδεση με άλλα μητρώα του δημοσίου. Επισημαίνεται ότι οι φορείς του δημοσίου εξακολουθούν και έχουν πρόσβαση μόνο στα απαραίτητα δεδομένα φυσικών προσώπων και μόνο για την άσκηση των αρμοδιοτήτων και των καθηκόντων τους. Για τους παραπάνω λόγους, δεν τίθεται ζήτημα μετάπτωσης των πληροφοριακών συστημάτων του δημοσίου και ενημέρωσής τους με τον Π.Α. Συναφώς, γίνεται σαφές ότι ο Προσωπικός Αριθμός δεν θα τηρείται «και στο χώρο της υγείας και της κοινωνικής ασφάλισης», καθώς προβλέπεται η τήρησή του μόνο σε ένα κεντρικό σημείο (ΓΓΠΣΔΔ).

Με το παρόν, λαμβάνουμε την ευκαιρία να διευκρινίσουμε ότι δεν αρκεί μόνο η χρήση του Π.Α.για την παροχή δημοσίων υπηρεσιών από τους φορείς του δημόσιου τομέα προς τα φυσικά πρόσωπα. Η επαλήθευση της ταυτότητας, η οποία απαιτείται για την παροχή δημοσίων υπηρεσιών, διεξάγεται με τον συνδυασμό του Προσωπικού Αριθμού, τον οποίο παρέχει ο πολίτης προς τον εκάστοτε δημόσιο φορέα, με τον ειδικό τομεακό αριθμό με τον οποίο ο πολίτης είναι καταγεγραμμένος σε μητρώο του φορέα αυτού. Απαραίτητη είναι η επίδειξη της ταυτότητας του φυσικού προσώπου όταν η χρήση του Προσωπικού Αριθμού θα γίνεται με φυσική παρουσία ή η χρήση ηλεκτρονικών κωδικών όταν η χρήση του Προσωπικού Αριθμού θα γίνεται εξ αποστάσεως με ηλεκτρονικά μέσα. Στο παράδειγμα που αναφέραμε στο υπό (β) σχετικό, ο πολίτης επισκέπτεται το αρμόδιο υποκατάστημα του ΕΦΚΑ του τόπου κατοικίας του, επιδεικνύει την ταυτότητα του και ενημερώνει τον υπάλληλο ότι ο Π.Α. του είναι ο «ΑΧΒ123456789». Ο πολίτης είναι καταγεγραμμένος στον εν λόγω φορέα με τον ΑΜΚΑ, ο οποίος αποτελεί τον ειδικό τομεακό αριθμό. Ο υπάλληλος του ΕΦΚΑ δεν μπορεί να αναζητήσει στο πληροφοριακό σύστημα του φορέα τον Προσωπικό Αριθμό, καθότι ο Προσωπικός Αριθμός τηρείται μόνο στη ΓΓΠΣΔΔ. Ο υπάλληλος του ΕΦΚΑ, αφού ολοκληρώσει τη φυσική ταυτοποίηση του πολίτη μέσω της επίδειξης του δελτίου αστυνομικής ταυτότητας, προβαίνει στην επαλήθευση της ταυτότητάς του μέσω της αντιστοίχισης του Προσωπικού Αριθμού (τον οποίο γνωρίζει ο πολίτης) με τον ειδικό τομεακό αριθμό (ο οποίος τηρείται στο πληροφοριακό σύστημα του φορέα). Η αντιστοίχιση αυτή γίνεται από την ΓΓΠΣΔΔ μέσω ασφαλούς δομής διαδικτυακής υπηρεσίας (secure web service). Συνεπώς, μόνο μέσα από τον συνδυασμό Προσωπικού Αριθμού και ειδικών τομεακών αριθμών είναι δυνατή η παροχή δημοσίων υπηρεσιών.

Στο ανωτέρω παράδειγμα, έγινε φανερή η χρήση και η λειτουργία του Προσωπικού Αριθμού ως στοιχείου αναγκαίου αλλά όχι επαρκούς από μόνο του για την επαλήθευση της ταυτότητας φυσικών προσώπων. Η χρησιμότητα της θέσπισης του Προσωπικού Αριθμού έγκειται στη διευκόλυνση των συναλλασσομένων με τους φορείς του δημόσιου τομέα φυσικών προσώπων, ώστε να απαιτείται η γνώση μόνο ενός αριθμού για την επαλήθευση

της ταυτότητάς τους και όχι περισσοτέρων αριθμών που του αποδίδουν οι εκάστοτε φορείς (ειδικοί τομεακοί αριθμοί/αριθμοί μητρώων).

Ο Προσωπικός Αριθμός δεν τηρείται από τους επιμέρους φορείς, όπως ρητά έχει διευκρινιστεί και ορίζεται στο σχέδιο της διάταξης. Ο Προσωπικός Αριθμός αποτελεί αλφαριθμητικό σύνολο που δεν είναι γνωστό σε τρίτους, όπως σήμερα ο ΑΜΚΑ, και η γνώση του ΑΦΜ και μόνο δεν αρκεί για το σχηματισμό του Προσωπικού Αριθμού. Το ίδιο συμβαίνει σήμερα με την ημερομηνία γέννησης, που μπορεί να είναι γνωστή σε τρίτους, αλλά αποτελεί ένα μέρος μόνο του ΑΜΚΑ, που συνολικά δεν είναι και δεν μπορεί να καταστεί γνωστός. Ενδεικτικώς, σε σχέση με την υπηρεσία αναζήτησης ΑΜΚΑ [https://www.amka.gr], που επιτρέπει τον συνδυασμό επιμέρους προσωπικών δεδομένων, το σύστημα του Π.Α. θα παρέχει υψηλότερο επίπεδο ασφαλείας, καθώς δεν θα μπορεί να αναζητηθεί online ή με άλλο τρόπο από μη εξουσιοδοτημένους τρίτους. Κατόπιν των ανωτέρω, θεωρούμε ότι η εισαγωγή του Προσωπικού Αριθμού ως εργαλείου επαλήθευσης της ταυτότητας των φυσικών προσώπων, ουδόλως αυξάνει την πιθανότητα απόκτησης πρόσβασης τρίτων σε ειδικές κατηγορίες δεδομένων.

Με την φράση «παύση χορήγησης» , περιγράφεται οργανωτικά η παύση ανάγκης γνώσης του εσωτερικού αριθμού μητρώου/ αναγνώρισης σε κάθε επιμέρους φορέα. Η εσωτερική διαδικασία απόδοσης του αριθμού αυτού για τη λειτουργία των επιμέρους μητρώων δεν θα παύσει να υφίσταται, αλλά πλέον το φυσικό πρόσωπο που θα προσέρχεται σε έναν φορέα ούτε θα απαιτείται, ούτε θα χρησιμεύει να γνωρίζει τον «εσωτερικό» αριθμό καταχώρισής του στα συστήματα (π.χ «πρώην» ΑΜΚΑ), παρά μόνο τον Προσωπικό Αριθμό. Συνεπώς, αποσαφηνίζουμε ότι η επαλήθευση της ταυτότητας θα πραγματοποιείται «με τον Προσωπικό Αριθμό και σύμφωνα με τις κατά νόμο διαδικασίες», αφού με την έκδοση του Προσωπικού Αριθμού, ο φορέας παροχής υπηρεσιών κοινωνικής ασφάλισης θα «ανοίγει» την καρτέλα / ιδιαίτερο αρχείο δεδομένων του φυσικού προσώπου, χωρίς να καταγράφει – αντιστοιχεί τον Προσωπικό Αριθμό, αλλά μόνο τον «εσωτερικό» αριθμό μητρώου ως ταυτότητα (ID) καρτέλας. Η «εσωτερική» αυτή αντιστοίχιση αυτή θα γίνεται μόνο στο Μητρώο Προσωπικού Αριθμού της ΓΓΠΣΔΔ, που θα παρέχει τις σχετικές υπηρεσίες επιβεβαίωσης της ταυτότητας (IDaaS) στους επιμέρους φορείς.

Κατόπιν των ανωτέρω, τα βασικά σημεία του Ελληνικού μοντέλου ως προς την αρχιτεκτονική του:

1. Η έκδοση Προσωπικού Αριθμού ως νέου συνόλου αριθμητικών ή αλφαριθμητικών χαρακτήρων χωρίς την ενσωμάτωση ή την κωδικοποίηση προσωπικών δεδομένων και ειδικότερα θα αποτελείται από ένα σύνολο χαρακτήρων το οποίο θα αποτελείται από 3 αλφαριθμητικά στοιχεία (με τα κοινά με το λατινικό αλφάβητο γράμματα και τους αριθμούς) και τον μέχρι σήμερα ονομαζόμενο ΑΦΜ .
2. Να παραμείνει ο ΑΦΜ ως αναγνωριστικός αριθμός που θα χρησιμοποιείται από τα φυσικά πρόσωπα για φορολογικούς σκοπούς.
3. Να αποσυνδεθεί η έκδοση ΑΦΜ από την απόδοση Π.Α., που θα είναι υποχρεωτική.
4. Να αποφευχθεί η δημόσια αναγραφή του ΠΑ σε φορολογικά παραστατικά και κάθε άλλη συναλλακτική συμπεριφορά του φυσικού προσώπου που ασκεί επιχειρηματική δραστηριότητα που απαιτεί την αναφορά σε ΑΦΜ / αριθμό ΦΠΑ

5. Κάθε άλλος αριθμός αναγνώρισης των φυσικών προσώπων να απορροφηθεί σταδιακά από τον Π.Α. σύμφωνα με τον ως άνω σχεδιασμό.

Με τον ενιαίο Προσωπικό Αριθμό πληρούνται:

- η αρχή του περιορισμού του σκοπού, καθώς επιτυγχάνεται ο ορθός σκοπός επεξεργασίας για το σύνολο του Προσωπικού Αριθμού ως ΔΠΧ ενώπιον του Δημοσίου και ο ορθός σκοπός αποκλειστικά για το σκέλος του ως ΔΠΧ, σε περίπτωση που το υποκείμενο έχει την ιδιότητα του αυτοαπασχολούμενου και έχει υποχρέωση δημοσιότητας (ανάρτησης) του σκέλους αυτού σε φορολογικά παραστατικά ή άλλες δημόσιες αναρτήσεις (VIES, Διαύγεια, κ.ο.κ).

- η αρχή της ελαχιστοποίησης των δεδομένων, αφού για τον ίδιο ως άνω λόγο η επεξεργασία περιορίζεται στο αναγκαίο.

Με την αρχιτεκτονική της προσθήκης τριών αλφαριθμητικών στοιχείων στον ΑΦΜ, ώστε να προκύπτει ότι ο Προσωπικός Αριθμός ικανοποιειούνται, μεταξύ άλλων, οι επιταγές της αρχής του περιορισμού του σκοπού, επιτυγχάνεται ο ορθός σκοπός επεξεργασίας για το σύνολο του Προσωπικού Αριθμού ως ΔΠΧ ενώπιον του Δημοσίου, και καλύπτεται ο ορθός σκοπός αποκλειστικά για το τμήμα του (ΑΦΜ) ως ΔΠΧ, σε περίπτωση που το υποκείμενο έχει την ιδιότητα του αυτοαπασχολούμενου και έχει υποχρέωση δημοσιότητας (ανάρτησης) του σκέλους αυτού σε φορολογικά παραστατικά ή άλλες δημόσιες αναρτήσεις (σύστημα VIES, Διαύγεια, κ.ο.κ). Παράλληλα, ικανοποιείται και η αρχή της ελαχιστοποίησης των δεδομένων, αφού για τον ίδιο ως άνω λόγο η επεξεργασία περιορίζεται μόνον στο αναγκαίο.

Ο Π.Α. καθιερώνεται ως ένας μοναδικός, για κάθε φυσικό πρόσωπο, αριθμός που αποτελείται από 12 αλφαριθμητικά στοιχεία, ήτοι 9 αριθμητικά και, μετά τις κατευθύνσεις της ΑΠΔΠΧ, 3 αλφαριθμητικά. Για κάθε ΑΦΜ οι πιθανοί συνδυασμοί των 3 αλφαριθμητικών στοιχείων είναι 243 = 13.284, ώστε για κάθε ΑΦΜ να αντιστοιχούν 13.284 πιθανοί Π.Α., γεγονός που διασφαλίζει την ασφάλεια του αριθμού. Ο Π.Α. χρησιμοποιείται πάντα σε συνδυασμό με την επίδειξη της ταυτότητας ή την χρήση ηλεκτρονικών κωδικών και παρέχει την ευχερέστερη επαλήθευση της ταυτότητας του εν λόγω φυσικού προσώπου στις συναλλαγές του με το Δημόσιο. Το φυσικό πρόσωπο μέσω του Π.Α. παρουσιάζεται με ένα «πρόσωπο» σε όλο το Δημόσιο και τους σχετικούς φορείς αποφεύγοντας τις πολλαπλές ταυτότητες και τυχόν ασυμφωνίες μεταξύ αυτών, με αποτέλεσμα η επίτευξη της βελτιστοποίησης της παροχής υπηρεσιών εκ μέρους του Δημοσίου. Ο συνδυασμός 12 αλφαριθμητικών ψηφίων αυξάνει κατά πολύ τους πιθανούς συνδυασμούς που μπορεί να προκύψουν, με αποτέλεσμα την αναλογική αύξηση της δυσκολίας παραβίασης του Π.Α. από τρίτους. Επίσης, η κεντρική τήρηση του Π.Α. σε ένα ασφαλές και κρυπτογραφημένο μητρώο αυξάνει την ευκολία προστασίας του, καθότι ένα μητρώο μπορεί να συγκεντρώσει με μεγαλύτερη ευκολία όλα τα μέσα αυτοπροστασίας του και κρυπτογράφησης, επιτυγχάνοντας οικονομίες κλίμακας σε αντιδιαστολή με ένα αποκεντρωμένο σύστημα πολλαπλών σημείων τήρησης.

