ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΠΛΗΡΟΦΟΡΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΦΟΡΙΚΗΣ

Οι επιπτώσεις της τεχνολογίας RFID στην ιδιωτικότητα και η αντιμετώπισή τους σε νομικό και τεχνολογικό επίπεδο

Διδακτορική διατριβή

Μαρία Νικήτα

Πτυχιούχος Τμήματος Εφαρμοσμένης Πληροφορικής

MSc, Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών (ΔΠΜΣ) στην «Πληροφορική και Διοίκηση»

Επιβλέπουσα

Ευγενία Αλεξανδροπούλου – Αιγυπτιάδου

Καθηγήτρια Τμήματος Εφαρμοσμένης Πληροφορικής

Θεσσαλονίκη, Ιανουάριος 2020

Big Brother is watching. ~ 1984

George Orwell

Περίληψη

Η πλέον σύγχρονη τεχνολογία αυτόματης αναγνώρισης και ηλεκτρονικής ταυτοποίησης είναι η τεχνολογία RFID. Η χρήση της έχει γίνει ιδιαίτερα ελκυστική και χρησιμοποιείται σε πληθώρα εφαρμογών, διότι με τις ιδιότητές της διευκολύνει σημαντικά μια σειρά από δραστηριότητες σε πολλούς τομείς. Πέρα όπως από πλεονεκτήματα, η χρήση της παρουσιάζει και αρκετά προβλήματα ασφαλείας και ιδιωτικότητας πολιτών τα οποία προκαλούν έντονο προβληματισμό.

Έχει παρατηρηθεί πως σε διεθνές επίπεδο έχουν αναληφθεί σχετικές νομοθετικές πρωτοβουλίες για την προστασία της ιδιωτικότητας από την εφαρμογή της τεχνολογίας RFID, όχι όμως και στον ελληνικό χώρο. Σκοπός της παρούσας διατριβής είναι να προταθεί η δημιουργία ενός ελληνικού νομοθετικού πλαισίου ρυθμιστικού της χρήσης της τεχνολογίας RFID, με βασικές αρχές οι οποίες θα αποβλέπουν στο σεβασμό και στην προστασία των δεδομένων που συγκεντρώνονται και χρησιμοποιούνται στα συστήματα που χρησιμοποιούν την εν λόγω τεχνολογία, αλλά δεν θα παρεμποδίζουν την εκμετάλλευση των πλεονεκτημάτων της και την περαιτέρω εξέλιξή της.

Η διατριβή χωρίζεται σε τέσσερα μέρη. Στο πρώτο μέρος της διατριβής δίνεται βαρύτητα στην τεχνολογία RFID, παρουσιάζονται αναλυτικά τα συστατικά της μέρη, οι σημαντικότεροι κίνδυνοι στην ιδιωτικότητα που προκύπτουν από τη χρήση της τεχνολογίας, οι βασικοί τύποι επιθέσεων κατά της τεχνολογίας και τα υπάρχοντα μέτρα προστασίας της ιδιωτικότητας. Στο δεύτερο μέρος μελετάται η νομική ρύθμιση της τεχνολογίας εξετάζοντας την εφαρμογή του δικαίου της ΕΕ στην επεξεργασία των προσωπικών δεδομένων, τα βήματα προς τη δημιουργία ενός πλαισίου για την προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές συστημάτων RFID στον ευρωπαϊκό χώρο και το προτεινόμενο αυτό πλαίσιο (PIA). Στο τρίτο μέρος ερευνώνται οι εφαρμογές της τεχνολογίας RFID πραγματοποιώντας συγκριτική επισκόπηση νομοθετικών πρωτοβουλιών σε ΕΕ και ΗΠΑ σχετικά με τρεις χαρακτηριστικούς τομείς εφαρμογής της τεχνολογίας RFID που αφορούν α) την εμφύτευση RFID ετικέτας στο

ανθρώπινο σώμα, β) τη χρήση της τεχνολογίας RFID στα ηλεκτρονικά διαβατήρια και γ) τη χρήση της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου. Ολοκληρώνοντας στο τέταρτο μέρος παρουσιάζονται συγκεντρωτικά οι προτάσεις για ειδική ρύθμιση της χρήσης της τεχνολογίας RFID στην ελληνική έννομη τάξη.

Λέξεις κλειδιά: RFID, ασφάλεια, προσωπικά δεδομένα, ιδιωτικότητα, μέτρα προστασίας, PIA, εμφύτευση, ηλεκτρονικά διαβατήρια, λιανικό εμπόριο

Abstract

Nowadays, the latest technology of electronic identification is the RFID technology. Its use has become highly attractive and it is being used to many applications because its advantages significantly facilitate a wide range of activities in many areas. But apart from advantages, its use also introduces a number of security and privacy issues for citizens of great concern.

It has been observed that there have been legislative initiatives at international level related to the privacy protection from the implementation of the RFID technology, but not in Greece. The aim of the thesis is to propose the creation of a Greek regulatory framework regulating the use of the RFID technology based on the protection of the data that are collected and used in systems using this technology but will not prevent exploiting its advantages and its further development.

The thesis is divided into four parts. At the first part emphasis is given to the RFID technology presenting its components, the most important risks to privacy resulting from its use, the main types of attacks against the technology and the existing privacy measures. At the second part the technology's legal regulation is presented examining the application of the EU law with regard to the processing of personal data, the steps towards creating a framework for the safe implementation of the RFID systems and the proposed framework (PIA). At the third part the RFID applications are presented and comparative study of the legislative initiatives at the European Union and the United States of America is carried out related to 1) the implantation of RFID chips on the human body, 2) the use of RFID technology in electronic passports and 3) the use of RFID technology in retail. Finally, at the fourth part, proposals are made for the creation of a Greek regulatory framework regulating the use of the RFID technology.

Keywords: RFID, security, personal data, privacy, privacy measures, PIA, implantation, electronic passports, retail

Ευχαριστίες

Ιδιαίτερες ευχαριστίες θέλω να απευθύνω στην επιβλέπουσα Καθηγήτρια και Αντιπρύτανη του Πανεπιστημίου Μακεδονίας κ. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, για την άριστη συνεργασία και την πνευματική και ηθική υποστήριξη που μου προσέφερε καθ' όλη τη διάρκεια εκπόνησης της διδακτορικής μου διατριβής. Οι γνώσεις της στο αντικείμενο της προστασίας των προσωπικών δεδομένων και οι συμβουλές της υπήρξαν πολύτιμες για την επιτυχημένη ολοκλήρωσή της.

Επιπλέον θα ήθελα να ευχαριστήσω θερμά τον Καθηγητή κ. Ιωάννη Μαυρίδη καθώς και τον Καθηγητή κ. Ιωάννη Ιγγλεζάκη που συμμετείχαν στην τριμελή επιτροπή, μελέτησαν τη διατριβή και συνέβαλαν στην επιτυχή περάτωσή της. Ομοίως, θερμές ευχαριστίες οφείλονται και στα τέσσερα μέλη που συμπληρώνουν την επταμελή επιτροπή, την Καθηγήτρια κ. Μάρω Βλαχοπούλου, τον Καθηγητή κ. Χρήστο Γεωργιάδη, τον Αναπληρωτή Καθηγητή κ. Εμμανουήλ Στειακάκη και τον Αναπληρωτή Καθηγητή κ. Κωνσταντίνο Ψάννη.

Επίσης θέλω να εκφράσω τις ευχαριστίες μου σε όλα τα υπόλοιπα μέλη της Ερευνητικής Ομάδας του Δικαίου Πληροφορικής του Πανεπιστημίου Μακεδονίας για τη συνεργασία τους.

Τέλος, σε μια πράξη ευγνωμοσύνης, θα ήθελα να ευχαριστήσω το σύζυγό μου Δημήτρη, το γιο μας Έκτορα και τους γονείς μου για την κατανόηση και την ενθάρρυνση που μου παρείχαν καθ' όλη τη διάρκεια εκπόνησης της διατριβής.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Πίνακας Πινάκων

I. Εισαγωγικές παρατηρήσεις

Στη σημερινή εποχή η τεχνολογία εξελίσσεται με αλματώδεις ρυθμούς επηρεάζοντας σε καθημερινή βάση τόσο την οικονομική ανάπτυξη όσο και την κοινωνική ζωή των ανθρώπων. Η εποχή των δεδομένων μεγάλης κλίμακας (big data) όπου με το διαδίκτυο των πραγμάτων και τη χρήση του υπολογιστικού νέφους[1], πληθώρα συσκευών και αντικείμενα κάθε είδους συνδέονται μεταξύ τους αυτοματοποιημένα με ελάχιστη έως και καθόλου συμμετοχή των φυσικών προσώπων είναι πλέον γεγονός. Αυτό έχει ως συνέπεια η ανταλλαγή των δεδομένων σε παγκόσμιο επίπεδο[2] να έχει αυξηθεί σε πολύ μεγάλο βαθμό όπου θα μπορούσε να χαρακτηριστεί ως και ανεξέλεγκτη. Έτσι λοιπόν, πληροφορίες[3] οι οποίες περιέχουν προσωπικά δεδομένα φυσικών προσώπων καθίστανται πολύ εύκολα διαθέσιμα ανά πάσα στιγμή και οπουδήποτε στον κόσμο με αποτέλεσμα να είναι εκτεθειμένα και η προσβολή της ιδιωτικότητας των κατόχων τους σε κίνδυνο.

Ταυτόχρονα είναι χαρακτηριστικό γεγονός και η εποχή όπου οι ιστότοποι κοινωνικής δικτυώσεως και οι υπηρεσίες που προσφέρουν έχουν κατακτήσει μεγάλο μέρος από τον ελεύθερό μας χρόνο. Όμως, πέρα από τα πλεονεκτήματα που προσφέρουν στην επικοινωνία και στην κοινωνικοποίηση των ανθρώπων, δεν πρέπει να αγνοούνται και οι κίνδυνοι[4] που προκύπτουν

[1] Σχετικά με την προστασία των προσωπικών δεδομένων από τη χρήση του υπολογιστικού νέφους βλ. Παπαδόπουλος Μ.–Ευγενίδης, Π. (2016). Νεφοϋπολογιστική (cloud computing) και προστασία προσωπικών δεδομένων, ΔiΜΕΕ 2/2016, 182-195, Μήτρου, Λ. (2015). Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος, ΔiΜΕΕ 4/2015, σελ: 534-549, Κίτσος, Π., Παππά, Π. (2012). Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στις υπηρεσίες του υπολογιστικού νέφους, ΔiΜΕΕ 2/2012, σελ: 166-176, 46, Κουσουνή-Πανταζοπούλου, Α. (2012). Νομικές Διαστάσεις του Cloud Computing, ΔiΜΜΕ 2/2012, σελ: 177-185.

[2] Σύμφωνα με τον Γεραρής Χ. (2010, σελ. 43), "*η παγκοσμιοποιημένη οικονομία αυξάνει την ανάγκη διακίνησης προσωπικών δεδομένων είτε μεταξύ ομίλων εταιρειών, είτε μεταξύ συνεργαζόμενων εταιρειών*".

[3] Σύμφωνα με τον Γέροντα Α. (1990, σελ. 12) "*οι πληροφορίες αποτελούν οικονομικό, πολιτιστικό και συνταγματικό αγαθό αλλά ταυτόχρονα και παράγοντα δημιουργίας κινδύνων για τον πολίτη, τονίζοντας έτσι την ανάγκη, την αποστολή και τη σημασία του δικαίου των πληροφοριών"*. Επίσης, αναφορικά με την εννοιολογική προσέγγιση του δικαίου των πληροφοριών ή της πληροφορικής, βλ. Ιγγλεζάκης, Ι. (2006). Εισαγωγή στο Δίκαιο της Πληροφορικής, εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη, σελ: 1-8.

[4] Ένα από τα βασικότερα προβλήματα το οποίο έχει να αντιμετωπίσει το δίκαιο στο χώρο του διαδικτύου είναι ο άυλος χαρακτήρας του διαδικτύου και η ανυπαρξία σαφών χρονικών και χωρικών ορίων τα οποία αποτελούν βασικές συνισταμένες της νομικής ρύθμισης. Βλ. Μαντζούφας, Π. (2007). Η Διακινδύνευση στην Κοινωνίας της Πληροφορίας και η Προστασία των Προσωπικών Δεδομένων, Αρμ Ζ΄, σελ. 1089.

από τη μαζική τους χρήση στην ιδιωτικότητα των χρηστών[5] και κυρίως των ανηλίκων[6] οι οποίοι περνάνε ακόμη περισσότερο χρόνο καθημερινά στον κυβερνοχώρο και καθιστούν διαθέσιμα δημόσια σε παγκόσμιο επίπεδο πλήθος προσωπικών δεδομένων που τους αφορούν, είτε μη γνωρίζοντας, είτε αγνοώντας τους πιθανούς κινδύνους[7].

Η ενίσχυση της σχέσης εμπιστοσύνης ανάμεσα στους χρήστες μιας τεχνολογίας και στην ίδια την τεχνολογία είναι καθοριστικής σημασίας τόσο για την εξέλιξη της τεχνολογίας όσο και για την οικονομική ανάπτυξη και την κοινωνική ζωή των χρηστών της. Όπως αναφέρεται και στην αιτιολογική έκθεση της πρότασης του Κανονισμού 2016/679[8] "*η οικοδόμηση εμπιστοσύνης στο επιγραμμικό περιβάλλον είναι καθοριστικής σημασίας για την οικονομική ανάπτυξη. Η έλλειψη εμπιστοσύνης κάνει τους καταναλωτές να διστάζουν να αγοράσουν επιγραμμικά και να υιοθετήσουν νέες υπηρεσίες. Αυτό απειλεί να επιβραδύνει την ανάπτυξη καινοτόμων χρήσεων των νέων τεχνολογιών*". Σε κάθε περίπτωση, απαραίτητη προϋπόθεση για την ενίσχυση

[5] Βλ. Παναγοπούλου-Κουτνατζή, Φ. (2010). Οι ιστότοποι κοινωνικής δικτυώσεως ως εθνική, ευρωπαϊκή και διεθνής πρόκληση της προστασίας της ιδιωτικότητας, εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη. Επίσης, σχετικά με την προστασία των προσωπικών δεδομένων στα κοινωνικά δίκτυα βλ. Ιγγλεζάκης, Ι. (2013). Προστασία προσωπικών δεδομένων στις υπηρεσίες κοινωνικής δικτύωσης με βάση την Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της ΕΕ για την προστασία των δεδομένων, σε Πρακτικά 4ου Πανελλήνιου Συνέδριου της Ένωσης Ελλήνων Νομικών «e-Θέμις» και του Πανεπιστημίου Μακεδονίας, με τίτλο «Legal Tech & Data Protection (Θεσσαλονίκη 22-24 Μαρτίου 2013), εκδ. Νομική Βιβλιοθήκη, Αθήνα 2013, σελ: 113-125.

[6] Σχετικά με το ευαίσθητο θέμα της προστασίας των ανηλίκων στο διαδίκτυο βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2018). Η προστασία των προσωπικών δεδομένων ανηλίκων στο Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679, ΔiΜΕΕ 1/2018, σελ: 5-19, Alexandropoulou-Egyptiadou, E. (2014). Minors' internet navigation and personal data protection, in International Organizations and the Protection of Human Rights, Essays in honor of Prof. Paroula Naskou-Perraki (eds.Th. Skouteris- M. Vagias), ed. Themis, N.A.Sakkoulas and Co, Athens 2014. 215-219, Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2013). Η προστασία των προσωπικών δεδομένων των ανηλίκων στην Πρόταση Κανονισμού για την προστασία των προσωπικών δεδομένων της 25.1.2012», σε Πρακτικά 4ου Πανελλήνιου Συνέδριου της Ένωσης Ελλήνων Νομικών «e-Θέμις» και του Πανεπιστημίου Μακεδονίας, με τίτλο «Legal Tech & Data Protection (Θεσσαλονίκη 22-24 Μαρτίου 2013), εκδ. Νομική Βιβλιοθήκη, Αθήνα 2013, σελ: 47-56, Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2008). Κοινωνία της Πληροφορίας και Νομική Προστασία των Προσωπικών Δεδομένων της Οικογένειας και των Μελών της, Ελληνική Δικαιοσύνη 49 (2008), σελ. 691-699, Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2007). Η Πλοήγηση των Ανηλίκων στο Διαδίκτυο και η Νομική Προστασία των Προσωπικών Δεδομένων, Αρμενόπουλος ΞΑ, σελ: 848-854.

[7] Σχετικά με τους κινδύνους που προκύπτουν από τη χρήση κοινωνικών δικτύων κυρίως από ανηλίκους βλ. Michalopoulos, D., Mavridis, I. (2010). Surveying privacy leaks through online social network, 14th Panhellenic Conference on Informatics, IEEE, pp. 184-187, ISBN: 978-1-4244-7838-5, DOI: 10.1109/PCI.2010.31.

[8] Η πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβούλιου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Γενικός Κανονισμός για την Προστασία Δεδομένων) διαθέσιμη στο https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX%3A52012PC0011

της σχέσης εμπιστοσύνης ανάμεσα στις νέες τεχνολογίες και στους χρήστες είναι η λήψη των κατάλληλων μέτρων ασφαλείας των πληροφοριών που επεξεργάζονται.

Επίσης, κρίνεται σκόπιμο να λαμβάνονται υπόψη τα σχετικά παραδείγματα διδακτικής της ιστορίας. Διότι όπως αναφέρει και ο Ο.Ο.Σ.Α. σε κείμενό του[9] το ίδιο λάθος που έγινε με τη γρήγορη εξάπλωση του διαδικτύου χωρίς τη λήψη των απαραίτητων μέτρων ασφαλείας εξαρχής το οποίο οδήγησε στην υποκλοπή πολλών πληροφοριών, δεν πρέπει να επαναληφθεί. Όσον αφορά τις τεχνολογικές εξελίξεις λοιπόν, το δίκαιο προστασίας είναι λογικό να μην έπεται αλλά πάντοτε να προηγείται των τεχνολογικών εξελίξεων για να αποτρέπονται από την αρχή ενδεχόμενοι κίνδυνοι στην ιδιωτικότητα.

Σκοπός της παρούσας διατριβής είναι να εξετάσει την τεχνολογία RFID, τις επιπτώσεις της στην ιδιωτικότητα και την αντιμετώπισή τους σε νομικό και τεχνολογικό επίπεδο και τελικά να προταθεί η δημιουργία ενός ελληνικού νομοθετικού πλαισίου ρυθμιστικού της χρήσης της τεχνολογίας RFID, με βασικές αρχές οι οποίες θα αποβλέπουν στο σεβασμό και στην προστασία των δεδομένων που συγκεντρώνονται και χρησιμοποιούνται στα συστήματα που χρησιμοποιούν την εν λόγω τεχνολογία, αλλά δεν θα παρεμποδίζουν την εκμετάλλευση των πλεονεκτημάτων της και την περαιτέρω εξέλιξή της. Για την επίτευξη του σκοπού αυτού η διατριβή χωρίστηκε σε τέσσερα μέρη τα οποία αφορούν 1) την παρουσίαση της τεχνολογίας, 2) τη νομική ρύθμιση της τεχνολογίας, 3) τις εφαρμογές της τεχνολογίας και συγκριτική επισκόπηση νομοθετικών πρωτοβουλιών σε ΕΕ και ΗΠΑ και 4) τις προτάσεις για ειδική ρύθμιση της χρήσης της τεχνολογίας RFID στην ελληνική έννομη τάξη.