δ. **Θεσμικό πλαίσιο για την έκδοση προεδρικού διατάγματος για τον Ενιαίο Προσωπικό Αριθμό**

Σύμφωνα με την **παρ. 5 του άρθρου 1 του ν. 4727/2020 (Α' 184)**, όπως προαναφέρθηκε, ορίζεται ότι «5. Ο Π.Α. χορηγείται στα φυσικά πρόσωπα σύμφωνα με τη διαδικασία και το χρονοδιάγραμμα που ορίζεται στο προεδ**ρικό διάταγμα που εκδίδεται σύμφωνα με την παρ. 6 του άρθρου 107**. Με την διαδικασία αυτή χορηγείται ο Π.Α. και σε όσα φυσικά πρόσωπα έχει χορηγηθεί Α.Φ.Μ. ή/και Α.Μ.Κ.Α.».

Περαιτέρω, με την **παρ. 6 του άρθρου 107 του ν. 4727/2020**, προβλέπεται ότι «6. Με προεδρικό διάταγμα που εκδίδεται ύστερα από πρόταση των Υπουργών Οικονομικών, Εργασίας και Κοινωνικών Υποθέσεων και Ψηφιακής Διακυβέρνησης και **ύστερα από γνωμοδότηση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα**, καθορίζονται τα μέτρα, οι εγγυήσεις και οι μηχανισμοί ασφαλείας για την πρόληψη και την αντιμετώπιση των κινδύνων για την προστασία των προσωπικών δεδομένων των φυσικών προσώπων, η διαδικασία χορήγησης του Προσωπικού Αριθμού, και ιδίως οι υπηρεσίες διεκπεραίωσης, τα απαιτούμενα δικαιολογητικά και οι υπηρεσίες ελέγχου αυτών, οι λόγοι αναστολής του, το χρονοδιάγραμμα που προβλέπεται στην παρ. 5 του άρθρου 11, η διαδικασία έκδοσης του Π.Α., οι όροι και η διαδικασία για την παροχή υπηρεσιών επαλήθευσης ταυτότητας των φυσικών προσώπων προς τους φορείς του δημόσιου τομέα και για την αντιστοίχιση των Π.Α. με τους αναγνωριστικούς αριθμούς των μητρώων (ειδικούς τομεακούς αριθμούς) των φορέων του δημόσιου τομέα, ιδίως Α.Φ.Μ. και Α.Μ.Κ.Α., τα ειδικότερα ζητήματα για την τήρηση του Μητρώου Προσωπικού Αριθμού, τα τεχνικά και οργανωτικά μέτρα που τηρεί η Γ.Γ.Π.Σ.Δ.Δ., τα τεχνικά και οργανωτικά μέτρα που τηρούν οι φορείς του δημοσίου τομέα που επεξεργάζονται τον Π.Α. μέσω του Κέντρου Διαλειτουργικότητας της Γ.Γ.Π.Σ.Δ.Δ., καθώς και κάθε τεχνική ή άλλη λεπτομέρεια για την εφαρμογή του άρθρου 11. Η Γ.Γ.Π.Σ.Δ.Δ. υποχρεούται να διενεργήσει πριν από την έκδοση του προεδρικού διατάγματος την εκτίμηση αντικτύπου της επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με τα οριζόμενα στον Γενικό Κανονισμό Προστασίας Δεδομένων.».

5.Συμπέρασμα – Αξιολόγηση της Αρχιτεκτονικής

Η απόδοση και χρήση του Π.Α. συνιστά μια μορφή παροχής υπηρεσίας αυθεντικοποίησης, αναλόγως με τις επιμέρους λειτουργίες, και όπως θα αναλυθεί κατωτέρω, δεν συνιστά όχημα διασύνδεσης δεδομένων διαφορετικών μητρώων ή δεδομένων διαφορετικών φορέων του Δημοσίου.

Ο φορέας τήρησης του Κεντρικού Αρχείου (Master Data File) (εν προκειμένω η ΓΓΠΣΔΔ) **θα λειτουργεί ως πάροχος υπηρεσιών ταυτοποίησης προς τους φορείς του Δημοσίου**, ώστε το φυσικό πρόσωπο που προσέρχεται σε μία Υπηρεσία για να πραγματοποιήσει συναλλαγές ή να χρησιμοποιήσει ηλεκτρονικές υπηρεσίες συναλλαγών, να ταυτοποιείται με τη βοήθεια του Π.Α. με τρόπο ακριβή, ασφαλή, γρήγορο και απλό. Ο Φορέας θα εξασφαλίσει τα κατάλληλα ανώτατου επιπέδου τεχνικά και οργανωτικά μέτρα για την προστασία του Κεντρικού Αρχείου και την ορθή λειτουργία του.

Οι επιμέρους φορείς του δημοσίου, λαμβάνοντας τις υπηρεσίες αυτές από την ΓΓΠΣΔΔ δεν θα διατηρούν – αποθηκεύουν – καταχωρούν τον Π.Α., ούτε θα έχουν γνώση ή πραγματική τεχνική δυνατότητα διασύνδεσης του Π.Α. με τα επιμέρους στοιχεία μητρώου που τηρούν.

Η σημαντική αυτή διαφοροποίηση της αρχιτεκτονικής του Π.Α. ως μία υπηρεσία ταυτοποίησης του φυσικού προσώπου, έρχεται σε πλήρη αντιδιαστολή με κάθε έννοια ευθείας ή έμμεσης ενοποίησης ή διασύνδεσης μητρώων και δεδομένων μητρώων, και ο

φορέας θα βεβαιώνεται με ασφάλεια, ταχύτητα και ακρίβεια για την ταυτότητα του συναλλασσόμενου φυσικού προσπώπου, ανεξαρτήτως του μέσου αλληλεπίδρασης (φυσική ή ηλεκτρονική συναλλαγή συναλλαγή).

IV. Οι προβληματισμοί σχετικά με την ψηφιακή ταυτότητα

1. e-ID - Ηλεκτρονική ταυτότητα και προστασία προσωπικών δεδομένων

Ένα βασικό ζήτημα που ανακύπτει με την υιοθέτηση και την εφαρμογή της ψηφιακής ταυτότητας σε εθνικό επίπεδο αφορά στην προστασία των δεδομένων προσωπικού χαρακτήρα, αφού εξ ορισμού μία ψηφιακή ταυτότητα εμπεριέχει ή διασυνδέεται με προσωπικά δεδομένα για τον προσδιορισμό της ταυτότητας ενός προσώπου.

Η χρήση των ηλεκτρονικών ταυτοτήτων, ως ένα εργαλείο ηλεκτρονικής διακυβέρνησης, εγείρει πολλές ανησυχίες για τα δικαιώματα και τις ελευθερίες των πολιτών αλλά και την ιδιωτικότητά τους. Μετά την αναφορά στις λειτουργίες των e-ID ταυτοτήτων, εξετάζονται οι ποιοτικές πτυχές των βιομετρικών χαρακτηριστικών ως ταυτοποιητικών στοιχείων. Παρουσιάζονται οι νομικές και θεσμικές ανησυχίες σε σχέση με τα δικαιώματα των ατόμων στην ιδιωτικότητα και την προστασία προσωπικών δεδομένων και **προτείνονται οι νομικές απαιτήσεις για την έκδοση των ηλεκτρονικών ταυτοτήτων σε συμμόρφωση με το Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων**.

Δεδομένης της ανακοίνωσης της δημιουργίας της ηλεκτρονικής ταυτότητας από την Ελληνική Κυβέρνηση, γίνεται μια επισκόπηση της ελληνικής περίπτωσης και προτείνουμε ένα νομικό πλαίσιο για την προστασία δεδομένων προσωπικού χαρακτήρα με αντίστοιχες σχετικές προβλέψεις του Συντάγματος.

2. e- ID: Εργαλείο για την ηλεκτρονική διακυβέρνηση και οφέλη

Η ηλεκτρονική ταυτότητα χρησιμοποιείται ως μια ένδειξη, ένα τεκμήριο για την ταυτοποίηση και την αυθεντικοποίηση ενός φυσικού προσώπου. Μια ηλεκτρονική ταυτότητα είναι βασικά μια έξυπνη κάρτα, η οποία αποτελείται κυρίως από ένα ορατό τομέα με προσωπικές πληροφορίες, όπως το όνομα του κατόχου, η ημερομηνία γέννησης, η διεύθυνση, η έκδοση της κάρτας και η ημερομηνία λήξης ισχύος της) και ένα μικροτσίπ με συνήθως επιπρόσθετες πληροφορίες που χρησιμοποιούνται ως ταυτοποιητικά στοιχεία του κατόχου της κάρτας και μπορεί να αναγνωσθούν, μέσω μιας συσκευής ανάγνωσης[49].

[49] Athina Antoniou & Lilian Mitrou. E-ID card & data protection: a path for good governance – a field of controversy

Η επικοινωνία της κάρτας και μιας εφαρμογής συνήθως λαμβάνει χώρα, μέσω μιας συσκευής ανάγνωσης κάρτας, που μπορεί να χρησιμοποιεί ηλεκτρικές επαφές και ένα ανέπαφο περιβάλλον ραδιοσυχνότητας (RF). Για την καθιέρωση ποιοτικών ηλεκτρονικών υπηρεσιών, το μικροτσίπ μιας ηλεκτρονικής κάρτας μπορεί να ενσωματώνει, επίσης, ψηφιακά πιστοποιητικά για ηλεκτρονική υπογραφή και ψηφιακή αυθεντικοποίηση για το νόμιμο κάτοχο, γεγονός που συμβάλλει στη διεξαγωγή πιο ασφαλών ηλεκτρονικών συναλλαγών.

3. Ηλεκτρονικές ταυτότητες και βιομετρικά στοιχεία

Οι ηλεκτρονικές ταυτότητες γίνονται αντιληπτές, σχεδιάζονται και εφαρμόζονται σε αυστηρή συνάρτηση με τη χρήση βιομετρικών. Με τον όρο **βιομετρικά στοιχεία** αναφερόμαστε σε μετρήσιμα βιολογικά χαρακτηριστικά του προσώπου, που μπορεί να χρησιμοποιηθούν για την αυτόματη αναγνώριση καθώς και σε μεθόδους αναγνώρισης ενός προσώπου, που βασίζονται στα χαρακτηριστικά αυτά. Η χρήση της ηλεκτρονικής ταυτότητας, περιλαμβάνει βιομετρικά χαρακτηριστικά ως αναγνωριστικά του προσώπου, προσφέρει μια πιο ακριβή ταυτοποίηση και πιο ασφαλή αυθεντικοποίηση του νόμιμου κατόχου της κάρτας[50], καθώς δεν βασίζεται σε κάτι που ο κάτοχος ήδη γνωρίζει, όπως ο αριθμός PIN, ή σχετικό με κάτι που κατέχει, αλλά σε αυτό που πραγματικά είναι. Επομένως, τα χαρακτηριστικά αυτά δεν μπορούν να ξεχαστούν ποτέ ή να χαθούν και είναι τα μοναδικά ταυτοποιητικά στοιχεία που επιτρέπουν την αρνητική αυθεντικοποίηση, δηλαδή μία σχεδόν απόλυτη απόδειξη ότι το άτομο είναι αυτό που λέει ότι είναι, ακόμη κι αν κατέχει ένα έγγραφο, που αποδεικνύει διαφορετικά.

Ωστόσο, δεν είναι όλα τα χαρακτηριστικά φυσιολογίας του ατόμου κατάλληλα ως ταυτοποιητικά, από τη στιγμή που απαιτείται να πληρούν συγκεκριμένες προϋποθέσεις και να ικανοποιούν συγκεκριμένα κριτήρια. Τα πιο κοινά βιομετρικά είναι τα δακτυλικά αποτυπώματα. Η ψηφιακή αναγνώριση του προσώπου χρησιμοποιείται, αλλά το πιο ακριβές και κατάλληλο στην περίπτωση του προσώπου είναι η ίριδα του ματιού. Ωστόσο, είναι σημαντικό να διευκρινιστεί ότι δεν είναι το βιομετρικό στοιχείο που αποθηκεύεται, αλλά ένα δείγμα αυτού, το οποίο συγκρατεί ένα μόνο μέρος της βιομετρικής πληροφορίας.

4. Ηλεκτρονική ταυτότητα και δικαίωμα ιδιωτικότητας του κατόχου

Ένα ζήτημα μείζονος σημασίας σχετικά με τις ηλεκτρονικές ταυτότητες είναι **η ιδιωτικότητα και το δικαίωμα του πληροφοριακού αυτοπροσδιορισμού του ατόμου, σύμφωνα με το άρθρο 9Α του Συντάγματος.** Το ερώτημα που έχουμε να απαντήσουμε είναι αν οι ηλεκτρονικές ταυτότητες και οι ψηφιακές κάρτες όντως αντιπροσωπεύουν μια πραγματική ανάμειξη στα δικαιώματα του κατόχου τους ή εάν η επεξεργασία τους και οι

[50] Athina Antoniou & Lilian Mitrou. E-ID card & data protection: a path for good governance – a field of controversy

συναφείς κίνδυνοι εξαρτώνται από τη φύση και τη χρήση των ταυτοποιητικών αυτών στοιχείων.

Η έκδοση των ηλεκτρονικών ταυτοτήτων που περιλαμβάνουν μοναδικά ταυτοποιητικά στοιχεία δίνει τη δυνατότητα και ενθαρρύνει μια ευρεία διασύνδεση των δεδομένων και των αρχείων. Ωστόσο, η πρόσβαση σε συγκεκριμένες πληροφορίες και η χρήση τους, μπορεί να είναι δικαιολογημένη και νόμιμη σε ορισμένες περιπτώσεις, ενώ αντίθετα η χωρίς διάκριση και έλεγχο πρόσβαση στα προσωπικά δεδομένα του ατόμου, οδηγεί στην αποκαλούμενη «διολίσθηση των λειτουργιών». Αυτό συνεπάγεται την παραβίαση του σκοπού συλλογής και επεξεργασίας των προσωπικών δεδομένων, ώστε ο κίνδυνος να γίνεται ακόμη πιο άμεσος για την ιδιωτικότητα του ατόμου.

Επίσης, ένας ορατός κίνδυνος είναι αυτός του «profiling». Με τη χρησιμοποίηση ενός μοναδικού ταυτοποιητικού στοιχείου για όλες τις κυβερνητικές βάσεις δεδομένων, που διατηρούνται ξεχωριστά, για διάφορους, αλλά και συγκεκριμένους σκοπούς, οι επιπλέον πληροφορίες σχετικά με το άτομο, μπορεί να διαδοθούν, παρά το γεγονός ότι το άτομο μπορεί να αποφασίζει σε ποιο βαθμό επιθυμεί να μοιράζεται τα προσωπικά του δεδομένα, όταν συμμετέχει σε διακριτούς τομείς της δημόσιας ζωής.

Υπάρχουν τρεις περιπτώσεις για την τοποθεσία αποθήκευσης των πληροφοριών:

1. Σε μία κεντρική βάση, στη μνήμη μιας κάρτας ανάγνωσης
2. Στην ηλεκτρονική κάρτα
3. Στο μικροτσίπ που ενσωματώνεται στην κάρτα.

Η απόφαση για το ποιά είναι η βέλτιστη λύση, είναι μεγάλης σημασίας, και συνήθως η απάντηση αναφέρεται στην αποθήκευση σε μία κεντρική βάση. Ωστόσο, **η αποθήκευση των δεδομένων σε μία κεντρική βάση**, σε σχέση με την αποθήκευση στο τσιπ της κάρτας, **εγκυμονεί κινδύνους, αφού απειλεί τα δικαιώματα του πολίτη, γεγονός που μπορεί να οδηγήσει σε κακόβουλες πρακτικές.**

5. Βιομετρικά δεδομένα και Ιδιωτικότητα

Η χρήση των βιομετρικών στοιχείων ως μοναδικών ταυτοποιητικών, μπορεί να εισάγει ακόμη περισσότερους κινδύνους ασφαλείας, από αυτούς που ίσως στοχεύει να μειώσει, αφού η χρήση βιομετρικών στοιχείων αποβλέπει καταρχάς στη διασφάλιση της επαλήθευσης του προσώπου που φέρει μία ψηφιακή ταυτότητα.

Η υπόθεση ενός δικηγόρου από το Oregon των Η.Π.Α.[51], ο οποίος κατά λάθος κατηγορήθηκε για την υποτιθέμενη εμπλοκή του σε ένα θανατηφόρο βομβαρδισμό είναι μια πραγματική απόδειξη ότι λάθη μπορεί να συμβούν και δικαιώματα να τεθούν υπό διακινδύνευση. Δεδομένου ότι η σύνδεση του κατόχου με την ταυτότητά του είναι μόνιμη

[51] Athina Antoniou & Lilian Mitrou. E-ID card & data protection: a path for good governance – a field of controversy

και το γεγονός ότι η ταυτότητα του περιέχει βιομετρικά στοιχεία , δημιουργεί την υποχρέωση τουκατόχου να πρέπει να αποδείξει ότι δεν είναι ο φορέας του βιομετρικού δεδομένου. Αυτό περιπλέκει τη νομική διαδικασία, από τη στιγμή που οδηγεί σε αναξιόπιστα αποτελέσματα, αλλά το πιο σημαντικό είναι, ότι η άσκηση των δικαιωμάτων του είναι εξαιρετικά δύσκολη.

Ακόμη, δεδομένου ότι υπάρχουν είδη βιομετρικών που η συλλογή τους δεν είναι καν σε γνώση μας, ένα τεχνικό σφάλμα, ένα πετυχημένος χάκερ ή απλώς ένα διαχειριστικό λάθος, εκθέτει χιλιάδες άτομα, σε κινδύνους μεγάλης σημασίας. Αυτό μπορεί, επομένως, να οδηγήσει σε ένα μεγάλο κενό εμπιστοσύνης μεταξύ κράτους και πολίτη.

6. Η ελληνική περίπτωση

Η Ελληνική Κυβέρνηση έχει ανακοινώσει κατά καιρούς τη θέσπιση των ηλεκτρονικών ταυτοτήτων, γνωστών ως **«Κάρτα του Πολίτη»,** ενώ πρόσφατα ανακοινώθηκε η **θεσμοθέτηση του Ενιαίου Προσωπικού Αριθμού**, προκειμένου να προωθηθεί η ασφαλής ηλεκτρονική διακυβέρνηση και η μείωση των διοικητικών εμποδίων και βαρών που απορρέουν από την περιορισμένη αξιοποίηση των ψηφιακών συναλλαγών. Στο σημείο αυτό αξίζει να θυμηθούμε και τον **Κανονισμό (ΕΕ) αριθ. 2019/1157** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Ιουνίου 2019, **για την ενίσχυση της ασφάλειας των δελτίων ταυτότητας των πολιτών της Ένωσης και των εγγράφων διαμονής που εκδίδονται για πολίτες της Ένωσης και τα μέλη των οικογενειών τους, που ασκούν το δικαίωμα ελεύθερης κυκλοφορίας** (ΕΕ L 188 της 12.7.2019).

Ουσιαστικά, η ηλεκτρονική ταυτότητα θα είχε **τριπλή χρήση, ήτοι ταυτότητα, ταξιδιωτικό έγγραφο και κάρτα πολίτη, ενώ θα είχε ενσωματωμένα δύο τσίπς, ένα ανέπαφο (RFID) για την ταυτοποίηση του προσώπου και ένα με επαφή για την κάρτα του πολίτη.**

Υπενθυμίζεται δε ότι η **έννοια της Κάρτας του Πολίτη** αναφέρθηκε, για πρώτη φορά, στην Ελλάδα στις 11-09-2010 στη Διεθνή Έκθεση Θεσσαλονίκης, πριν τη θέσπιση των κανόνων της Ε.Ε., ενώ και παλαιότερα, ήδη πριν το 2000 είχε εξαγγελθεί η έκδοση ηλεκτρονικών ταυτοτήτων.

Σύμφωνα με το **άρθρο 3 του Κανονισμού (ΕΕ) αριθ. 2019/1157,** προσδιορίζονται τα πρότυπα ασφαλείας, ο μορφότυπος και οι προδιαγραφές των δελτίων ταυτότητας. Συγκεκριμένα,

«**1.** Τα δελτία ταυτότητας που εκδίδονται από τα κράτη μέλη παράγονται σε **μορφότυπο ID-1 και περιέχουν μηχαναγνώσιμη ζώνη (MRZ). Τα εν λόγω δελτία ταυτότητας βασίζονται στις προδιαγραφές και τα ελάχιστα πρότυπα ασφαλείας που παρατίθενται στο έγγραφο ICAO 9303** και συμμορφώνονται με τις απαιτήσεις που

ορίζονται στα στοιχεία γ), δ), στ) και ζ) του Παραρτήματος του κανονισμού (ΕΚ) αριθ. 1030/2002, όπως έχει τροποποιηθεί με τον κανονισμό (ΕΕ) 2017/1954.

2. Τα στοιχεία δεδομένων που περιλαμβάνονται στα δελτία ταυτότητας **πληρούν τις προδιαγραφές που ορίζονται στο μέρος 5 του εγγράφου ICAO 9303.** Κατά παρέκκλιση από το πρώτο εδάφιο, ο αριθμός του εγγράφου μπορεί να εισαχθεί στη ζώνη Ι και ο προσδιορισμός του φύλου ενός προσώπου είναι προαιρετικός.

3. Το έγγραφο φέρει τον τίτλο («**Δελτίο ταυτότητας**») ή άλλον καθιερωμένο εθνικό προσδιορισμό στην επίσημη γλώσσα ή στις επίσημες γλώσσες του κράτους μέλους που το εκδίδει, και τις λέξεις «Δελτίο ταυτότητας» σε μία τουλάχιστον άλλη επίσημη γλώσσα των θεσμικών οργάνων της Ένωσης.

4. Το δελτίο ταυτότητας περιέχει, στην εμπρόσθια όψη, τον **διψήφιο κωδικό χώρας του κράτους μέλους που εκδίδει το δελτίο**, τυπωμένο αρνητικά μέσα σε ένα μπλε παραλληλόγραμμο και περιβαλλόμενο από δώδεκα κίτρινα αστέρια.

5. Τα δελτία ταυτότητας **περιλαμβάνουν μέσο αποθήκευσης υψηλής ασφάλειας το οποίο περιέχει βιομετρικά δεδομένα που συνίστανται σε εικόνα του προσώπου του κατόχου του δελτίου και δύο δακτυλικά αποτυπώματα σε ψηφιακούς μορφοτύπους**. Για τη λήψη των βιομετρικών αναγνωριστικών στοιχείων, τα κράτη μέλη εφαρμόζουν τις τεχνικές προδιαγραφές που θεσπίζονται με την εκτελεστική απόφαση C(2018)7767 της Επιτροπής (13).

6. Το μέσο αποθήκευσης διαθέτει επαρκή χωρητικότητα και ικανότητα προκειμένου να διασφαλίζεται η **ακεραιότητα, η γνησιότητα και η εμπιστευτικότητα των δεδομένων**. **Τα δεδομένα που αποθηκεύονται είναι προσβάσιμα χωρίς επαφή και ασφαλισμένα όπως προβλέπεται στην εκτελεστική απόφαση C(2018)7767.** Τα κράτη μέλη ανταλλάσσουν τις πληροφορίες που απαιτούνται για την εξακρίβωση της γνησιότητας του μέσου αποθήκευσης και για την πρόσβαση στα βιομετρικά δεδομένα που αναφέρονται στην παράγραφο 5 και την επαλήθευσή τους.

7. Τα παιδιά **κάτω των 12 ετών** μπορούν να απαλλαγούν από την υποχρέωση παροχής δακτυλικών αποτυπωμάτων. Τα παιδιά **κάτω των 6 ετών** απαλλάσσονται από την υποχρέωση παροχής δακτυλικών αποτυπωμάτων. Τα πρόσωπα που **αδυνατούν να δώσουν δακτυλικά αποτυπώματα** για σωματικούς λόγους απαλλάσσονται από την υποχρέωση παροχής δακτυλικών αποτυπωμάτων.

8. Όταν είναι αναγκαίο και αναλογικό προς τον επιδιωκόμενο στόχο, τα κράτη μέλη μπορούν να αναγράφουν προς εθνική χρήση στοιχεία και παρατηρήσεις, όπως απαιτείται σύμφωνα με το εθνικό δίκαιο. Τούτο δεν μειώνει την αποτελεσματικότητα των ελάχιστων προτύπων ασφαλείας και τη διασυνοριακή συμβατότητα των δελτίων ταυτότητας.

9. Αν τα κράτη μέλη ενσωματώνουν **διπλή διεπαφή ή ξεχωριστό μέσο αποθήκευσης στο δελτίο ταυτότητας**, το πρόσθετο μέσο αποθήκευσης συμμορφώνεται με τα σχετικά πρότυπα ISO και δεν επηρεάζει το μέσο αποθήκευσης που αναφέρεται στην παράγραφο 5.

10. Αν τα κράτη μέλη αποθηκεύουν στα δελτία ταυτότητας **δεδομένα για ηλεκτρονικές υπηρεσίες** όπως η **ηλεκτρονική διακυβέρνηση και οι ηλεκτρονικές επιχειρηματικές δραστηριότητες**, τα εν λόγω εθνικά δεδομένα πρέπει να είναι φυσικά ή λογικά διαχωρισμένα από τα βιομετρικά δεδομένα που αναφέρονται στην παράγραφο 5.

11. Αν τα κράτη μέλη προσθέσουν **πρόσθετα εθνικά χαρακτηριστικά ασφάλειας στα δελτία ταυτότητας**, η διασυνοριακή συμβατότητα των δελτίων ταυτότητας αυτών και η αποτελεσματικότητα των ελάχιστων προτύπων ασφάλειας δεν πρέπει να μειωθεί.».

Η **διάρκεια ισχύος των δελτίων αυτών ταυτότητας** ανέρχεται τουλάχιστον στα **5 έτη, με μέγιστη διάρκεια ισχύος 10 έτη** (παρ. 1 άρθρου 4 Κανονισμού). Επίσης, δελτία που δεν πληρούν τις προϋποθέσεις του άρθρου 3 του Κανονισμού **παύουν σταδιακά να ισχύουν από τη λήξη τους ή το αργότερο έως τις 3 Αυγούστου του 2031** (παρ. 1 άρθρου 5 Κανονισμού).

Στο **άρθρο 6 του Κανονισμού ορίζονται οι ελάχιστες πληροφορίες που πρέπει να αναφέρονται στα δελτία ταυτότητας**, ήτοι

«α) τον τίτλο του εγγράφου στην επίσημη γλώσσα ή στις επίσημες γλώσσες του κράτους μέλους που το εκδίδει και σε μία τουλάχιστον άλλη επίσημη γλώσσα των θεσμικών οργάνων της Ένωσης·

β) σαφή αναφορά ότι το έγγραφο εκδίδεται για πολίτη της Ένωσης σύμφωνα με την οδηγία 2004/38/ΕΚ·

γ) τον αριθμό του εγγράφου·

δ) το όνομα [επώνυμο και όνομα (-τα)] του κατόχου·

ε) την ημερομηνία γέννησης του κατόχου· στ) τις πληροφορίες που πρέπει να περιλαμβάνονται στις βεβαιώσεις εγγραφής και στα έγγραφα που πιστοποιούν τη μόνιμη διαμονή, τα οποία εκδίδονται σύμφωνα με τα άρθρα 8 και 19 της οδηγίας 2004/38/ΕΚ, αντίστοιχα·

ζ) την εκδούσα αρχή·

η) στην εμπρόσθια όψη, τον διψήφιο κωδικό χώρας του κράτους μέλους που εκδίδει το έγγραφο, τυπωμένο αρνητικά μέσα σε ένα μπλε παραλληλόγραμμο περιβαλλόμενο από δώδεκα κίτρινα αστέρια. Εάν ένα κράτος μέλος αποφασίσει να λάβει δακτυλικά αποτυπώματα, εφαρμόζεται το άρθρο 3 παράγραφος 7 αναλόγως. Τα πρόσωπα που αδυνατούν να δώσουν δακτυλικά αποτυπώματα για σωματικούς λόγους απαλλάσσονται από την υποχρέωση παροχής δακτυλικών αποτυπωμάτων.».