Στο πρώτο μέρος της διατριβής, το οποίο εστιάζεται στην παρουσίαση της τεχνολογίας RFID, αρχικά γίνεται λόγος για το διαδίκτυο των πραγμάτων του οποίου η ανάπτυξη επηρεάζεται από τις εφαρμογές της τεχνολογίας RFID (κεφάλαιο 1) και για το γραμμωτό κώδικα ο οποίος είναι προγενέστερο σύστημα αυτόματης αναγνώρισης της τεχνολογίας RFID (κεφάλαιο 2).

[9] OECD (2008), OECD Policy Guidance on Radio Frequency Identification (RFID), Ministerial Meeting on the future of the meeting economy, Seoul, Korea, 17-18 June, p.p. 37, διαθέσιμο σε http://www.oecd.org/sti/ieconomy/oecdpolicyguidanceonradiofrequencyidentificationrfid.htm.

Ακολουθεί αναλυτική παρουσίαση των συστατικών μερών της τεχνολογίας (κεφάλαιο 3) και η σύγκρισή της με το γραμμωτό κώδικα (κεφάλαιο 4), παρουσιάζονται οι διάφορες εφαρμογές της τεχνολογίας RFID ανά κατηγορία φορέων των ετικετών (κεφάλαιο 5), οι κίνδυνοι για την ιδιωτικότητα που προκύπτουν από τη χρήση της, οι επιθέσεις κατά της τεχνολογίας RFID και τα προτεινόμενα μέτρα προστασίας της ιδιωτικότητας για την αντιμετώπιση των κινδύνων και των επιθέσεων (κεφάλαιο 6).

Στο δεύτερο μέρος της διατριβής, το οποίο αφορά τη νομική ρύθμιση της τεχνολογίας, αρχικά γίνεται αναφορά στην εφαρμογή του δικαίου της ΕΕ στην επεξεργασία των προσωπικών δεδομένων (κεφάλαιο 1). Έπειτα εξετάζονται οι συστάσεις της Ομάδας εργασίας του άρθρου 29 σε γνώμη της σχετικά με τις πρόσφατες εξελίξεις στο ΔτΠ οι οποίες σχετίζονται με την εφαρμογή της τεχνολογίας RFID (κεφάλαιο 2). Σε επόμενα κεφάλαια μελετάται η συμβολή του Ο.Ο.Σ.Α. (OECD) στην υιοθέτηση ενός αποδεκτού πλαισίου για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων από εφαρμογές των συστημάτων RFID στον ευρωπαϊκό χώρο (κεφάλαιο 3), τα βήματα που έγιναν προς τη δημιουργία αυτού του πλαισίου (κεφάλαιο 4) και η παρουσίαση του προτεινόμενου πλαισίου για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID (κεφάλαιο 5). Ολοκληρώνοντας, γίνεται σύντομη παρουσίαση του ελληνικού νομοθετικού πλαισίου για την προστασία των προσωπικών δεδομένων (κεφάλαιο 6).

Στο τρίτο μέρος της διατριβής, το οποίο ασχολείται με τις εφαρμογές της τεχνολογίας και τη συγκριτική επισκόπηση των νομοθετικών πρωτοβουλιών σε ΕΕ και ΗΠΑ, εξετάζεται περιπτωσιολογία εφαρμογών της τεχνολογίας RFID. Συγκεκριμένα, μελετώνται νομοσχέδια, νόμοι και γνώμες που έχουν δημοσιευτεί κατά περιόδους στην Ευρωπαϊκή Ένωση και στις Ηνωμένες Πολιτείες της Αμερικής σχετικά με τρεις χαρακτηριστικούς τομείς εφαρμογής της τεχνολογίας RFID που αφορούν α) την εμφύτευση RFID ετικέτας στο ανθρώπινο σώμα (κεφάλαιο 1), β) τη χρήση της τεχνολογίας RFID στα ηλεκτρονικά διαβατήρια (κεφάλαιο 2) και γ) τη χρήση της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου (κεφάλαιο 3). Για κάθε

μία από τις τρεις παραπάνω περιπτώσεις, στο τέλος κάθε κεφαλαίου παρατίθενται τα συμπεράσματα που έχουν προκύψει.

Τέλος, στο τέταρτο μέρος της διατριβής παρουσιάζονται οι προτάσεις για ειδική ρύθμιση της χρήσης της τεχνολογίας RFID στην ελληνική έννομη τάξη.

II. ΜΕΡΟΣ ΠΡΩΤΟ

Παρουσίαση της τεχνολογίας RFID

Η τεχνολογία της ταυτοποίησης μέσω ραδιοσυχνοτήτων (Radio Frequency Identification, RFID), στο εξής τεχνολογία RFID, αποτελεί την πλέον σύγχρονη τεχνολογία αυτόματης αναγνώρισης και ηλεκτρονικής ταυτοποίησης η οποία θεωρείται η μετεξέλιξη της τεχνολογίας των ραβδωτών κωδικών (barcodes)[10]. Με αυτή τη σύγχρονη και επαναστατική, όπως χαρακτηρίζεται, τεχνολογία επιτυγχάνεται η ταυτόχρονη αναγνώριση πολλών αντικειμένων και προσώπων χωρίς την προϋπόθεση της φυσικής ή οπτικής επαφής, με τρόπο εύκολο και γρήγορο.

Σημαντικά πλεονεκτήματα προσφέρονται στους χρήστες της τεχνολογίας RFID και ήδη μέχρι σήμερα εφαρμόζεται και χρησιμοποιείται με επιτυχία σε πολλές εφαρμογές. Χαρακτηριστικές εφαρμογές της τεχνολογίας RFID είναι οι αυτοματοποιημένες πληρωμές (όπως στα διόδια), ο έλεγχος πρόσβασης σε εγκαταστάσεις και κτίρια (όπως στα αεροδρόμια και στα εργαστήρια), τα επίσημα έγγραφα (όπως στα διαβατήρια), η σήμανση των αγαθών, η διαχείριση των τροφοδοσιών και των αποθηκών, η ηλεκτρονική παρακολούθηση των αντικειμένων, των ζώων αλλά και των ανθρώπων.

Όμως, πέρα από τα πλεονεκτήματα που προσφέρει, η εφαρμογή της τεχνολογίας RFID καθιστά το άτομο διαρκή πομπό δεδομένων. Αυτό έχει ως αποτέλεσμα να δημιουργούνται και σημαντικά ζητήματα ασφαλείας, καθώς οι πληροφορίες αυτές είναι δυνατόν να αναγνωσθούν και να γίνουν αντικείμενο επεξεργασίας από τρίτους, διαταράσσοντας τη σχέση επικοινωνίας που υπήρχε μέχρι σήμερα μεταξύ αποστολέα και παραλήπτη[11].

Η χωρίς προβλήματα εφαρμογή της τεχνολογίας RFID προϋποθέτει ότι τα εμπλεκόμενα μέρη λειτουργούν με ασφαλή τρόπο και σύμφωνα με το

[10] Βλ. Roberts, C. M. (2006). Radio frequency identification (RFID). Computers & security, Vol. 25(1), pp. 18-26.

[11] Βλ. Συνοδινού, Τ.-Ε. (2005). Η ανίχνευση της ιδιωτικότητας μέσα από τις ραδιοσυχνότητες: Προστασία προσωπικών δεδομένων και τεχνολογιών αναγνώρισης μέσω ραδιοσυχνοτήτων (RFID), Αρμ ΝΘ', σελ. 1365.

πνεύμα της προστασίας της ιδιωτικότητας[12]. Όμως, το γεγονός ότι το άτομο καθίσταται διαρκής πομπός δεδομένων τα οποία μπορούν να αναγνωστούν και από τρίτους χωρίς να το γνωρίζει, εισάγουν ένα σημαντικό αριθμό προβλημάτων καθιστώντας αναγκαία τη λήψη μέτρων για την ασφάλειά του.

Σε αυτό το μέρος της διατριβής αρχικά γίνεται λόγος για το διαδίκτυο των πραγμάτων του οποίου η ανάπτυξη επηρεάζεται κατά κόρον από τις εφαρμογές της τεχνολογίας RFID. Σε επόμενο κεφάλαιο παρουσιάζεται ο γραμμωτός κώδικας ο οποίος είναι το πιο διαδεδομένο σύστημα αυτόματης αναγνώρισης σε πραγματικό χρόνο, προγενέστερο της τεχνολογίας RFID. Ακολουθεί η αναλυτική παρουσίαση της τεχνολογίας RFID και η σύγκριση με τον γραμμωτό κώδικα. Ολοκληρώνοντας, παρουσιάζονται οι διάφορες εφαρμογές της τεχνολογίας RFID ανά κατηγορία φορέων των ετικετών, οι κίνδυνοι για την ιδιωτικότητα που προκύπτουν από τη χρήση της, οι επιθέσεις κατά της τεχνολογίας RFID και τέλος τα προτεινόμενα μέτρα προστασίας της ιδιωτικότητας για την αντιμετώπιση των κινδύνων και των επιθέσεων.