Στο **άρθρο 7 του Κανονισμού** προβλέπεται ενιαίος μορφότυπος για τα **δελτία διαμονής για μέλη της οικογένειας που δεν είναι υπήκοοι κράτους-μέλους**, ενώ **στο άρθρο 8 προβλέπεται η σταδιακή κατάργηση των υφιστάμενων δελτίων διαμονής**, είτε κατά τη λήξη τους είτε το αργότερο έως τις 3 Αυγούστου 2026.

Το **<u>άρθρο 10 του Κανονισμού</u>** αναφέρεται στη **συλλογή βιομετρικών αναγνωριστικών στοιχείων**, ορίζοντας ότι:

1. Η συλλογή βιομετρικών αναγνωριστικών στοιχείων διενεργείται **μόνον από ειδικευμένο και δεόντως εξουσιοδοτημένο προσωπικό,** το οποίο ορίζεται από τις αρχές που είναι αρμόδιες για την έκδοση δελτίων ταυτότητας ή δελτίων διαμονής, και με σκοπό την ενσωμάτωσή τους στο υψηλής ασφάλειας μέσο αποθήκευσης που προβλέπεται στο άρθρο 3 παράγραφος 5 για τα δελτία ταυτότητας και στο άρθρο 7 παράγραφος 1 για τα δελτία διαμονής. Κατά παρέκκλιση της πρώτης περιόδου, η λήψη δακτυλικών αποτυπωμάτων διενεργείται **αποκλειστικά από ειδικευμένο και δεόντως εξουσιοδοτημένο προσωπικό των εν λόγω αρχών**, με εξαίρεση την περίπτωση αιτήσεων που υποβάλλονται στις διπλωματικές και προξενικές αρχές του κράτους μέλους. Προκειμένου να διασφαλιστεί η συνοχή των βιομετρικών αναγνωριστικών στοιχείων με την ταυτότητα του αιτούντος, ο αιτών εμφανίζεται αυτοπροσώπως τουλάχιστον μία φορά κατά τη διαδικασία έκδοσης για κάθε αίτηση.

2. Τα κράτη μέλη εξασφαλίζουν ότι εφαρμόζονται κατάλληλες και αποτελεσματικές διαδικασίες συλλογής βιομετρικών αναγνωριστικών στοιχείων, και ότι οι διαδικασίες αυτές συνάδουν με τα δικαιώματα και τις αρχές που ορίζονται στον Χάρτη, στη Σύμβαση για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών, και στη Σύμβαση των Ηνωμένων Εθνών για τα δικαιώματα του παιδιού. Σε περίπτωση ανάκυψης δυσκολιών στη συλλογή των βιομετρικών αναγνωριστικών στοιχείων, **τα κράτη μέλη εξασφαλίζουν ότι εφαρμόζονται κατάλληλες διαδικασίες που διασφαλίζουν την προστασία της αξιοπρέπειας του ενδιαφερομένου.**

3. Εκτός εάν απαιτείται με σκοπό την επεξεργασία σύμφωνα με το ενωσιακό και το εθνικό δίκαιο, τα βιομετρικά αναγνωριστικά στοιχεία που αποθηκεύονται με σκοπό την εξατομίκευση των δελτίων ταυτότητας ή των εγγράφων διαμονής **φυλάσσονται με τρόπο υψηλής ασφάλειας και μόνον έως την ημερομηνία παραλαβής του εγγράφου** και σε κάθε περίπτωση, **όχι για περίοδο μεγαλύτερη από 90 ημέρες από την ημερομηνία έκδοσης του εν λόγω εγγράφου**. Μετά την παρέλευση της περιόδου αυτής, τα εν λόγω βιομετρικά αναγνωριστικά στοιχεία διαγράφονται αμέσως ή καταστρέφονται.».

Περαιτέρω, στο **άρθρο 11 του Κανονισμού προβλέπεται η προστασία των δεδομένων προσωπικού χαρακτήρα** και ορίζεται ότι:

«1. Κ**ατά παρέκκλιση του κανονισμού (ΕΕ) 2016/679**, τα κράτη μέλη μεριμνούν για την **ασφάλεια, την αξιοπιστία, τη γνησιότητα και την εμπιστευτικότητα των δεδομένων π**ου συλλέγονται και αποθηκεύονται για τον σκοπό του παρόντος κανονισμού.

2. Για τον σκοπό του παρόντος κανονισμού, οι **αρχές που είναι αρμόδιες για την έκδοση δελτίων ταυτότητας και εγγράφων διαμονής** θεωρούνται οι **υπεύθυνες επεξεργασίας** κατά την έννοια του άρθρου 4 παράγραφος 7 του κανονισμού (ΕΕ) 2016/679 και είναι υπεύθυνες για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

3. Τα κράτη μέλη εξασφαλίζουν ότι οι εποπτικές αρχές μπορούν να ασκούν πλήρως τα καθήκοντά τους όπως αναφέρονται στον κανονισμό (ΕΕ) 2016/679, συμπεριλαμβανομένης

της **πρόσβασης σε όλα τα δεδομένα προσωπικού χαρακτήρα και σε όλες τις αναγκαίες πληροφορίες, καθώς και της πρόσβασης σε κάθε χώρο ή εξοπλισμό επεξεργασίας δεδομένων των αρμόδιων αρχών**.

4. Η συνεργασία με εξωτερικούς παρόχους υπηρεσιών δεν αποκλείει καμία ευθύνη στο μέρος του κράτους μέλους που μπορεί που απορρέει από το ενωσιακό ή το εθνικό δίκαιο για παραβάσεις υποχρεώσεων που αφορούν δεδομένα προσωπικού χαρακτήρα.

5. Πληροφορίες σε μηχαναγνώσιμη μορφή περιλαμβάνονται σε δελτίο ταυτότητας ή σε έγγραφο διαμονής μόνο σύμφωνα με τον παρόντα κανονισμό και με το εθνικό δίκαιο του κράτους μέλους έκδοσης.

6. Τα βιομετρικά δεδομένα που αποθηκεύονται στο μέσο αποθήκευσης των δελτίων ταυτότητας και των εγγράφων διαμονής χρησιμοποιούνται μόνο σύμφωνα με το ενωσιακό και το εθνικό δίκαιο, από δεόντως εξουσιοδοτημένο προσωπικό των αρμόδιων εθνικών αρχών και οργανισμών της Ένωσης, με σκοπό την εξακρίβωση: α) της γνησιότητας του δελτίου ταυτότητας ή του εγγράφου διαμονής, β) της ταυτότητας του κατόχου μέσω άμεσα διαθέσιμων συγκρίσιμων χαρακτηριστικών στις περιπτώσεις που είναι υποχρεωτική διά νόμου η επίδειξη δελτίου ταυτότητας ή εγγράφου διαμονής.

7. Τα κράτη μέλη τηρούν, και διαβιβάζουν ετησίως τον εν λόγω κατάλογο στην Επιτροπή, κατάλογο των αρμόδιων αρχών που έχουν πρόσβαση στα βιομετρικά δεδομένα τα οποία είναι αποθηκευμένα στο μέσο αποθήκευσης που αναφέρεται στο άρθρο 3 παράγραφος 5 του παρόντος κανονισμού. Η Επιτροπή δημοσιεύει στο διαδίκτυο συγκεντρωτικό πίνακα των εν λόγω εθνικών καταλόγων.».

Περαιτέρω, το **άρθρο 14 του Κανονισμού** προβλέπει πρόσθετες τεχνικές προδιαγραφές, ως εξής:

«1. Προκειμένου να εξασφαλιστεί, κατά περίπτωση, ότι τα δελτία ταυτότητας και τα έγγραφα διαμονής που αναφέρονται στο άρθρο 2 στοιχεία α) και γ) συμμορφώνονται με τα μελλοντικά ελάχιστα πρότυπα ασφάλειας, η Επιτροπή θεσπίζει, μέσω εκτελεστικών πράξεων, πρόσθετες τεχνικές προδιαγραφές όσον αφορά τα ακόλουθα: **α)** πρόσθετα χαρακτηριστικά και απαιτήσεις ασφάλειας, συμπεριλαμβανομένων ενισχυμένων προτύπων για την καταπολέμηση της πλαστογράφησης, απομίμησης και παραποίησης· **β)** τεχνικές προδιαγραφές για το μέσο αποθήκευσης των βιομετρικών στοιχείων που αναφέρονται στο άρθρο 3 παράγραφος 5 και τη διασφάλισή τους, συμπεριλαμβανομένων της αποτροπής μη εξουσιοδοτημένης πρόσβασης και της διευκόλυνσης του ελέγχου εγκυρότητας· **γ)** απαιτήσεις για την ποιότητα και τα κοινά τεχνικά πρότυπα όσον αφορά την εικόνα προσώπου και τα δακτυλικά αποτυπώματα. […].».

Τέλος, με το **άρθρο 16 του Κανονισμού** ορίζεται η έναρξη εφαρμογής του, από 2 Αυγούστου 2021.

Ασφαλώς, υπενθυμίζεται ότι στο ελληνικό θεσμικό πλαίσιο συμπεριλαμβάνεται και ο **ν. 4624/2019** «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ)2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προ-στασία των φυσικών προσώπων έναντι της επεξεργασίας

δεδομένων προσωπικού χαρακτή-ρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου2016 και άλλες διατάξεις.» (Α' 137).

Η απάντηση στο εάν η έκδοση της ηλεκτρονικής ταυτότητας μπορεί να είναι σύμφωνη με την προστασία δεδομένων προσωπικού χαρακτήρα δεν είναι ούτε αρνητική, ούτε θετική εκ των προτέρων. Πράγματι, η απάντηση εξαρτάται από το πλαίσιο που επιλέγουμε να εφαρμόσουμε και στα μέσα που χρησιμοποιούμεκαθώς και στις διαδικασίες και τις εγγυήσεις, προκειμένου να διασφαλιστούν τα δικαιώματα των πολιτών. Η χρήση πολλών, και ειδικών τομεακών αναγνωριστικών ως ηλεκτρονικές ταυτότητες δεδομένου ότι αποτελούν χαρακτηριστικό γνώρισμα της ιδιωτικότητας, αναδεικνύουν την απαίτηση για αυστηρή εφαρμογή της αρχής της αναλογικότητας,έναντι στην διευρυμένη συλλογή δεδομένων με την επιπρόσθετη απαίτηση της συγκεκριμενοποίησης των σκοπών συλλογής δεδομένων, σε ένα σταθερό και προσβάσιμο νομικό περιβάλλον. Έτσι ώστε να εκληφθούν ως παράγοντες-κλειδιά και να αντιμετωπιστούν οι κίνδυνοι που αφορούν στην ιδιωτικότητα οι οποίοι ελλοχεύουν στο περιβάλλον λειτουργίας και έκδοσης των ηλεκτρονικών καρτών.

7. Ψηφιακή ταυτότητα και δημόσια διοίκηση

Ένα καίριο ζήτημα αφορά στα χαρακτηριστικά της νέας δημόσιας διοίκησης και του τρόπου που πρέπει εκείνη να ανταποκριθεί εγκαίρως και αποτελεσματικά στις μελλοντικές ανάγκες και προσδοκίες των πολιτών.[52] Σήμερα, **η δημόσια διοίκηση έχει να αντιμετωπίσει τις προκλήσεις της διακυβέρνησης της ψηφιακής εποχής που διακρίνεται από την ανάγκη αξιοποίησης της τεχνολογίας**, για την επανένταξη των δημοσίων υπηρεσιών στο νέο περιβάλλον διεθνούς ανταγωνισμού, τον σχεδιασμό υπηρεσιών βάσει των αναγκών των πολιτών και την παροχή ψηφιακών υπηρεσιών στους πολίτες on-line.

Με τον τρόπο αυτό, επιτυγχάνεται η «**αποδιαμεσολάβηση**» μεταξύ κράτους και πολίτη, αφού επέρχεται η αλληλεπίδραση και η σύνδεση τους, μέσω του Διαδικτύου, που συμβάλει στη μείωση της πολυπλοκότητας του θεσμικού πλαισίου που αντιμετωπίζουν οι πολίτες στην προσπάθεια πρόσβασης στις δημόσιες υπηρεσίες. Το γεγονός αυτό γίνεται εφικτό με την αξιοποίηση της **τεχνολογίας** και την **παροχή ψηφιακών υπηρεσιών** στους πολίτες, ενθαρρύνοντας έτσι τις ψηφιακές συναλλαγές μαζί τους, ιδιαίτερα στην εποχή ανάπτυξης του Διαδικτύου, που απαιτεί την προσαρμογή και τον εκσυγχρονισμό της δημόσιας διοίκησης για την απόκτηση ανταγωνιστικότητας σε παγκόσμιο επίπεδο.

[52] Patrick Dunleavy. The Future Joined-up Public Services. 2020 Public Services Trust at the RSA.

Είναι δε χαρακτηριστικό ότι **η σύγχρονη δημόσια διοίκηση καλείται να συλλέξει, να συστηματοποιήσει και να αναλύσει σε πραγματικό χρόνο, με ολοένα και πιο εξελιγμένους τρόπους, σειρά δεδομένων των πολιτών κατά την άσκηση του έργου της**. Παράλληλα, παρατηρείται μία ισχυρή αποσυγκέντρωση των βάσεων δεδομένων λόγω των νέων Τ.Π.Ε., ώστε να παρέχεται πρόσβαση σε περισσότερες πληροφορίες. Αυτή η αποσυγκέντρωση οδηγεί σε διάσπαση μεγάλων γραφειοκρατικών διαδικασιών σε επιμέρους φορείς, είτε του δημόσιου είτε του ιδιωτικού τομέα, λ.χ. λόγω εξωτερικής ανάθεσης, στρατηγικής αναθεώρησης της δημόσιας διοίκησης, απορρύθμισης, κ.ο.κ. Άλλωστε, συχνά υπάρχουν κίνητρα που ενθαρρύνουν τους φορείς να κάνουν βέλτιστη χρήση των πόρων τους, μέσω ιδιωτικοποιήσεων ή Συμπράξεων Δημοσίου και Ιδιωτικού Τομέα, με αποτέλεσμα τα δεδομένα του πολίτη να διαχέονται εκτός του σκληρού πυρήνα της δημόσιας διοίκησης.

Παρατηρείται όμως και μία **αντίστροφη πορεία επανένταξης** από πλευράς δημόσιας διοίκησης, η οποία αποβλέπει στη συνένωση και επανασυγκέντρωση εκ νέου των διαδικασιών στην ίδια, με «**επαναδιακυβέρνηση**», ιδίως για ζητήματα που από τη φύση τους πρέπει να χειριστεί το κράτος. Η τάση αυτή εντοπίζεται, **με τη δημιουργία νέων κεντρικών κυβερνητικών διαδικασιών, κυρίως με διαδικασίες μίας στάσης**, με στόχο την **απλοποίηση της οργάνωσης των δημοσίων υπηρεσιών**. Επίσης, προτεραιότητα και **σημείο αναφοράς στις διεργασίες αυτές αποκτά ο πολίτης-πελάτης**, γεγονός που οδηγεί σε **ευέλικτες κυβερνητικές δομές και επανασχεδιασμό διοικητικών διαδικασιών για τη βέλτιστη εξυπηρέτηση του πολίτη σε πραγματικό χρόνο**. Κεντρικό ρόλο στον ως άνω επανασχεδιασμό επιτελεί η ψηφιοποίηση διαδικασιών, λ.χ. για την υιοθέτηση κεντρικών διαδικτυακών προμηθειών, νέες μορφές αυτοματισμού, κ.λ.π. που για παράδειγμα δεν απαιτούν ανθρώπινη παρέμβαση («τεχνολογίες μηδενικής αφής») ή οδηγούν σε συμπαραγωγή δημοσίων υπηρεσιών με την ενεργό συμμετοχή των πολιτών, ιδίως σε τοπικό επίπεδο.

8. Συμπεράσματα - Προτάσεις για την ασφαλή υιοθέτηση Ενιαίου Προσωπικού Αριθμού στην Ελλάδα

Η **ενιαία ταυτοποίηση εμφανίζεται σε πλήθος χωρών εντός της Ευρωπαϊκής Ένωσης**, όπως στην Αυστρία, την Ισπανία, το Βέλγιο, τη Βουλγαρία, τη Δανία, την Εσθονία, τη Φιλανδία, τη Λιθουανία, την Πολωνία, τη Σουηδία, ενώ **χαρακτηριστικό παράδειγμα αποτελεί η Ολλανδία.**

Βασικές δε παράμετροι για την προώθηση του εν λόγω προεδρικού διατάγματος αποτέλεσαν, εκτός από τη θεσμική υποχρέωση της Χώρας για ρύθμιση του ζητήματος βάσει του άρθρου 11 του ν. 4727/2020 (Α' 184), η συγκριτική μελέτη των ισχυουσών ρυθμίσεων σε επίπεδο κρατών-μελών της Ευρωπαϊκής Ένωσης καθώς και η ανάγκη θεσμοθέτησης ενός πλαισίου εναρμονισμένου με την πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την τροποποίηση του Κανονισμού (ΕΕ) αριθ. 910/2014, όσον αφορά τη θέσπιση πλαισίου για την ευρωπαϊκή ψηφιακή ταυτότητα.

.

Στη Χώρα μας το μοντέλο που κυριαρχεί όπως προαναφέρθηκε είναι το **μοντέλο της αποκεντροποιημένης ταυτοποίησης**. Δηλαδή, ένα φυσικό πρόσωπο συνάπτει σχέσεις εμπιστοσύνης απευθείας με τον πάροχο υπηρεσιών και ταυτοποιείται απευθείας σε αυτόν (π.χ. Φορολογική Διοίκηση και Α.Φ.Μ., Υπηρεσίες Κοινωνικής Ασφάλισης και Α.Μ.Κ.Α., Υπηρεσίες Ασφάλειας και Α.Δ.Τ., κ.ο.κ.). **Άμεση απόρροια του μοντέλου της αποκεντροποιημένης ταυτοποίησης αποτελεί η δημιουργία και διατήρηση πολλών και ανεπαρκώς συνδεδεμένων - μη διαλειτουργικών μητρώων, στα οποία πολλές φορές τηρούνται στοιχεία για τις ίδιες οντότητες, ενώ σε αρκετές περιπτώσεις τα στοιχεία αυτά δεν συμπίπτουν είτε λόγω μη επικαιροποίησης τους είτε λόγω μη σωστής ή πλημμελούς διαδικασίας αρχικής εισαγωγής τους**.

Η σημερινή κατάσταση, όπως περιγράφεται, έχει ως συνέπειες, μεταξύ άλλων, **ένα φυσικό πρόσωπο να «εμφανίζεται με πολλά πρόσωπα» έναντι του Δημοσίου και το Δημόσιο να «εμφανίζεται με πολλά πρόσωπα» έναντι του φυσικού προσώπου**. **Με τη χρήση του Προσωπικού Αριθμού, απλουστεύεται η ζωή του πολίτη, ο οποίος δεν θα έχει πλέον την υποχρέωση απομνημόνευσης πολλών αριθμών ταυτοποίησης και διατήρησης αντίστοιχων πιστοποιητικών.**

Παράλληλα, με τον Προσωπικό Αριθμό, αποφεύγονται καταστάσεις που ταλαιπωρούν τον πολίτη και διαρρηγνύουν τη σχέση εμπιστοσύνης του πολίτη με το κράτος, όπως, επί παραδείγματι, φαινόμενα καταβολής αχρεωστήτως καταβληθέντων ή η δυσχερής ικανοποίηση δικαιωμάτων των πραγματικών δικαιούχων, λόγω αδυναμίας διασταύρωσης των επιμέρους και αποσπασματικών πληροφοριών που αφορούν στον πολίτη. Λόγω του κατακερματισμένου τρόπου διατήρησης στοιχείων που αφορούν τον πολίτη σε διακριτού δημόσιους μηχανισμούς στο πλαίσιο του αποκεντρωμένου συστήματος ταυτοποίησης[53].

Επομένως, **περιορίζεται σημαντικά η ύπαρξη διπλοεγγραφών στα διάφορα μητρώα του Δημοσίου**. **Απώτερος δε στόχος είναι η πλήρης εξάλειψη των διπλοεγγραφών και η διόρθωση σφαλμάτων στις εγγραφές** (αναγραμματισμοί, ορθογραφικά λάθη σε ονοματεπώνυμα, κ.λπ.), που πλήττουν το κύρος της ακρίβειας των δεδομένων των φυσικών προσώπων και το βαθμό αξιοπιστίας του Δημοσίου, επιφέροντας έτσι έλλειψη εμπιστοσύνης στις ηλεκτρονικές συναλλαγές με το Δημόσιο.

Εν συνεχεία, η θέσπιση του Ενιαίου Προσωπικού Αριθμού συμβάλλει στην τήρηση των κανόνων της ενωσιακής και εθνικής νομοθεσίας αναφορικά με την προστασία των δεδομένων προσωπικού χαρακτήρα. **Ειδικότερα, οι αρχές της ελαχιστοποίησης, της ακρίβειας και της τήρησης του συγκεκριμένου κάθε φορά σκοπού επεξεργασίας εφαρμόζονται βάσει του Κανονισμού (ΕΕ) αριθ. 679/2016**.

[53] Élise Debiès, Renforcement des droit des individus sur leurs données personnelles: Quelles conséquences sur l'utilisation du numéro d' inscription au repertoire national d' identification des personnes physiques (NIR), EN3S-École nationale supérieure de Sécurité sociale, pages 149 à 155.

Χαρακτηριστικό παράδειγμα για τα πλεονεκτήματα του Προσωπικού Αριθμού είναι το ακόλουθο: Στην παρούσα κατάσταση χρησιμοποιούνται οι κωδικοί Taxisnet για τη σύνδεση στις ηλεκτρονικές υπηρεσίες Ενιαίου Φορέα Κοινωνικής Ασφάλισης (Ε.Φ.Κ.Α.). Το αποτέλεσμα είναι ο ήδη υφιστάμενος αυτόματος συσχετισμός Αριθμού Φορολογικού Μητρώου (Α.Φ.Μ.) και Αριθμού Μητρώου Κοινωνικής Ασφάλισης (Α.Μ.Κ.Α.) στο φορέα να διαιωνίζει τις εσφαλμένες εγγραφές (ορθογραφικά, διπλοεγγραφές λάθος πατρώνυμο ή μητρώνυμο) στα επιμέρους μητρώα, για το ίδιο πρόσωπο. Αυτό συμβαίνει, διότι διασυνδέονται διαφορετικοί αριθμοί, για να επιτευχθεί η επαλήθευση της ταυτότητας του φυσικού προσώπου.

Με τη χρήση του Προσωπικού Αριθμού, αυτό δεν θα είναι, πλέον, απαραίτητο, αφού αυτή την υπηρεσία θα την παρέχει με ασφαλή - μη φανερό - τρόπο το Μητρώο Προσωπικού Αριθμού. **Ακόμη, λοιπόν, κι αν τα στοιχεία του φυσικού προσώπου στο σώμα ενός εγγράφου είναι εσφαλμένα σε σχέση με τα στοιχεία στο σώμα άλλου εγγράφου** (π.χ. ορθογραφικό λάθος σε επώνυμο), **η αναφορά θα γίνεται σε συνάρτηση με τα τηρούμενα δεδομένα της Γενικής Γραμματείας Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης (Γ.Γ.Π.Σ.Δ.Δ.)**[54].

Δεδομένου όλων των παραπάνω, διαπιστώνουμε ότι **οι πολίτες έχουν τον έλεγχο των προσωπικών τους δεδομένων, ικανοποιώντας κατ' αυτόν τον τρόπο το δικαίωμα του πληροφοριακού αυτοκαθορισμού** (**άρθρο 9Α του Συντάγματος**), αφού θα είναι πλέον σε θέση να γνωρίζουν ποια προσωπικά τους δεδομένα, από ποιόν οργανισμό και για ποιο σκοπό τυγχάνουν επεξεργασίας.

Το **δικαίωμα στη χρήστη διοίκηση**, όπως ορίζεται στο **άρθρο 41 του Χάρτη Θεμελιωδών Δικαιωμάτων** αναφέρεται στην υποχρέωση της Διοίκησης να δρα αμερόληπτα, δίκαια και εντός εύλογου χρόνου. Αυτό συνεπάγεται δίχως άλλο, την κατάρριψη/απομείωση των διοικητικών εμποδίων που δεν είναι αναγκαία για τη λειτουργία της και την αλληλεπίδραση με τους πολίτες[55]. **Η θέσπιση του Ενιαίου Προσωπικού Αριθμού συμβάλλει αναμφίβολα και στην τήρηση της συνταγματικά κατοχυρωμένης αρχής της αναλογικότητας, καθώς και στην εφαρμογή της αρχής «μόνον άπαξ»** (παρ. 1 του άρθρου 3 του ν. 4727/2020, Α' 184), υπό την έννοια ότι, η **δράση της Διοίκησης διέπεται από τη μία πλευρά από την απαιτούμενη διαφάνεια και την εντός εύλογου χρόνου εξέταση των υποθέσεων των πολιτών**, ενώ από την άλλη πλευρά, η **λειτουργία των διοικητικών υπηρεσιών και του ευρύτερου δημόσιου τομέα γίνεται πιο αποτελεσματική και χαρακτηρίζεται από συνέχεια (αρχή της συνέχειας της Δημόσιας Διοίκησης).**

[54] Η Γενική Γραμματεία Πληροφοριακών Συστημάτων, όπως αυτή οργανώθηκε με τα άρθρα 19 έως 28 του π.δ. 142/2017 (Α΄ 181), μεταφέρθηκε από το Υπουργείο Οικονομικών στο Υπουργείο Ψηφιακής Διακυβέρνησης με το π.δ. 81/2019 (Α΄ 119) και μετονομάστηκε σε Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης. Με το ν. 4623/2019 (Α' 134) έγινε η διάρθρωση της Γ.Γ.Π.Σ.Δ.Δ. και με το άρθρο 51 του ν. 4635/2019 (Α' 167) η αναδιάρθρωση της.

[55] Robert Krimmer Andriana Prentza Szymon Mamrot , The Once-Only Principle, The Toop Project, 2021. Springer, p. 106.

Η **θέσπιση του Προσωπικού αριθμού εναρμονίζεται με την πρόβλεψη του άρθρου 87 του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων** βάσει της οποίας, τα «**κράτη μέλη μπορούν να καθορίζουν περαιτέρω τις ειδικές προϋποθέσεις για την επεξεργασία εθνικού αριθμού ταυτότητας ή άλλου αναγνωριστικού στοιχείου ταυτότητας γενικής εφαρμογής**. **Στην περίπτωση αυτή, ο εθνικός αριθμός ταυτότητας ή οποιοδήποτε άλλο αναγνωριστικό στοιχείο ταυτότητας γενικής εφαρμογής χρησιμοποιείται μόνο με τις δέουσες εγγυήσεις για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων δυνάμει του παρόντος κανονισμού.**». Η διάταξη αυτή **παρέχει τη δυνατότητα εισαγωγής ενός** «**αναγνωριστικού στοιχείου ταυτότητας γενικής εφαρμογής**», ευχέρεια την οποία το Υπουργείο Ψηφιακής Διακυβέρνησης αξιοποιεί, με τη θέσπιση του Ενιαίου Προσωπικού Αριθμού ή Προσωπικού Αριθμού.