1. Διαδίκτυο των Πραγμάτων

Το Διαδίκτυο των Πραγμάτων (Internet of Things) είναι μία έννοια η οποία έχει απασχολήσει έντονα τους ερευνητές. Το διαδίκτυο είναι ένα παγκόσμιο δίκτυο επικοινωνίας διασυνδεδεμένων δικτύων υπολογιστών το οποίο επιτρέπει την επικοινωνία των χρηστών του ανά πάσα στιγμή και από οποιοδήποτε μέρος του κόσμου. Αρχικά είχε στατική μορφή και προσέφερε κυρίως τη δημιουργία στατικών ιστοσελίδων μόνο για ανάγνωση από επιχειρήσεις προς ενημέρωση των χρηστών του, χωρίς να έχουν οι χρήστες τη δυνατότητα συμμετοχής (web 1.0). Μετέπειτα, με την εξέλιξη των τεχνολογιών του διαδικτύου, το διαδίκτυο απέκτησε δυναμική μορφή και η σχέση επικοινωνίας των χρηστών με τις επιχειρήσεις έγινε αμφίδρομη. Οι χρήστες απέκτησαν τη δυνατότητα αλληλεπίδρασης σε πραγματικό χρόνο και καταγραφής των δικών τους σχολίων διαθέσιμων προς το ευρύ κοινό του

[12] Βλ. Αλεξανδροπούλου–Αιγυπτιάδου, Ε., Μαυρίδης, Ι. (2007). Η Προστασία των Προσωπικών Δεδομένων Ενόψει της Εφαρμογής της Νέας Τεχνολογίας της Ταυτοποίησης με Ραδιοσυχνότητες (RFID): Νομική και Τεχνολογική Προσέγγιση, Αρμ ΞΑ΄, σελ: 497.

διαδικτύου, χωρίς να απαιτείται να έχουν εξειδικευμένες γνώσεις. Σήμερα πλέον, με την εξέλιξη της τεχνητής νοημοσύνης, το διαδίκτυο έχει μετατραπεί σε σημασιολογικό ιστό ο οποίος αντιλαμβάνεται τις απαιτήσεις του χρήστη. Οι ιστοσελίδες περιέχουν πληροφορίες κατανοήσιμες και από μηχανές (μετα-δεδομένα) βοηθώντας έτσι στην καλύτερη συλλογή και επεξεργασία, με αποτέλεσμα να βελτιώνεται ο τρόπος αναζήτησης πληροφοριών στο διαδίκτυο και η εμπειρία του χρήστη.

Η εποχή της πανταχού συνδεσιμότητας είναι πλέον γεγονός. Με την εξέλιξη των νέων τεχνολογιών και με τη βοήθεια του διαδικτύου επιτυγχάνεται η ασύρματη σύνδεση όχι μόνο μεταξύ υπολογιστών, αλλά και οποιουδήποτε αντικειμένου με ένα άλλο αντικείμενο, ή πρόσωπο, ή ζώο, αρκεί να φέρουν την κατάλληλη τεχνολογία. Χρησιμοποιώντας δηλαδή τις υποδομές του διαδικτύου, οι νέες τεχνολογίες προσφέρουν τη διασύνδεση όλων των αντικειμένων και των ανθρώπων σε πραγματικό χρόνο, δημιουργώντας έτσι ένα δυναμικό παγκόσμιο δίκτυο όπου παράγονται, συλλέγονται και ανταλλάσσονται κάθε είδους δεδομένα, το γνωστό Διαδίκτυο των Πραγμάτων (στο εξής ΔτΠ).

Το ΔτΠ έχει εξέχουσα οικονομική και κοινωνική σημασία, ενώ ταυτόχρονα ξαναφέρνει στο προσκήνιο το ευαίσθητο θέμα της προστασίας της ιδιωτικότητας. Όπως δήλωσε και η Neelie Kroes, Αντιπρόεδρος της Ευρωπαϊκής Επιτροπής, «*[τ]ο διαδίκτυο των πραγμάτων με νοημοσύνη ενσωματωμένη σε αντικείμενα καθημερινής χρήσης είναι το επόμενο μεγάλο βήμα. Θέλω να προωθήσω ένα διαδίκτυο των πραγμάτων που θα εξυπηρετεί τους οικονομικούς και κοινωνικούς στόχους μας, διατηρώντας παράλληλα την ασφάλεια, την προστασία της ιδιωτικής ζωής και τον σεβασμό των ηθικών αξιών*.».[13]

Το εύρος των εφαρμογών του ΔτΠ είναι μεγάλο και συμβάλλει σημαντικά στη βελτίωση της ποιότητας της ζωής των ανθρώπων.

[13] Βλ. Δελτίο Τύπου (IP/12/360), Ψηφιακό θεματολόγιο: Η Επιτροπή ανοίγει διαβούλευση σχετικά με τις έξυπνες, συνδεδεμένες συσκευές- το «διαδίκτυο των πραγμάτων», 12 Απριλίου 2012, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-12-360_el.htm

Παραδείγματος χάριν[14], ορισμένες υφιστάμενες εφαρμογές είναι η προσκόλληση ετικετών στα φαρμακευτικά προϊόντα οι οποίες επιτρέπουν την επαλήθευση της γνησιότητας κάθε σκευάσματος προτού χορηγηθεί στον ασθενή μειώνοντας έτσι την παραχάραξη και τα σφάλματα χορήγησης, η εγκατάσταση έξυπνων ηλεκτρικών συστημάτων μέτρησης της κατανάλωσης τα οποία παρέχουν πληροφορίες στους καταναλωτές σε πραγματικό χρόνο και επιτρέπουν στους παρόχους ηλεκτρικής ενέργειας την από απόσταση παρακολούθηση των ηλεκτρικών συσκευών και τα «έξυπνα αντικείμενα» τα οποία διευκολύνουν την ανταλλαγή πληροφοριών και αυξάνουν την αποτελεσματικότητα του κύκλου παραγωγής σε παραδοσιακούς κλάδους όπως η διακίνηση εμπορευμάτων, η μεταποίηση και η λιανική πώληση. Εκτός άλλων, η τεχνολογία κλειδί η οποία εφαρμόζεται στις προαναφερόμενες εφαρμογές και επομένως συμβάλλει στην ανάπτυξη του ΔτΠ, είναι η τεχνολογία RFID με την οποία ασχολείται και η παρούσα διατριβή.

Είναι ξεκάθαρο πως το ΔτΠ ενδέχεται να ενσωματωθεί στην καθημερινή ζωή των ανθρώπων. Έχει παρατηρηθεί πως ο αριθμός των αντικειμένων που συνδέονται με το διαδίκτυο και διαθέτει ο μέσος άνθρωπος αναμένεται να αυξηθεί σε 7 με 25 δισεκατομμύρια συσκευές συνδεμένες ασύρματα παγκοσμίως, ενώ έως το 2020 ο αριθμός αυτός μπορεί να διπλασιαστεί φτάνοντας τα 50 δισεκατομμύρια[15]. Ταυτόχρονα και το μέγεθος των συστημάτων αυτών έχει την τάση να μειώνεται τόσο πολύ που σε πολλές περιπτώσεις δεν είναι εύκολα ορατό από το ανθρώπινο μάτι, όπως σε εφαρμογές της τεχνολογίας RFID όπου οι ετικέτες ενδέχεται να έχουν ακόμη και το μέγεθος ενός κόκκου ρυζιού (βλ. Μέρος πρώτο, υποκεφάλαιο 3.3.1.3).

Ένα παράδειγμα[16] μίας πιθανής μελλοντικής κατάστασης, όπου το ΔτΠ θα έχει ενσωματωθεί σε όλα τα καθημερινά αντικείμενα, είναι η περίπτωση

[14] Βλ. Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των περιφερειών, Το Ίντερνετ των πραγμάτων- Ένα σχέδιο δράσης για την Ευρώπη, COM(2009) 278 τελικό, σελ. 3-4, διαθέσιμη στο http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2009)0278_/com_com(2009)0278_el.pdf

[15] Βλ. δελτίο τύπου (IP/12/360), Ψηφιακό θεματολόγιο: Η Επιτροπή ανοίγει διαβούλευση σχετικά με τις έξυπνες, συνδεδεμένες συσκευές- το «διαδίκτυο των πραγμάτων», ό.π.

[16] Βλ. δελτίο τύπου (IP/12/360), Ψηφιακό θεματολόγιο: Η Επιτροπή ανοίγει διαβούλευση σχετικά με τις έξυπνες, συνδεδεμένες συσκευές- το «διαδίκτυο των πραγμάτων», ό.π. και Παναγοπούλου-

στην οποία ένα ηλικιωμένο άτομο έχει παραλείψει να πάρει ένα σημαντικό χάπι, οπότε θα μπορούσε να σταλεί ένα προειδοποιητικό μήνυμα σε κάποιο άλλο πρόσωπο ή σε τοπικό κέντρο έκτακτης ανάγκης ώστε κάποιος να επικοινωνήσει με το ηλικιωμένο άτομο και να ελέγξει την κατάσταση. Επίσης, οτιδήποτε καταναλώνεται θα ελέγχεται μέσω της χρήσεως μικροσκοπικών ετικετών και με τον τρόπο αυτό οι παραγωγοί θα ενημερώνονται άμεσα για τις ανάγκες των πελατών τους. Η ιστορία οποιουδήποτε προϊόντος από την παραγωγή έως την τοποθέτησή του στο ράφι θα μπορεί να αποθηκευθεί προσφέροντας αυξημένη διαχείριση ποιότητας καθ' όλη τη διάρκεια της αλυσίδας εφοδιασμού. Τέλος, ευφυή δίκτυα σε οικίες ή στον εργασιακό χώρο για την καταμέτρηση και τον έλεγχο της θερμοκρασίας με σκοπό την εξοικονόμηση ενέργειας θα επιτρέπουν να ανιχνευθεί με τι ασχολούνται οι παρευρισκόμενοι στο χώρο αναλύοντας τα χαρακτηριστικά όλων με βάση τις δραστηριότητές τους.