Το Μητρώο Προσωπικού Αριθμού οφείλει να περιλαμβάνει, σύμφωνα με την **αρχή της αναγκαιότητας**, **τα στοιχεία που είναι απολύτως αναγκαία για την επαλήθευση της ταυτότητας του φυσικού προσώπου, ήτοι όνομα, επώνυμο, πατρώνυμο, μητρώνυμο, ημερομηνία γέννησης, τόπο γέννησης, Αριθμό Δελτίου Ταυτότητας, Α.Μ.Κ.Α. και Α.Φ.Μ.** Η τήρηση των δεδομένων του Μητρώου Προσωπικού Αριθμού λαμβάνει χώρα, ακόμα και ύστερα από την απενεργοποίηση του Προσωπικού Αριθμού για τους λόγους που προβλέπονται στην παρ. 1, στο πλαίσιο εκπλήρωσης καθήκοντος που εκτελείται προς το δημόσιο συμφέρον και κατά την άσκηση της ειδικής δημόσιας εξουσίας τήρησης του Μητρώου Προσωπικού Αριθμού, που έχει ανατεθεί στον Υπεύθυνο Επεξεργασίας και υπό τους όρους που προβλέπονται στον Γενικό Κανονισμό για την Προστασία Δεδομένων και την εθνική νομοθεσία.

Καταληκτικά, ως προς τα ζητήματα ασφάλειας των προσωπικών δεδομένων υπογραμμίζεται ότι **το φυσικό πρόσωπο μέσω του Προσωπικού Αριθμού παρουσιάζεται με ένα «πρόσωπο» σε όλο το Δημόσιο και τους σχετικούς φορείς**, **αποφεύγοντας τις πολλαπλές ταυτότητες και τυχόν ασυμφωνίες μεταξύ αυτών**, **με αποτέλεσμα τη βελτιστοποίηση της παροχής υπηρεσιών εκ μέρους του Δημοσίου**.

Ο συνδυασμός 12 αλφαριθμητικών ψηφίων αυξάνει κατά πολύ τους πιθανούς συνδυασμούς που μπορεί να προκύψουν, με αποτέλεσμα την αναλογική αύξηση της δυσκολίας παραβίασης του Προσωπικού Αριθμού από τρίτους. Επίσης, η **κεντρική τήρηση του Προσωπικού Αριθμού σε ένα ασφαλές και κρυπτογραφημένο μητρώο** αυξάνει την ευκολία προστασίας του, καθότι ένα μητρώο μπορεί να συγκεντρώσει με μεγαλύτερη ευκολία όλα τα **μέσα αυτοπροστασίας και κρυπτογράφησης του**, επιτυγχάνοντας έτσι **οικονομίες κλίμακας, σε αντιδιαστολή με ένα αποκεντρωμένο σύστημα.**

Υπάρχει αυξημένη ζήτηση για λύσεις ηλεκτρονικής ταυτότητας που μπορεί να προσφέρουν δυνατότητες ασφαλών ψηφιακών συναλλαγών, παρέχοντας οφέλη αποδοτικότητας και υψηλό επίπεδο εμπιστοσύνης σε ολόκληρη την Ε.Ε., τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα, με βάση την ανάγκη για ταυτοποίηση και επαλήθευση της ταυτότητας των χρηστών με υψηλό επίπεδο διασφάλισης.

Σε εναρμόνιση με την Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την τροποποίηση του Κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά (eIDAS) και τον Κανονισμό για ΓΚΠΔ, στόχος είναι η εξασφάλιση, με δυνατότητα διασυνοριακής χρήσης, των κάτωθι:

- Πρόσβαση σε εξαιρετικά ασφαλείς και αξιόπιστες λύσεις ηλεκτρονικής ταυτότητας.
- Δυνατότητα των δημόσιων και ιδιωτικών υπηρεσιών να βασίζονται σε αξιόπιστες και ασφαλείς λύσεις ψηφιακής ταυτότητας.
- Δυνατότητας των φυσικών και νομικών προσώπων να χρησιμοποιούν λύσεις ψηφιακής ταυτότητας.
- Ανάδειξη λύσεων που επιτρέπουν στη στοχευμένη κοινοχρησία δεδομένων ταυτότητας που περιορίζονται στις ανάγκες της συγκεκριμένης υπηρεσίας που ζητείται κάθε φορά (**αρχή της αναγκαιότητας**).
- Αποδοχή συγκεκριμένων υπηρεσιών εμπιστοσύνης στην Ε.Ε. και ισότιμων τρόπων παροχής τους.

Από την **αξιολόγηση του Κανονισμού eIDAS κατέστη φανερό ότι ο τελευταίος δεν ανταποκρίνεται στις απαιτήσεις της σύγχρονης εποχής και της αγοράς**. Το γεγονός αυτό προκύπτει λόγω των εγγενών περιορισμών του στο δημόσιο τομέα, των περιορισμένων του δυνατοτήτων και της πολυπλοκότητας που χαρακτηρίζει τους ιδιωτικούς παρόχους επιγραμματικών υπηρεσιών για τη σύνδεσή τους στο σύστημα ταυτοποίησης, της ανεπάρκειας κοινοποίησης λύσεων ηλεκτρονικής ταυτοποίησης στο σύνολο των κρατών-μελών της Ε.Ε. και της έλλειψης ευελιξίας του.

Επιπλέον, οι **λύσεις ταυτότητας που δεν εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού eIDAS, όπως αυτές προσφέρονται από παρόχους μέσων κοινωνικής δικτύωσης και χρηματοπιστωτικά ιδρύματα, εγείρουν ανησυχίες όσον αφορά στην προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων.** Δεν μπορούν να ανταποκριθούν αποτελεσματικά στις νέες απαιτήσεις της αγοράς και δεν διαθέτουν διασυνοριακή προσέγγιση για την αντιμετώπιση ειδικών τομεακών αναγκών όπου η ταυτοποίηση είναι ευαίσθητη και απαιτεί υψηλό βαθμό βεβαιότητας.

Με την παροχή ευρωπαϊκού πλαισίου για την ψηφιακή ταυτότητα που βασίζεται στην αναθεώρηση του ισχύοντος πλαισίου, τουλάχιστον το 80 % των πολιτών αναμένεται να είναι σε θέση να χρησιμοποιεί μια λύση ψηφιακής ταυτότητας για πρόσβαση σε βασικές δημόσιες υπηρεσίες έως το 2030. Σε κάθε περίπτωση, κύρια παράμετρος επιτυχίας του ευρωπαϊκού πλαισίου για την ψηφιακή ταυτότητα θα αποτελέσει η καλλιέργεια κλίματος **εμπιστοσύνης, ασφάλειας, ελέγχου και λογοδοσίας** στους πολίτες και τις επιχειρήσεις. Τούτο προϋποθέτει υψηλό επίπεδο ασφαλείας για την παροχή ψηφιακής ταυτότητας, όπως και για την έκδοση ευρωπαϊκού πορτοφολιού ψηφιακής ταυτότητας, καθώς και οργανωσιακές αλλαγές στις υποδομές για τη συλλογή, αποθήκευση και γνωστοποίηση δεδομένων ψηφιακής ταυτότητας.

Επιπλέον, η πρόταση Κανονισμού της Ε.Ε. (2021), για να ανταποκριθεί στη δυναμική των αγορών και στις τεχνολογικές εξελίξεις, επεκτείνει τον τρέχοντα κατάλογο υπηρεσιών εμπιστοσύνης eIDAS με τρεις νέες εγκεκριμένες υπηρεσίες εμπιστοσύνης. Συγκεκριμένα την παροχή υπηρεσιών ηλεκτρονικής αρχειοθέτησης, τα ηλεκτρονικά καθολικά και τη διαχείριση διατάξεων εξ αποστάσεως δημιουργίας ηλεκτρονικών υπογραφών και σφραγίδων.

Η **ηλεκτρονική ταυτότητα** χρησιμοποιείται ως απόδειξη ταυτοποίησης και αυθεντικοποίησης[56]. Για την εγκαθίδρυση ποιοτικών ηλεκτρονικών υπηρεσιών, το μικροτσίπ της ηλεκτρονικής ταυτότητας μπορεί να συμπεριλάβει ψηφιακά πιστοποιητικά για ψηφιακή υπογραφή και ψηφιακή αυθεντικοποίηση του νόμιμου κατόχου, που καθιστά εφικτή ή διευκολύνει ασφαλείς και πραγματοποιήσιμες ηλεκτρονικές συναλλαγές. Οι ηλεκτρονικές ταυτότητες συχνά γίνονται αντιληπτές, είναι σχεδιασμένες και εφαρμοσμένες σε αυστηρή σύνδεση των βιομετρικών δεδομένων.

Η **χρήση μιας ηλεκτρονικής ταυτότητας που περιλαμβάνει βιομετρικά χαρακτηριστικά ως αναγνωριστικά στοιχεία**, προσφέρει **πιο ακριβή ταυτοποίηση** και περισσότερο **ασφαλή αυθεντικοποίηση του νομίμου κατόχου της κάρτας**.

Ωστόσο, **δεν είναι όλα τα χαρακτηριστικά φυσιολογίας κατάλληλα για ταυτοποίηση**, καθώς απαιτείται να πληρούν συγκεκριμένες προϋποθέσεις. Τα πιο κοινά βιομετρικά χαρακτηριστικά που χρησιμοποιούνται είναι τα δαχτυλικά αποτυπώματα. Η ψηφιακή αναγνώριση προσώπου χρησιμοποιείται ήδη, αλλά το πιο ακριβές και κατάλληλο χαρακτηριστικό είναι η ίριδα του ματιού (iris scan). Πρέπει δε να διευκρινιστεί ότι κανένα βιομετρικό χαρακτηριστικό δεν είναι αυτό που αποθηκεύεται και τυγχάνει επεξεργασίας αλλά ένα πρότυπο-υπόδειγμα αυτού και άρα μια επεξεργασμένη μορφή του βιομετρικού χαρακτηριστικού, η οποία διατηρεί μόνο ένα μέρος της βιομετρικής πληροφορίας.

Επομένως, τίθεται **ζήτημα ως προς την ιδιωτικότητα (άρθρο 2, παρ. 1 και άρθρο 5, παρ. 1 του Συντάγματος), το δικαίωμα στον πληροφοριακό αυτοπροσδιορισμό του προσώπου (άρθρο 9Α του Συντάγματος)**, αλλά και ως προς τη φύση και την χρήση των αναγνωριστικών. Άλλωστε, η έκδοση ηλεκτρονικών ταυτοτήτων που περιλαμβάνει μοναδικά αναγνωριστικά δίνει τη δυνατότητα μιας ευρείας διασυνδεσιμότητας αρχείων και δεδομένων.

Η **προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση βασίζεται σε 5 κυρίως αρχές, βάσει του Κανονισμού (ΕΕ) αριθ. 2016/679 (εφεξής ΓΚΠΔ)**:

- **Σκοπός**: Τα προσωπικά δεδομένα πρέπει να συλλέγονται για ένα συγκεκριμένο και ξεκάθαρο σκοπό.
- **Αναλογικότητα**: Συλλογή και επεξεργασία των προσωπικών δεδομένων πρέπει να είναι επαρκής, σχετική και όχι παραπάνω από την απαιτούμενη για την επεξεργασία.
- **Ανωνυμία:** Τα προσωπικά δεδομένα πρέπει να διατηρούνται σε ένα τύπο, ο οποίος επιτρέπει την ταυτοποίηση των υποκειμένων των προσωπικών δεδομένων.

[56] E-ID Card and Data Protection: a path for good governance - a field of controversy.

- **Ασφάλεια**: Τα κατάλληλα μέτρα ασφαλείας, τα τεχνικά και οργανωσιακά, πρέπει να λαμβάνονται από τους ελεγκτές των δεδομένων και να προστατεύονται από την ακούσια ή τη μη εξουσιοδοτημένη δημοσιοποίηση, καταστροφή ή τροποποίηση σύμφωνα με τις αρχές της ακεραιότητας και της εμπιστευτικότητας.

Μια σημαντική ομάδα βιομετρικών μεθόδων ταυτοποίησης είναι η συμπεριφορική βιομετρική μέθοδος, μέσω της οποίας μπορεί να προσδιοριστεί η ταυτοποίηση του ατόμου, ιδίως αναφορικά με την ανάλυση της γραφής και της υπογραφής.[57]

Οι τεχνολογικές εξελίξεις και οι εφαρμογές τους, επιτρέπουν μια λεπτομερή εκτίμηση, όχι μόνο της απορρέουσας στατικής εικόνας της γραφής, αλλά και της διαδικασίας της δημιουργίας μιας υπογραφής. Αναφερόμαστεστην έγκριση της περίφημης δυναμικής υπογραφής, σε πραγματικό χρόνο, την ταχύτητα μέσα στην οποία αυτή πραγματοποιείται, και την πίεση της πένας στις ατομικές φάσεις της γραφής. Η προσωπική ταυτοποίηση μπορεί να εκληφθεί ως εναλλακτική της υπογραφής. Με την έννοια αυτή, μπορεί να υποστηριχθεί ότι αυτή η απαίτηση μπορεί να εκπληρωθεί, για παράδειγμα, μέσω ενός βιομετρικού ή άλλου ταυτοποιητικού με την στενή έννοια στοιχείου που δεν καθιστά υπογραφή με την νομική έννοια, αλλά παρουσιάζει χαρακτηριστικά με παρόμοιους σκοπούς και λειτουργία.

Παράλληλα, υπογραμμίζεται ότι η ταυτοποίηση ή αυθεντικοποίηση ενός φυσικού προσώπου με τεχνικά μέσα είναι επιτρεπτή, σύμφωνα με τη σκέψη 51 του Γενικού Κανονισμού για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα. **Η Αυθεντικοποίηση μπορεί να εκληφθεί ως η επιβεβαίωση της ταυτότητας με τη μέθοδο (one to one comparison) έναντι του ορισμού της (one-to-many comparison**). Το άρθρο 4 θεμελιώνει ότι τα βιομετρικά δεδομένα επιβεβαιώνουν ή επιτρέπουν το μοναδικό αναγνωριστικό, ενώ το άρθρο 9 δεν καθορίζει, και εφαρμόζεται και στις δύο περιπτώσεις: της αυθεντικοποίησης και της ταυτοποίησης.