Σύμφωνα με σχετική ανακοίνωση της Επιτροπής[17], το ΔτΠ ναι μεν συμβάλλει σημαντικά στη βελτίωση της ποιότητας της ζωής των ανθρώπων, ταυτόχρονα όμως επιφέρει και βαθιές κοινωνικές αλλαγές. Επομένως, πολλές από αυτές τις αλλαγές πρέπει να αντιμετωπιστούν από ευρωπαϊκούς φορείς χάραξης πολιτικής και δημόσιες αρχές, ώστε να εξασφαλιστεί ότι η χρήση τεχνολογιών και εφαρμογών του ΔτΠ θα τονώσει την οικονομική ανάπτυξη, θα βελτιώσει την ευημερία των ατόμων και θα αντιμετωπίσει ορισμένα από τα προβλήματα της σημερινής κοινωνίας. Μάλιστα, σε πρόσφατο έγγραφό της[18] σχετικά με την προώθηση του ΔτΠ στην Ευρώπη, η Επιτροπή πρότεινε μία ανθρωποκεντρική προσέγγιση. Συγκεκριμένα πρότεινε την ενίσχυση της εμπιστοσύνης, της ασφάλειας και της προστασίας των προσωπικών

Κουτνατζή, Φ. (2014). Διαδίκτυο των πραγμάτων (Internet of Things-IoT): Αποικισμός της καθημερινής ζωής ή νέα τεχνολογική πρόκληση;, ΔiΜΕΕ 3/2014, σελ. 346.

[17] Βλ. Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των περιφερειών, Το Ίντερνετ των πραγμάτων-Ένα σχέδιο δράσης για την Ευρώπη, ό.π., σελ. 6.

[18] Βλ. Commission Staff working document, Advancing the Internet of Things in Europe, accompanying the document "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Digitising European Industry - Reaping the full benefits of a Digital Single Market COM(2016) 180", Brussels, 19.4.2016, διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016SC0110.

δεδομένων και της ιδιωτικότητας λαμβάνοντας ταυτόχρονα υπόψη και τις ανάγκες για την ψηφιοποίηση της βιομηχανίας.

Τέλος, η Ομάδα εργασίας του άρθρου 29 εξέδωσε γνώμη[19] για τις πρόσφατες εξελίξεις στο ΔτΠ στην οποία προσδιορίζονται οι κυριότεροι κίνδυνοι που απειλούν την προστασία των δεδομένων στο ΔτΠ και παρέχει καθοδήγηση για τον τρόπο εφαρμογής του νομικού πλαισίου της ΕΕ. Η γνώμη αυτή παρουσιάζεται αναλυτικά παρακάτω στο δεύτερο μέρος της διατριβής (βλ. Μέρος δεύτερο, Κεφάλαιο 2).

2. Ο γραμμωτός κώδικας

Ο γραμμωτός κώδικας (ή αλλιώς γραμμοκώδικας ή ραβδοκώδικας, barcode) είναι το πρώτο και το πιο διαδεδομένο σύστημα αυτόματης αναγνώρισης σε πραγματικό χρόνο το οποίο δημιουργήθηκε για τις ανάγκες αναγνώρισης κυρίως προϊόντων. Πρόκειται για μία κωδικοποιημένη πληροφορία η οποία αναπαριστάται από κάθετες διαδοχικές μαύρες και λευκές λωρίδες (bars) διαφορετικού πάχους και αναγράφεται πάνω σε αυτοκόλλητες ετικέτες οι οποίες προσκολλώνται στη συσκευασία των προϊόντων. Η αλληλουχία των λωρίδων αυτών κάθε φορά είναι διαφορετική και με αυτό τον τρόπο αντιστοιχεί σε διαφορετικό αριθμό.

Ειδικοί οπτικοί αναγνώστες γραμμωτών κωδικών (barcode scanners) διαβάζουν στιγμιαία το γραμμωτό κώδικα. Συγκεκριμένα, μία δέσμη ακτινών laser πέφτει πάνω στις διαδοχικές μαύρες και λευκές λωρίδες του γραμμωτού κώδικα και στη συνέχεια με τη βοήθεια της ανάκλασης αποκωδικοποιούνται και μεταφράζονται σε ένα δυαδικό αριθμό (μία αλληλουχία από 0 και 1). Μετέπειτα, με τη χρήση αυτού του αριθμού και με τη βοήθεια ενός υπολογιστή ο οποίος συνδέεται σε μία βάση δεδομένων, αναζητώνται όλες οι σχετικές εγγραφές για το προϊόν που φέρει το συγκεκριμένο γραμμωτό κώδικα, όπως η τιμή και η περιγραφή του προϊόντος.

[19] Βλ. Γνώμη 8/2014 σχετικά με τις πρόσφατες εξελίξεις στο διαδίκτυο των πραγμάτων, 1471/14/EL, WP 223, 6 Σεπτεμβρίου, σελ. 26-30, διαθέσιμη στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_el.pdf

Για τη δημιουργία ενός γραμμωτού κώδικα, ο πιο διαδεδομένος τύπος που χρησιμοποιείται είναι ο EAN-13 (European Article Number, EAN) ο οποίος ανήκει στην οικογένεια προτύπων EAN/UPC. Αρχικά δημιουργήθηκε το UPC-A (Universal Product Code, UPC) πρότυπο το οποίο αποτελείται από 12 ψηφία και χρησιμοποιείται κυρίως στις ΗΠΑ. Μετέπειτα, επειδή αυξήθηκε η ζήτηση στην Ευρώπη, στην Ασία και στην Αυστραλία και δημιουργήθηκε η ανάγκη να προστεθούν κωδικοί χωρών, αναπτύχθηκε το EAN-13 πρότυπο το οποίο αποτελείται από 13 ψηφία και είναι υπερσύνολο του UPC-A. Ωστόσο, υπάρχουν και άλλοι τύποι γραμμωτών κωδικών με λιγότερα ή περισσότερα ψηφία (όπως οι UPC-E, EAN-8, ISBN, PostNet, Code 39, Code 128, DataMatrix) οι οποίοι χρησιμοποιούνται σε διαφορετικούς επιχειρηματικούς τομείς[20].

Εικόνα 1 Πρότυπα γραμμωτών κωδίκων UPC-A και EAN-13

Πηγή: https://www.gs1.org/docs/barcodes/GS1_Barcodes_Fact_Sheet-GS_%20EAN_UPC_family.pdf

Ο γραμμωτός κώδικας είναι απλός και εύκολος στη χρήση του και μέχρι σήμερα εξακολουθεί να είναι η επικρατούσα τεχνολογία στη διαχείριση της εφοδιαστικής αλυσίδας. Ενώ η τεχνολογία RFID, για την οποία θα γίνει αναλυτική παρουσίαση στο παρακάτω κεφάλαιο, είναι ο απόγονος του γραμμωτού κώδικα, φέρει πολλά πλεονεκτήματα και όπως σχολιάζεται στη βιβλιογραφία είναι θέμα χρόνου για να αντικαταστήσει το γραμμωτό κώδικα (σύγκριση του γραμμωτού κώδικα με την τεχνολογία RFID βλ. Μέρος πρώτο, Κεφάλαιο 4).

[20] Περισσότερες πληροφορίες σχετικά με την οικογένεια προτύπων EAN/UPC διαθέσιμες στο https://www.gs1.org/standards/barcodes/ean-upc

3. Η τεχνολογία RFID

Η συντόμευση RFID είναι τα αρχικά του όρου Radio Frequency Identification ο οποίος στα ελληνικά μεταφράζεται ως ταυτοποίηση με τη χρήση ραδιοσυχνοτήτων. Η τεχνολογία RFID είναι ένας γενικός όρος που χρησιμοποιείται για τις τεχνολογίες οι οποίες χρησιμοποιούν ραδιοκύματα για την αυτόματη αναγνώριση ανθρώπων και, κατά κύριο λόγο, αντικειμένων[21].

Στο παρόν κεφάλαιο θα γίνει η αναλυτική παρουσίαση της τεχνολογίας RFID. Αρχικά γίνεται μία ιστορική αναδρομή της τεχνολογίας, έπειτα παρουσιάζονται τα βασικά συστατικά μέρη και οι συχνότητες λειτουργίας των συστημάτων RFID, το επίπεδο ισχύος που εκπέμπουν, τα πρότυπα ISO που έχουν δημιουργηθεί ανά ζώνη συχνοτήτων για τις διάφορες εφαρμογές της τεχνολογίας και τα πρότυπα του ηλεκτρονικού κώδικα προϊόντος (EPC).

3.1. Ιστορική αναδρομή

Η τεχνολογία RFID δεν είναι καινούρια, όπως συχνά αναφέρεται, και γι' αυτό πολλές φορές χαρακτηρίζεται και ως the "world's oldest new technology"[22].

Η εφεύρεση και η ανάπτυξη της τεχνολογίας δεν είναι εύκολο να προσδιοριστεί χρονικά. Κάποιος θα μπορούσε να υποστηρίξει πως η ιστορία ξεκινά από την εφεύρεση του ραντάρ το οποίο στέλνει ραδιοκύματα για τον εντοπισμό αντικειμένων και αργότερα με τη χρήση των συστημάτων αναμετάδοσης μεγάλης εμβέλειας για την αναγνώριση και τη διάκριση των φιλικών αεροσκαφών από τα εχθρικά στο Β' Παγκόσμιο Πόλεμο (Identification, Friend or Foe, IFF). Ακόμη, η πρώτη εργασία η οποία ασχολήθηκε με την τεχνολογία είναι του Harry Stockman με τίτλο «Communication by Means of Reflected Power» το 1948[23].

[21] Βλ. Roberts, C. M. (2006). Radio frequency identification (RFID), ό.π., σελ. 19.
[22] Βλ. OECD (2008). OECD Policy Guidance on Radio Frequency Identification (RFID), Ministerial Meeting on the future of the meeting economy, Seoul, Korea, 17-18 June, σελ. 20.
[23] Βλ. Roberts, C. M. (2006). Radio frequency identification (RFID), ό.π. σελ: 18.

Η δεκαετία του 1950 ήταν περίοδος ανακάλυψης της τεχνολογίας RFID μετά την εξέλιξη του ασυρμάτου και του ραντάρ από τις προηγούμενες δεκαετίες[24]. Επίσης, μεταξύ άλλων, μία από τις μελέτες οι οποίες ασχολήθηκαν και προώθησαν την ανάπτυξη της τεχνολογίας είναι του Vernon F. με τίτλο «Application of the microwave homodyne» το 1952 και η ευρεσιτεχνία του Harris D.B. με τίτλο «Radio transmission systems with modulatable passive responder» το 1960.

Η εμπορική εκμετάλλευση της τεχνολογίας και επομένως και η εξάπλωσή της ξεκίνησε μία δεκαετία αργότερα, τη δεκαετία του 1960, όπου άρχισε να χρησιμοποιείται για πρώτη φορά ως σύστημα ηλεκτρονικής παρακολούθησης αντικειμένων (Electronic Article Surveillance, EAS) με τον εντοπισμό ή όχι της ετικέτας RFID για την αντιμετώπιση των κλοπών σε καταστήματα λιανικής πώλησης στα αντικείμενα μεγάλης αξίας και στο ρουχισμό. Έπειτα, τη δεκαετία του 1970 παρουσιάστηκε έντονο ενδιαφέρον από ερευνητές, πολλές εταιρείες και οργανισμούς, ακαδημαϊκά ινστιτούτα και ερευνητικά εργαστήρια και γι' αυτό παρατηρείται αλματώδης ανάπτυξη και πρόοδος της τεχνολογίας με πρώτες εφαρμογές την παρακολούθηση των ζώων, την παρακολούθηση των οχημάτων και την αυτοματοποίηση των διαδικασιών στα εργοστάσια[25].

Τη δεκαετία του 1980 επιτυγχάνεται πλέον η εφαρμογή της τεχνολογίας σε πολλούς διαφορετικούς τομείς ανά τον κόσμο. Συγκεκριμένα, στις ΗΠΑ αναπτύχθηκαν συστήματα RFID κυρίως για τη διευκόλυνση των μεταφορών, τον έλεγχο πρόσβασης προσωπικού και λιγότερο για την παρακολούθηση των ζώων. Ενώ στην Ευρώπη αναπτύχθηκαν συστήματα RFID μικρής εμβέλειας κυρίως για την παρακολούθηση των ζώων και για εφαρμογές στη βιομηχανία και στις επιχειρήσεις[26].

Τη δεκαετία του 1990 η εφαρμογή της τεχνολογίας RFID στα διόδια επεκτάθηκε ευρέως στις ΗΠΑ γεγονός που εκτόξευσε τη διάδοση της τεχνολογίας σε άλλες χώρες αλλά και σε άλλους επιχειρηματικούς τομείς.

[24] Βλ. Landt, J. (2005). The history of RFID. IEEE potentials, Vol. 24(4), σελ: 9.
[25] Βλ. Roberts, C. M. (2006). Radio frequency identification (RFID), ό.π. σελ: 18-19.
[26] Βλ. Landt, J. (2005). The history of RFID, ό.π. σελ: 10.

Συγκεκριμένα, πρώτη η Οκλαχόμα το 1991 εφάρμοσε την αυτόματη πληρωμή των διοδίων με τη χρήση της τεχνολογίας RFID και ένα χρόνο μετά το Χιούστον παράλληλα με την αυτόματη πληρωμή των διοδίων πραγματοποίησε και παρακολούθηση της κίνησης. Την ίδια δεκαετία, αναπτύχθηκαν και διεθνή πρότυπα ώστε να είναι εφικτό να μπορεί να χρησιμοποιηθεί η τεχνολογία RFID παγκοσμίως[27].

Σε έρευνα που έγινε από την Ευρωπαϊκή Στατιστική Υπηρεσία (Eurostat)[28] και καταμετρήθηκαν ανά χώρα οι επιχειρήσεις[29] οι οποίες χρησιμοποιούν την τεχνολογία RFID είναι φανερό πως από το 2009 ο αριθμός τους έχει αυξηθεί σημαντικά με τη Φιλανδία (23%), το Βέλγιο (21%) και τη Σερβία (20%) να έχουν το μεγαλύτερο ποσοστό. Επίσης, στη λίστα των χωρών αυτών είναι και η Ελλάδα[30] και φαίνεται πως η χρήση της τεχνολογίας RFID στη χώρα μας έχει ανοδικές τάσεις καθώς από 2% το 2011 έφτασε στο 7% το 2017. Είναι πλέον φανερό λοιπόν πως η τεχνολογία RFID πρόκειται να γίνει αναπόσπαστο κομμάτι της ζωής των ανθρώπων καθώς ήδη βρίσκεται σε πολλές εφαρμογές και συναντάται σε πολλά καθημερινά αντικείμενα[31].

3.2. Κατανόηση της τεχνολογίας RFID

Σκοπός της τεχνολογίας RFID είναι η διευκόλυνση της μετάδοσης δεδομένων και ειδικότερα η δημιουργία ενός περιβάλλοντος όπου όλα τα αντικείμενα που θα φέρουν την εν λόγω τεχνολογία θα μπορούν να αναγνωριστούν, να ταυτοποιηθούν και να εντοπιστούν από απόσταση, ασύρματα και χωρίς να απαιτείται οπτική επαφή. Πρόκειται λοιπόν για μία μέθοδο ασύρματου εντοπισμού και ηλεκτρονικής ταυτοποίησης αντικειμένων η οποία βασίζεται στη χρήση ραδιοκυμάτων.

[27] Βλ. Landt, J. (2005). The history of RFID, ό.π. σελ: 10.
[28] Έρευνα της Ευρωπαϊκής Στατιστικής Υπηρεσίας "Enterprises using radio frequency identification (RFID) instrument" διαθέσιμη στο https://ec.europa.eu/eurostat/web/products-datasets/-/tin00126.
[29] Η έρευνα αφορά επιχειρήσεις που απασχολούν 10 άτομα και άνω.
[30] Οι πληροφορίες που αφορούν την Ελλάδα είναι διαθέσιμες στο https://ec.europa.eu/eurostat/tgm/refreshTableAction.do?tab=table&plugin=1&pcode=tin00126&language=en
[31] Βλ. Landt, J. (2005). The history of RFID, ό.π. σελ: 8.

Επί παραδείγματι, η τεχνολογία RFID χρησιμοποιείται πολύ συχνά στη διαχείριση της εφοδιαστικής αλυσίδας για τον εντοπισμό αντικειμένων καθ' όλη τη διαδρομή τους, από την αποθήκευσή τους όταν εισέρχονται στην εφοδιαστική αλυσίδα ως πρώτη ύλη έως ότου φτάσουν στα χέρια των καταναλωτών με τη μορφή τελικού προϊόντος προς πώληση. Με αυτό τον τρόπο ελέγχονται σε πραγματικό χρόνο τα αποθέματα, βελτιστοποιείται και επιταχύνεται η γραμμή παραγωγής, μειώνονται τα ανθρώπινα λάθη και επομένως και το λειτουργικό κόστος και τελικά επιτυγχάνεται η ικανοποίηση του καταναλωτή στο μέγιστο[32].

3.3. Συστατικά μέρη των συστημάτων RFID

Τα βασικά μέρη ενός RFID συστήματος είναι η ετικέτα (tag) και ο αναγνώστης (reader) τα οποία με τη βοήθεια του ενδιάμεσου λογισμικού (middleware) συνδέονται με το υπολογιστικό σύστημα (βλ. Εικόνα 2). Αναλυτικότερα, η ετικέτα είναι προσκολλημένη στο αντικείμενο και επικοινωνεί με τον αναγνώστη χρησιμοποιώντας μία κεραία και έπειτα ο αναγνώστης με τη βοήθεια του ενδιάμεσου λογισμικού επικοινωνεί με το υπολογιστικό σύστημα για την ταυτοποίηση του αντικειμένου που φέρει την ετικέτα.

Εικόνα 2 Ένα τυπικό σύστημα RFID

Πηγή: Sardroud, J. M. (2012, σελ. 384)

[32] Βλ. Nikita, M. (2012). RFID in the Supply Chain and the Privacy Concerns, in Bottis, M., Alexandropoulou,E., Iglezakis,I., (edit.). Values and Freedoms in Modern Information Law & Ethics, Proceedings of the 4th International Conference of Information Law and Ethics, University of Macedonia, 20-22 May 2011, ed. Nomiki Bibliothiki Group, Athens 2012, pp. 1212-1233.