Παρότι, η επεξεργασία των βιομετρικών δεδομένων είναι γενικά απαγορευμένη, κατά το άρθρο 9 του ΓΚΠΔ, τα δεδομένα μπορεί να τύχουν επεξεργασίας, εφόσον το υποκείμενο των προσωπικών δεδομένων έχει δώσει τη ρητή συγκατάθεσή του στην επεξεργασία αυτών των δεδομένων.

Η πιθανή χρήση αυτών σύγχρονων μορφών υπογραφής από πολλές απόψεις, η θέση των ηλεκτρονικών γραπτών κειμένων και η νομική τους χρήση, χωρίς αμφιβολία, οδηγεί στην τυποποίηση νέων πρακτικών διαδικασιών συνδυασμών βιομετρικών μεθόδων (ως μια ιδανική αυθεντικοποίηση ή κατά το ήμισυ εργαλείο ταυτοποίησης) και μεθόδους κρυπτολογίας (πιστοποιημένη ηλεκτρονική υπογραφή).

Η μη ελεγχόμενη και χωρίς διακρίσεις είσοδος σε συγκεκριμένες πληροφορίες, οδηγεί στο φαινόμενο του “function creep” (μη υφέρπουσα διεύρυνση των λειτουργιών), την πολύπλευρη και μη δικαιολογημένη επεξεργασία. Αυτό συνεπάγεται την παραβίαση των

[57] Electronic Written Documents and Biometric Options of their Signing - Problem of Evidentiary reliability and personal Data Protection

δικαιωμάτων στην προστασία δεδομένων προσωπικού χαρακτήρα. Αυτός ο κίνδυνος γίνεται πιο άμεσος, όταν η ηλεκτρονική ταυτότητα είναι ο μόνος τρόπος αλληλεπίδρασης με τους δημόσιους οργανισμούς.

Επιπρόσθετα, υπάρχει **κίνδυνος «profiling»** που ρητά απαγορεύεται από τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων. Η χρήση ενός μοναδικού αριθμού για όλες τις βάσεις δεδομένων του κράτους για διάφορους - αν και συγκεκριμένους σκοπούς και παρά το γεγονός ότι το άτομο μπορεί να αποφασίσει, εάν και σε ποιο βαθμό αποδέχεται να αποκαλύψει προσωπικά του δεδομένα, ενώ συμμετέχει σε διαφορετικούς τομείς της δημόσιας ζωής - μπορεί να επιφέρει τον κίνδυνο της κοινωνικής ταξινόμησης των προσώπων.

Υπάρχουν τρεις επιλογές για την τοποθεσία αποθήκευσης των συγκεκριμένων δεδομένων:

- Σε μια συγκεκριμένη βάση δεδομένων
- Στην μνήμη ενός αναγνώστη κάρτας
- Στην ίδια την ηλεκτρονική ταυτότητα

Η απόφαση σχετικά με την πιο κατάλληλη επιλογή είναι υψίστης σημασίας, καθώς στην πράξη διακυβεύεται το ποιος θα έχει νόμιμη πρόσβαση στα αποθηκευμένα δεδομένα.

Η αποθήκευση των δεδομένων σε κεντρική βάση δεδομένων απειλεί το δικαίωμα των πολιτών στην ιδιωτικότητα, κυρίως επειδή δημιουργεί «αποθέματα δεδομένων», τα οποία μπορεί να είναι επιρρεπή και ευάλωτα σε κακόβουλες πρακτικές ή στο ίδιο το κράτος αν εκμεταλλευτεί αυτά τα δεδομένα, χωρίς τη γνώση του κατόχου.

Επιπρόσθετα, λαμβάνοντας υπόψη ότι **τα βιομετρικά δεδομένα είναι χαρακτηριστικά της φυσιολογίας μας, η χρήση τους για την αυτό-ενοχοποίηση προκαλεί ανησυχία, ιδίως σε περιπτώσεις τεχνικών ζητημάτων**, όπως μιας επιτυχούς κυβερνοεπίθεσης, ή απλού λάθους στη διαχείριση της κεντρικής βάσης δεδομένων. Έτσι, ο ν. 4727/2020 (Α’ 184) για την ψηφιακή μετάβαση της Χώρας είναι ένα πολύ ενδιαφέρον θεσμικό πλαίσιο, και ένα ορόσημο για την εισαγωγή ειδικών αναγνωριστικών.

Η ταυτοποίηση του ατόμου σε διαφορετικούς δημόσιους οργανισμούς βασίζεται σε διαφορετικά αναγνωριστικά με περιορισμένη χρήση, που δημιουργήθηκε κρυπτογραφώντας την πηγή του **Pin,** το οποίο ταυτοποιεί τον κάτοχο στην κάρτα, αλλά δεν είναι εκείνο που μεταφέρεται στο άλλο μέρος της επικοινωνίας. Αξίζει να σημειωθεί ότι η ΑΠΔΠΧ είναι εκείνη που πραγματοποιεί την κρυπτογράφηση των αναγνωριστικών, ως ένα κεντρικός εμπιστευτικός εκδότης.

Τα βιομετρικά δεδομένα θα πρέπει να χρησιμοποιούνται, μόνο όταν δεν υπάρχει άλλη μέθοδος ταυτοποίησης ή αυθεντικοποίησης, αλλά ακόμη και τότε, μπορεί να επιλεχθεί η λιγότερο επιβλαβής για την προστασία των προσωπικών δεδομένων μέθοδος σύμφωνα με την (**αρχή της αναλογικότητας**) για την επίτευξη ανάλογου σκοπού.

Όταν το μικροτσίπ μιας ηλεκτρονικής ταυτότητας ενσωματώνει ένα πιστοποιητικό για ψηφιακή αυθεντικοποίηση και κάποιο άλλο πιστοποιητικό ψηφιακής υπογραφής, η ψηφιακή υπογραφή δεν θα πρέπει να ζητείται για την αυθεντικοποίηση, καθώς δεν είναι ανάλογο μέτρο για την επίτευξη του στόχου της αυθεντικοποίησης, καθώς αποκαλύπτονται περισσότερα δεδομένα από όσα θα έπρεπε.

Τα project της Ηλεκτρονικής Διακυβέρνησης συχνά περιλαμβάνουν μεγάλης κλίμακας διαμοιρασμό δεδομένων, τα οποία αφορούν προσωπικά δεδομένα πολιτών[58]. Μάλιστα, τα IDMs (Integrated Data Management System) αποτελούν την προσωπική προϋπόθεση ενός επιτυχημένου e-government.

Είναι απολύτως αναγκαίο τα υπό επεξεργασία δεδομένα να μειώνονται στο απολύτως αναγκαίο (**αρχή της αναγκαιότητας**) και (**αρχή της ελαχιστοποίησης)**.

Ειδικά, οι διασταυρούμενες συγκρίσεις διαφορετικών βάσεων δεδομένων πρέπει να επιτρέπονται από το νόμο, όπως ακριβώς και η είσοδος σε αυτά τα δεδομένα από εταιρείες ή επιχειρήσεις. Συμπληρωματικά, δεν πρέπει να είναι εφικτό να διαγνωστούν δεδομένα, τα οποία είναι αποθηκευμένα σε τακτικές ηλεκτρονικές ταυτότητες από ραδιοφωνική συχνότητα ή από κάποια άλλη ανέπαφη μέθοδο, επειδή η κωδικοποίηση και η κρυπτογράφηση ή η προστασία της πρόσβασης θα διασπαστεί.

Οι κεντρικές βάσεις δεδομένων, τα βιομετρικά και η ασύρματη τεχνολογία είναι ευάλωτα ανοιχτά πρότυπα που η διαλειτουργικότητα συχνά απαιτείται συμπληρωματικά με την έλλειψη της ανεξαρτησίας της πλατφόρμας. – όλα αυτά έχουν αναφερθεί ως παραδείγματα των λόγων ανησυχίας και προβληματισμού των πολιτών αναφορικά με την κλιμάκωση της ανάπτυξης των διαλειτουργικών ηλεκτρονικών ταυτοτήτων. Η ορατή χαμηλή επιτυχία για μεγάλα project του δημοσίου τομέα στο Ηνωμένο Βασίλειο, παρατέθηκε ως επιπλέον απόδειξη για το λόγο για τον οποίο οι πολίτες πρέπει να προβληματίζονται.

Τα **άρθρα 5-11 του Κανονισμού (ΕΕ) αριθ. 2016/679** (ΓΚΠΔ), που ισχύει από τον Μάιο του 2018, θέτει τις βασικές αρχές της επεξεργασίας και αφορά και σε απλά και σε ευαίσθητα δεδομένα. Βασικές αρχές που διέπουν την επεξεργασία των δεδομένων είναι οι αρχές της νομιμότητας, της αντικειμενικότητας και της διαφάνειας. Τα δεδομένα πρέπει να υποβάλλονται σε σύννομη, με θεμιτό τρόπο διαφανή επεξεργασία, με την συγκατάθεση του υποκειμένου ή άλλη συγκατάθεση, βάσει του θεσμικού δικαίου. Η διαφάνεια εισάγεται για πρώτη φορά με τον ΓΚΠΔ και διασφαλίζεται με την ενημέρωση του υποκειμένου για τη συλλογή των δεδομένων και τον σκοπό της συλλογής. Η δε ενημέρωση οφείλει να είναι συνοπτική και κατανοητή, με σαφή και απλή διατύπωση.

Η **αρχή του σκοπού** αφορά στη δήλωση του σκοπού για τον οποίο συλλέγονται τα δεδομένα, η οποία πρέπει να είναι σαφής. Ο ΓΚΠΔ προβλέπει μία εξαίρεση: την περαιτέρω επεξεργασία δεδομένων για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, με την προϋπόθεση της

[58] Security and Privacy Perceptions of E-ID: a grounded research.

διασφάλισης της μη ταυτοποίησης των υποκειμένων των δεδομένων με τεχνικές, όπως η κρυπτογράφηση, η ψευδωνυμοποίηση των δεδομένων, δηλαδή την ανωνυμοποίηση ττους.

Σε κάθε περίπτωση, στο πλαίσιο του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας, προκειμένου να εξακριβώσει κατά πόσο η επεξεργασία για άλλο σκοπό είναι συμβατή με τον οποίο συλλέγονται αρχικώς τα δεδομένα, πρέπει να λαμβάνει υπόψη, μεταξύ άλλων, τα εξής:

- Τη σχέση μεταξύ των σκοπών για τους οποίους έχουν συλλεχθεί τα δεδομένα και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας.
- Τη σχέση υποκειμένου δεδομένων και υπευθύνου επεξεργασίας.
- Τη φύση των δεδομένων, ιδίως των ευαίσθητων.
- Τις συνέπειες περαιτέρω επεξεργασίας για τα υποκείμενα δεδομένων.
- Την ύπαρξη κατάλληλων εγγυήσεων που μπορεί να περιλαμβάνουν η κρυπτογράφηση ή ψευδωνυμοποίηση.
- Σύμφωνα με το **άρθρο 6 του ΓΚΠΔ**, που αφορά στις προϋποθέσεις νόμιμης επεξεργασίας προσωπικών δεδομένων που είναι απλά, είναι απαραίτητη η συγκατάθεση του υποκειμένου των δεδομένων για την επεξεργασία για συγκεκριμένο νόμιμο σκοπό. Επιπροσθέτως, η επεξεργασία των δεδομένων πρέπει να κρίνεται αναγκαία για την εκπλήρωση της εκ του νόμου υποχρέωσης του υπευθύνου επεξεργασίας ή για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή για την άσκηση δημόσιας εξουσίας του υπευθύνου επεξεργασίας.

Σε κάθε περίπτωση, σύμφωνα με το **άρθρο 7 του ΓΚΠΔ**, ο υπεύθυνος επεξεργασίας θα πρέπει να μπορεί να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε ελεύθερα και ρητά, αφού γνωρίζει ποιος είναι ο υπεύθυνος επεξεργασίας και τους σκοπούς της επεξεργασίας.

Η **αρχή της αναλογικότητας** ορίζει ότι τα δεδομένα που συλλέγονται είναι συναφή, πρόσφορα και αναγκαία, ήτοι με βάση την **αρχή της «ελαχιστοποίησης των δεδομένων»**.

Επίσης, η επεξεργασία είναι νόμιμη για άλλους σκοπούς από τους αρχικούς, εφόσον η επεξεργασία είναι συμβατή με τους σκοπούς για τους οποίους τα δεδομένα αρχικά συλλέχθηκαν. Δεν απαιτείται διακριτή νομική βάση.

Η **αρχή της ακρίβειας των δεδομένων** προβλέπει ότι τα δεδομένα θα πρέπει να είναι ακριβή και το υποκείμενο των δεδομένων πρέπει να έχει ενημέρωση ως προς τα δεδομένα τα οποία τυγχάνουν επεξεργασίας.

Επίσης, οι **αρχές της ακεραιότητας και της εμπιστευτικότητας** προβλέπουν ότι τα δεδομένα υποβάλλονται σε επεξεργασία με τρόπο που εγγυάται την ασφάλεια και την προστασία τους από παράνομη επεξεργασία ή απώλεια, καταστροφή ή φθορά τους.

Επιπλέον, η **αρχή της λογοδοσίας** προβλέπει ότι ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να λογοδοτεί κάθε φορά για την ορθή και νόμιμη επεξεργασία των δεδομένων.