Σε αυτή την ενότητα, θα παρουσιαστούν τα συστατικά μέρη των συστημάτων RFID, όπως έχουν καταγραφεί στη σχετική βιβλιογραφία, για την καλύτερη κατανόηση του τρόπου λειτουργίας της τεχνολογίας RFID.

3.3.1. Ετικέτες ή πομποδέκτες

Η ετικέτα[33] (ή αλλιώς πομποδέκτης) αποτελεί την ταυτότητα του αντικειμένου που τη φέρει καθώς έχει αποθηκευμένες πληροφορίες που το χαρακτηρίζουν μοναδικά και βοηθάνε στην αναγνώρισή του. Αποτελείται από ένα ολοκληρωμένο κύκλωμα στο οποίο αποθηκεύονται δεδομένα και από μία κεραία με τη βοήθεια της οποίας μεταδίδονται τα δεδομένα αυτά στον αναγνώστη. Η πιο συνηθισμένη μορφή ετικετών που κυκλοφορεί στην αγορά είναι οι αυτοκόλλητες ετικέτες πάνω στις οποίες εκτυπώνεται και οπτική πληροφορία, όπως ο αναγνωριστικός κωδικός του αντικειμένου που τη φέρει.

Εικόνα 3 Ετικέτα RFID.

Πηγή: http://www.teotec.gr/articleb3cd.html?cat=89

Η ετικέτα μπορεί να χαρακτηριστεί και ως το πιο κρίσιμο στοιχείο του συστήματος, συνεπώς είναι σημαντικό πάντοτε να επιλέγεται η κατάλληλη ετικέτα σύμφωνα με τη χρήση για την οποία προορίζεται. Πιο συγκεκριμένα, ορισμένες από τις πιο βασικές κατηγοριοποιήσεις ετικετών βάσει των χαρακτηριστικών τους είναι οι παρακάτω:

- ανάλογα με την πηγή ενέργειας διακρίνονται σε:
    - παθητικές (passive)

[33] Η ετικέτα ονομάζεται στη βιβλιογραφία και ως αναμεταδότης καθώς διαθέτει μία κεραία και επικοινωνεί με τον αναγνώστη.

- ενεργητικές (active)
- ημι-παθητικές (semi-passive)

- ανάλογα με τη δυνατότητα εγγραφής-ανάγνωσης διακρίνονται σε:
  - αναγνώσιμες (read only)
  - μίας εγγραφής (write once)
  - επανεγγράψιμες (Read/write)
- ανάλογα με την κατασκευή και την εφαρμογή τους διακρίνονται σε:
  - έξυπνες κάρτες
  - γυάλινους σωλήνες
  - ετικέτες ενωτίου
  - δίσκους ετικετών
- ανάλογα με τα λειτουργικά τους χαρακτηριστικά διακρίνονται σε:
  - κατηγορία 1/0
  - κατηγορία 2
  - κατηγορία 3
  - κατηγορία 4
  - κατηγορία 5

Πίνακας 1 Κατηγοριοποίηση ετικετών RFID βάσει των χαρακτηριστικών τους

Πηγή Ενέργειας	**Δυνατότητα εγγραφής - ανάγνωσης**	**Κατασκευή και εφαρμογή**	**Λειτουργικότητα**
Παθητικές	Αναγνώσιμες	Έξυπνες κάρτες	Κατηγορία 1/0
Ενεργητικές	Επανεγγράψιμες	Γυάλινοι σωλήνες	Κατηγορία 2
Ημι-παθητικές	Μίας εγγραφής	Ετικέτες ενωτίου	Κατηγορία 3
		Δίσκοι	Κατηγορία 4
			Κατηγορία 5

Στις παρακάτω υποενότητες παρουσιάζονται οι ετικέτες όπως έχουν καταταχθεί ανά κατηγορία βάσει των χαρακτηριστικών τους.

3.3.1.1. Κατηγοριοποίηση βάσει της πηγής ενέργειας

Ανάλογα με τον τρόπο με τον οποίο τροφοδοτούνται ενέργεια για να λειτουργήσουν οι ετικέτες χωρίζονται σε παθητικές, ενεργητικές και ημι-παθητικές.

Στην περίπτωση των παθητικών ετικετών, η σημαντικότερη διαφορά τους με τις ενεργητικές είναι ότι δε διαθέτουν πηγή ενέργειας και επομένως είναι ανενεργές έως ότου λάβουν ενέργεια από τον αναγνώστη. Ο αναγνώστης λοιπόν είναι αυτός ο οποίος ξεκινάει την επικοινωνία με την ετικέτα όταν αυτή εισέλθει στο ηλεκτρομαγνητικό πεδίο που εκπέμπει και συγκεκριμένα μέσω ραδιοκυμάτων τα οποία λαμβάνονται από την κεραία της ετικέτας. Έτσι, τροφοδοτείται η ετικέτα με ενέργεια ώστε να τεθεί σε λειτουργία και έπειτα να αποστείλει στον αναγνώστη τα ζητούμενα δεδομένα. Λόγω της έλλειψης της πηγής ενέργειας, οι παθητικές ετικέτες έχουν συγκριτικά μικρό μέγεθος, αρκετά μικρότερο κόστος και σχεδόν απεριόριστη ζωή. Τα μειονεκτήματά τους όμως είναι ότι δεν μπορούν να εκπέμψουν σε μεγαλύτερες αποστάσεις από μερικά μέτρα, η ισχύς του σήματος του αναγνώστη πρέπει να είναι αρκετά δυνατή για να ληφθεί και έχουν μικρό χώρο αποθήκευσης δεδομένων.

Οι ενεργητικές ετικέτες, σε αντίθεση με τις παθητικές, διαθέτουν τη δική τους πηγή ενέργειας (συνήθως μία μπαταρία) και είναι ενεργειακά ανεξάρτητες. Επομένως είναι συνεχώς ενεργές, μπορούν να λειτουργήσουν και ως αισθητήρες περιβάλλοντος και να καταγράφουν δεδομένα από το περιβάλλον, όπως τη θερμοκρασία και την υγρασία και έχουν και τη δυνατότητα οι ίδιες να ξεκινήσουν την επικοινωνία με έναν αναγνώστη και να αποστείλουν τα ζητούμενα δεδομένα. Λόγω όμως της ενσωματωμένης πηγής ενέργειας η οποία κάποια στιγμή αποφορτίζεται, έχουν περιορισμένη διάρκεια ζωής καθώς και μεγαλύτερο μέγεθος και κόστος. Συγκριτικά με τις παθητικές ετικέτες τα σημαντικότερα πλεονεκτήματά τους είναι ότι διαθέτουν μεγαλύτερο χώρο αποθήκευσης δεδομένων, μπορούν να αναγνωστούν σε πολύ μεγαλύτερες αποστάσεις έως και εκατοντάδες μέτρα και να επικοινωνήσουν με έναν αναγνώστη ο οποίος έχει πολύ χαμηλότερη ισχύ σήματος. Οι

διαφορές ανάμεσα στις ενεργητικές και παθητικές ετικέτες παρουσιάζονται συγκεντρωτικά στον παρακάτω πίνακα όπως καταγράφηκαν από τον OECD (Πίνακας 2).

Οι ημι-παθητικές ετικέτες, είναι ένας συνδυασμός των δύο παραπάνω κατηγοριών. Πιο συγκεκριμένα, διαθέτουν μεν δική τους πηγή ενέργειας ώστε να μπορούν να τεθούν σε λειτουργία από μόνες τους όπως οι ενεργητικές ετικέτες, αλλά δεν μπορούν να ξεκινήσουν οι ίδιες την επικοινωνία με τον αναγνώστη. Χρειάζονται να λάβουν ενέργεια από τον αναγνώστη για να του αποστείλουν τα ζητούμενα δεδομένα. Έχουν μεγαλύτερο μέγεθος και κόστος από τις παθητικές ετικέτες, αλλά διαθέτουν και μεγαλύτερο χώρο αποθήκευσης δεδομένων και μπορούν να αναγνωστούν και στις μεγάλες αποστάσεις.

Πίνακας 2 Διαφορές ανάμεσα στις ενεργητικές και παθητικές ετικέτες

Πηγή: OECD (2008), OECD Policy Guidance on Radio Frequency Identification (RFID), Ministerial Meeting on the future of the meeting economy, Seoul, Korea, σελ. 26.