Επίσης, θα πρέπει, σύμφωνα με το **άρθρο 15** του ΓΚΠΔ, να διασφαλίζεται το δικαίωμα πρόσβασης του υποκειμένου των δεδομένων στα στοιχεία του, μέσω του υπευθύνου επεξεργασίας, ήτοι το Υπουργείο Ψηφιακής Διακυβέρνησης. Στο ίδιο πλαίσιο, είναι αναγκαίο να διασφαλίζεται η άσκηση του δικαιώματος διόρθωσης (**άρθρο 16**) και του δικαιώματος διαγραφής («δικαίωμα στη λήθη», **άρθρο 17** ΓΚΠΔ) έναντι του υπευθύνου επεξεργασίας.

Σε κάθε περίπτωση, είναι αναγκαία η πλήρης αποτύπωση των δικαιωμάτων των υποκειμένων δικαίου (πολιτών) και των υποχρεώσεων του υπευθύνου επεξεργασίας, συγκεκριμένα, για τον Ενιαίο Προσωπικό Αριθμό, λαμβανομένης της υποχρέωσης προστασίας των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού, σύμφωνα με το **άρθρο 25** του ΓΚΠΔ. Ειδικότερα, βάσει του άρθρου αυτού, προβλέπεται ότι:

«1. Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία, ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.

2. Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Αυτή η υποχρέωση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους. Ειδικότερα, τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων.

3. Εγκεκριμένος μηχανισμός πιστοποίησης σύμφωνα με το άρθρο 42 μπορεί να χρησιμοποιηθεί ως στοιχείο που αποδεικνύει τη συμμόρφωση με τις απαιτήσεις που προβλέπονται στις παραγράφους 1 και 2 του παρόντος άρθρου.».

Εν κατακλείδι, **η καθιέρωση του Προσωπικού Αριθμού** ως νέου τρόπου ταυτοποίησης ή και αυθεντικοποίησης των φυσικών προσώπων στις συναλλαγές τους με τους φορείς του δημοσίου τομέα, **κρίνεται αναγκαία για τη λειτουργία ενός σύγχρονου, αποδοτικού και αποτελεσματικού Κράτους Δικαίου.** Μέσω της θέσπισης ενός σύγχρονου συστήματος ψηφιακής διακυβέρνησης και παροχής ψηφιακών δημόσιων υπηρεσιών στους πολίτες, που θα υλοποιηθεί με σεβασμό στην προστασία των προσωπικών δεδομένων και στην ιδιωτικότητα, θα επιτευχθεί η έμφαση στην στάθμιση μέσου προς σκοπό και η τήρηση των

αρχών του σκοπού, της αναλογικότητας και της ελαχιστοποίησης της επεξεργασίας των δεδομένων των φυσικών προσώπων.

Επιπλέον, **κρίνεται απαραίτητη η συνεργασία με την αρμόδια εποπτική αρχή, ήτοι την Ανεξάρτητη Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,** σύμφωνα με το **άρθρο 31** του ΓΚΠΔ, καθώς και η διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων εξειδικευμένα για την περίπτωση της θεσμοθέτησης του Ενιαίου Προσωπικού Αριθμού στην Ελλάδα.

V.ΒΙΒΛΙΟΓΡΑΦΙΑ

1. ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ Βρυξέλλες, 4.6.2012 COM(2012) 238 final 2012/0146 (COD). https://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2012)0238_/com_com(2012)0238_el.pdf

2. Θ.Κ. ΠΑΠΑΧΡΙΣΤΟΥ, Τ. ΒΙΔΑΛΗΣ, Λ. ΜΗΤΡΟΥ, ΑΝ. ΤΑΚΗΣ. ΤΟ ΔΙΚΑΙΩΜΑ ΣΥΜΜΕΤΟΧΗΣ ΣΤΗΝ ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ. Σειρά: Δίκαιο και Κοινωνία στον 21ο Αιώνα,Αριθμός τεύχους: 11

3. Μπιθιζής – Πέτσης Νικόλαος, Πετρινός Τριαντάφυλλος. Εφαρμογή και χρήση του κανονισμού της ΕΕ 910/2014 στις Ευρωπαϊκές Ένοπλες Δυνάμεις.

4. ΟΔΗΓΙΑ 1999/93/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31999L0093&from=MT

5. Abubakar-sadiq Shehu, Ant´onio Pinto, and Manuel E. Correia. On the Interoperability of European National Identity Cards. https://www.researchgate.net/publication/328736120_On_the_Interoperability_of_European_National_Identity_Cards

6. ALIN DANIEL MUNTEANU. E- BUSINESS – SECURITY AND SPEED. Issue Year: XVI/2010 Issue No: 16 Page Range: 873-877.

7. Ana Bedusch. Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. https://journals.sagepub.com/doi/pdf/10.1177/2053951719855091

8. Annika Selzer, Ulrich Waldmann. eID in Deutschland und den USA. https://ur.art1lib.com/dl/12853267/a05edc

9. Arnis Parsovs. Solving the Estonian ID Card Crisis: the Legal Issues. http://idl.iscram.org/files/arnisparsovs/2020/2245_ArnisParsovs2020.pdf

10. Athina Antoniou. e-ID card & data protection : A path for good governance – a field of controversy

11. Athina Antoniou & Lilian Mitrou. E-ID card & data protection: a path for good governance – a field of controversy.

12. Cavallini S., Bisogni F., Gallozzi D., Cozza C., Aglietti C., (2012), "Study on the supply-side of EU e-signature market", Final Report for the DG Information Society and Media of the European Commission. https://www.researchgate.net/profile/Fabio-Bisogni/publication/263304956_eSignature_-_Study_on_the_supply_side_of_EU_e-signature_market_-_Final_Study_Report_by_Formit/links/0f31753a847d326433000000/eSignature-Study-on-the-supply-side-of-EU-e-signature-market-Final-Study-Report-by-Formit.pdf

13. Christos K. Georgiadis and Emmanouil Stiakakis, Extending an e-Government Service Measurement Framework to m-Governement Services https://www.researchgate.net/publication/229049184_Extending_an_e-Government_Service_Measurement_Framework_to_m-Governement_Services

14. Computer Law & Security Report, Volume 26, Issue 2, 2010, Pages 151-157, http://dx.doi.org/10.1016/j.clsr.2009.11.002

15. Corien Prins. E-government: A Comparative Study of the Multiple Dimensions of Required Regulatory Change

16. Danielle Morgan and Arnis Parsovs. Using the Estonian Electronic Identity Card for Authentication to a Machine. https://eprint.iacr.org/2017/880.pdf

17. Danny De Cock, Christopher Wolf, and Bart Preneel. The Belgian Electronic Identity Card (Overview). https://www.esat.kuleuven.be/cosic/publications/article-769.pdf

18. Digital Agenda: new Regulation to enable cross-border electronic signatures and to get more value out of electronic identification in Digital Single Market.

19. EBMS Working Paper EBMS/2004/2 Personal Identification in the Information Age: The Case of the National Identity Card in the UK Paul Beynon-Davies https://www.researchgate.net/publication/221407164_Personal_Identification_in_the_Information_Age_The_Case_of_the_National_Identity_Card_in_the_UK

20. EU study on the New rules for a new age? Legal analysis of a Single Market for the Information Society. https://op.europa.eu/el/publication-detail/-/publication/a856513e-ddd9-45e2-b3f1-6c9a0ea6c722

21. European Union Agency for Cybersecurity (ENISA), 2020 Reproduction is authorised provided the source is acknowledged. https://www.enisa.europa.eu/recruitment/working-for-enisa/general-information-for-newcomers/enisa-welcome-guide

22. European Union Agency for Cybersecurity (ENISA), 2019 Reproduction is authorised provided the source is acknowledged.

23. European Union Agency for Cybersecurity (ENISA), 2021 Reproduction is authorised provided the source is acknowledged. https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2021-2023

24. Frank Byszio, Detlef Houdeau, Gisela Meister, Klaus-Dieter Wolfenstetter Elektronische Identifikation in Europa: die neue EU-Verordnung

25. Gerli Aavik, Robert Krimmer. Integrating Digital Migrants: Solutions for Cross-border Identification from E-residency to eIDAS. https://www.researchgate.net/publication/301693948_Integrating_Digital_Migrants_Identifying_Solutions_for_Cross-border_Identification_between_E-residency_and_eIDAS_A_Case_Study_from_Estonia

26. Giovanni BUTTARELLI. ΕΥΡΩΠΑΙΟΣ ΕΠΟΠΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ. Συνοπτική παρουσίαση της γνωμοδότησης του Ευρωπαίου Επόπτη Προστασίας Δεδομένων σχετικά με την πρόταση κανονισμού για την ενίσχυση της ασφάλειας των δελτίων ταυτότητας των πολιτών της Ένωσης και άλλων εγγράφων. https://edps.europa.eu/sites/default/files/publication/19-01-04_opinion_new_deal_consumers_summary_el.pdf

27. Herbert Kubicek & Torsten Noack.The path dependency of national electronic identities. A comparison of innovation processes in four European countries. Received: 14 October 2009 / Accepted: 9 March 2010 / Published online: 10 April 2010 # The Author(s) 2010. This article is published with open access at Springerlink.com https://www.researchgate.net/publication/47617776_The_path_dependency_of_national_electronic_identities

28. Identity Management: a Key e-Business Enabler Marco Casassa Mont, Pete Bramhall, Mickey Gittler, Joe Pato, Owen Rees https://www.researchgate.net/publication/2525054_Identity_Management_a_Key_e-Business_Enabler

29. Ingo Naumann, Giles Hogben European Network and Information Security Agency (ENISA) https://www.enisa.europa.eu/publications/archive/pet/view/++widget++form.widgets.fullReport/@@download/privacy_features_of_eid_cards.pdf

30. James Backhouse and Ruth Halperin. SECURITY AND PRIVACY PERCEPTIONS OF E- ID: A GROUNDED RESEARCH. https://core.ac.uk/download/pdf/301350573.pdf

31. Ján Matejka, Vojen Güttler. ELECTRONIC WRITTEN DOCUMENTS AND BIOMETRIC OPTIONS OF THEIR SIGNING – PROBLEM OF EVIDENTIARY RELIABILITY AND PERSONAL DATA PROTECTION. https://tlq.ilaw.cas.cz/index.php/tlq/article/download/267/252

32. J. Espinosa García, L. Hernández Encinas, and A. Queiruga Dios. THE NEW SPANISH ELECTRONIC IDENTITY CARD: DNI-e. https://digital.csic.es/bitstream/10261/15941/3/IT07_DNIe.pdf

33. John Nugent. The E-business security imperative: important issues and drivers.

34. Maxim Chanillon,Prof. Joep Cromvoets,Athanasios Deligiannis,Vassilis Koulolias,Gideon Mekonnen Jonathan and Asst. Prof. Vassilios Peristeras. Report: Managing the Public Sector Digital Transformation. https://web.ihu.edu.gr/mdt2017/media-files/documents/Report_web.pdf

35. Michael Koch and Kathrin M. Möslein. Identities Management for E-Commerce and Collaboration Applications. https://www.researchgate.net/profile/Michael-Koch-21/publication/230634651_Identities_Management_for_E-Commerce_and_Collaboration_Applications/links/0912f50be785846b91000000/Identities-Management-for-E-Commerce-and-Collaboration-Applications.pdf

36. Niko Tsakalakis, Sophie Stalla-Bourdillon and Kieron O'Hara. What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation. https://eprints.soton.ac.uk/400477/2/paper.pdf

37. Oldrich Bures · Helena Carrapico. Security Privatization How Non-security-related Private Businesses Shape Security Governance. https://www.researchgate.net/publication/319186182_Security_Privatization_How_Non-security-related_Private_Businesses_Shape_Security_Governance

38. Oliver Terbu, Stefan Vogl and Sebastian Zehetbauer. One mobile ID to secure physical and digital Identity. https://dl.gi.de/bitstream/handle/20.500.12116/603/43.pdf?sequence=1&isAllowed=y

39. Paul Beynon-Davies. Personal identity management and electronic government The case of the national identity card in the UK

40. Paul Przemysław Polan´ski, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union

41. Pieter Verhaeghe , Jorn Lapon , Vincent Naessens , Bart De Decker , Kristof Verslype and Girma Nigusse. Security and Privacy Threats of the Belgian Electronic Identity Card and Middleware. https://www.academia.edu/18861969/Security_and_Privacy_Improvements_for_the_Belgian_eID_Technology

42. Prof. Dr. Victor J.J.M. Bekkers, Prof. Jean Hartley and Prof. Sharon S. Dawes. Innovation and the Public Sector. Volume: 14 of Innovation and the Public Sector, Publication date: March 2009.

43. Stakeholder Workshop Digital Agenda for Europe: electronic identification, authentication and signatures in the European digital single market 10 March 2011, Brussels.

44. Stephen E. Blythe, Digital Signature Law of the United Nations, European Union, United Kingdom and United Stats: Promotion of Growth in E-Commerce with Enhanced Security, 11 RICH. J.L. & TECH. 2 (2005), at http://law.richmond.edu/jolt/v11i2/article6.pdf.

45. Study on an electronic identification, authentication and signature policy (IAS) IAS in the European policy context 17 August 2012 D.1 Final

46. Study on the standardisation aspects of eSignatures Final Report Published in November 2007. http://publications.europa.eu/resource/cellar/c3870b23-20ea-4009-b8b9-cf1fbb3680a4.0001.01/DOC_1

47. THE USE AND RISKS OF ELECTRONIC IDENTITY CARDS: THE CASE OF GREECE. http://arno.uvt.nl/show.cgi?fid=116052

48. Vassilios Peristeras, Konstantinos Tarabanis. The Connection, Communication, Consolidation, Collaboration Interoperability Framework (C4 IF) For Information Systems Interoperability https://repository.dinus.ac.id/docs/ajar/6.pdf

49. William Echikson. EUROPE'S DIGITAL IDENTIFICATION OPPORTUNITY . https://www.ceps.eu/wp-content/uploads/2020/06/TFR_Europe-Digital-Identification-Opportunity.pdf

50. Waltraut Kotschy. THE AUSTRIAN E-GOVERNMENT SYSTEM – TOWARDS DATA PROTECTION COMPATIBLE E-GOVERNMENT. https://www.iprs.si/fileadmin/user_upload/Pdf/razno/W21.pdf