	ΠΑΘΗΤΙΚΕΣ	ΕΝΕΡΓΗΤΙΚΕΣ
Περιέχει μπαταρία	Όχι	Ναι
Πηγή ενέργειας	Ενέργεια μεταφέρεται από τον αναγνώστη	Ενσωματωμένη μπαταρία
Διαθεσιμότητα παροχής ενέργειας	Μόνο όταν βρίσκεται στο πεδίο του αναγνώστη	Συνεχόμενη
Απαιτούμενη ισχύς σήματος από τον αναγνώστη στην ετικέτα	Δυνατή	Χαμηλή
Διαθέσιμη ισχύς σήματος από την ετικέτα στον αναγνώστη	Χαμηλή	Δυνατή
Εμβέλεια επικοινωνίας	Μικρή (έως 3 μέτρα)	Μεγάλη (έως και πάνω από 100 μέτρα)
Διάρκεια ζωής	Πολύ μεγάλη	Περιορίζεται βάσει της ζωής της μπαταρίας
Τυπικό μέγεθος	Μικρό	Μεγάλο
Ταυτόχρονη ανάγνωση ετικετών	Εκατοντάδες ετικέτες σε απόσταση 3 μέτρων. 20 ετικέτες κινούμενες με 20 χλμ/ώρα	Χιλιάδες ετικέτες σε πάνω από 2800m^2. 20 ετικέτες κινούμενες με 160 χλμ/ώρα
Δυνατότητα αισθητήρα	Μόνο ανάγνωση και μεταφορά δεδομένων όταν είναι στο πεδίο του αναγνώστη, χωρίς ημερομηνία και χρόνο	Συνεχόμενη παρακολούθηση και καταγραφή δεδομένων περιβάλλοντος, με ημερομηνία και ώρα
Αποθήκευση δεδομένων	Μικρή χρητικότητα για ανάγνωση/εγγραφή (bytes)	Μεγάλη χρητικότητα για ανάγνωση/εγγραφή (Kbytes)
Κόστος	Μικρό (κάτω από 0.50€)	Μεγάλο

3.3.1.2. Κατηγοριοποίηση βάσει της δυνατότητας εγγραφής-ανάγνωσης

Ανάλογα με τη δυνατότητα εγγραφής-ανάγνωσης, οι ετικέτες κατηγοριοποιούνται σε αναγνώσιμες, μίας εγγραφής και επανεγγράψιμες ετικέτες. Οι αναγνώσιμες ετικέτες μπορούν μονάχα να αναγνωστούν, είναι οι πιο ευρέως διαδομένες, είναι φθηνές και είναι συνήθως παθητικές ετικέτες. Συγκεκριμένα, έχουν μικρή χωρητικότητα δεδομένων, εγγράφονται σε αυτές τα απαραίτητα δεδομένα μία φορά κατά την παραγωγή τους και έπειτα

μπορούν μόνο να αναγνωστούν απεριόριστες φορές από τους αναγνώστες. Οι ετικέτες μίας εγγραφής μετά την παραγωγή τους παρέχουν τη δυνατότητα στο χρήστη να εγγράψει πληροφορίες σε αυτές αλλά μόνο μία φορά και έπειτα μπορούν να αναγνωστούν απεριόριστες φορές από τους αναγνώστες. Τέλος, οι επανεγγράψιμες ετικέτες παρέχουν τη δυνατότητα εγγραφής, προσθήκης ή και τροποποίησης των αποθηκευμένων δεδομένων απεριόριστες φορές και γι' αυτό έχουν μεγαλύτερη χωρητικότητα δεδομένων. Προσφέρουν περισσότερα πλεονεκτήματα συγκριτικά με τις αναγνώσιμες και τις ετικέτες μίας εγγραφής, αλλά είναι και αρκετά πιο ακριβές.

Σε κάθε περίπτωση, από τη στιγμή που θα αναγνωστεί μία ετικέτα από έναν αναγνώστη ο αναγνώστης συνδέεται με ένα υπολογιστικό σύστημα και από εκεί αντλεί παραπάνω πληροφορίες σχετικά με το αντικείμενο.

3.3.1.3. Κατηγοριοποίηση βάσει της κατασκευής και της εφαρμογής τους

Ανάλογα με την κατασκευή και την εφαρμογή τους, οι ετικέτες διακρίνονται σε έξυπνες ετικέτες, γυάλινους σωλήνες, ετικέτες ενωτίου και δίσκους.

Οι έξυπνες ετικέτες είναι οι πιο ευρέως χρησιμοποιούμενες ετικέτες στη διαχείριση της εφοδιαστικής αλυσίδας. Είναι είτε χάρτινες, είτε πλαστικές πάνω στις οποίες εκτυπώνεται ο αναγνωριστικός κωδικός του αντικειμένου και εμπεριέχουν ενσωματωμένη μία ετικέτα RFID. Συνήθως είναι πλαστικά αυτοκόλλητα και προσκολλώνται πάνω στο αντικείμενο.

Εικόνα 4 Έξυπνη ετικέτα RFID

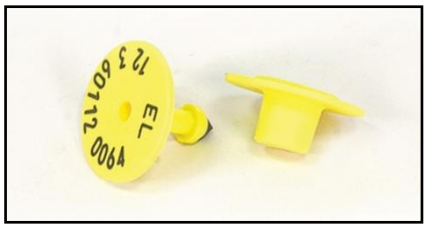
Πηγή: http://www2.cpttm.org.mo/cyberlab/rfid/intro.html.en

Οι γυάλινοι σωλήνες χρησιμοποιούνται για τον εντοπισμό κυρίως των κατοικίδιων ζώων[34] και ακόμη και των ανθρώπων. Έχουν το μέγεθος ενός κόκκου ρυζιού (12mm μήκος και 1,2mm πλάτος) και τοποθετούνται κάτω από το δέρμα με ένεση. Όταν πρόκειται για ζώα συνήθως τοποθετούνται στην περιοχή του λαιμού, ενώ όταν πρόκειται για ανθρώπους συνήθως τοποθετούνται στο χέρι ενδιάμεσα από τον αντίχειρα και το δείκτη.

Εικόνα 5 Ετικέτα γυάλινος σωλήνας RFID

Πηγή: http://www.implantable-device.com/2011/12/30/verimeds-human-implantable-verichip-patient-rfid/

Οι ετικέτες ενωτίου χρησιμοποιούνται για τον εντοπισμό των ζώων υπό εξαφάνιση και στην κτηνοτροφία από τον κτηνίατρο για την καταγραφή ιστορικών δεδομένων σχετικά με τα ζώα, όπως παρακολούθηση ασθενειών, εμβόλια και αντιβιώσεις που μπορεί να έχουν πάρει. Συνήθως τοποθετούνται στο αφτί των ζώων.



Εικόνα 6 Ετικέτα ενωτίου RFID

Πηγή: http://agroktinotrofiki.gr/simansi-zoon/

Τέλος, οι ετικέτες δίσκοι είναι στρόγγυλες πλαστικές ετικέτες με μεγάλη αντοχή και συναντώνται συχνά για τον εντοπισμό παλετών σε πραγματικό

[34] Στην Ελλάδα η ταυτοποίηση των ζώων έχει καθοριστεί βάσει Ν. 3170/2003 (ΦΕΚ 191/Α/29.7.2003).

χρόνο αλλά και στα καταστήματα λιανικής πώλησης ρούχων ως αντικλεπτικό σύστημα.

Εικόνα 7 Ετικέτα δίσκος RFID

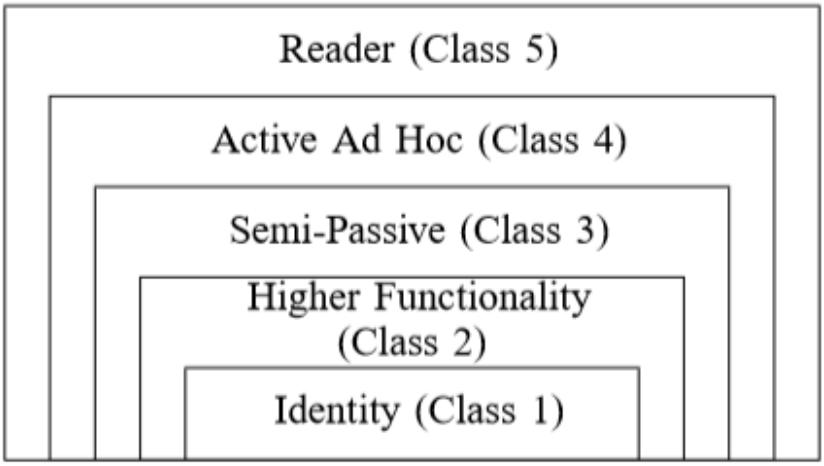
Πηγή http://www.rfidsolutionglobal.com/wp-content/uploads/2017/10/Clothes-RFID-Smart-Lock-Security-Apparel-Tag-280x315.jpg

3.3.1.4. Κατηγοριοποίηση βάσει των λειτουργικών χαρακτηριστικών

Η κατηγοριοποίηση των ετικετών βάσει των λειτουργικών τους χαρακτηριστικών έγινε από το Auto-ID Center[35]. Η κάθε κατηγορία, όπως φαίνεται και στο παρακάτω σχήμα (Εικόνα 8), αποτελεί υπερσύνολο της προηγούμενης και εμπεριέχει τα χαρακτηριστικά της δημιουργώντας έτσι μία διαβαθμισμένη ταξινόμηση[36].

[35] Η κατηγοριοποίηση αυτή αποτελεί τη βάση για την ανάπτυξη RFID προτύπων από τον οργανισμό EPC Global. Βλ. Μέρος πρώτο, υποκεφάλαιο 3.7.

[36] Engels, D. W., & Sarma, S. E. (2005). Standardization requirements within the RFID class structure framework, MIT Auto-ID Labs Technical Report, σελ. 1, διαθέσιμο στο https://www.researchgate.net/publication/267835808_Standardization_Requirements_within_the_RFID_Class_Structure_Framework



Εικόνα 8 Κατηγοριοποίηση ετικετών RFID βάσει των λειτουργικών τους χαρακτηριστικών

Πηγή: Engels, D. W., & Sarma, S. E. (2005). Standardization requirements within the RFID class structure framework, MIT Auto-ID Labs Technical Report, σελ. 2.

Η κατηγορία 1/0[37] αποτελεί τη βάση για τις υπόλοιπες κατηγορίες και επομένως σε αυτήν ανήκουν οι πιο απλές και οι πιο φθηνές ετικέτες με τα ελάχιστα λειτουργικά χαρακτηριστικά. Συγκεκριμένα, σε αυτή την κατηγορία ανήκουν αναγνώσιμες παθητικές ετικέτες οι οποίες εφόσον παρέχουν μόνο τη δυνατότητα ανάγνωσης από τους αναγνώστες, λειτουργούν κυρίως ως αναγνωριστικά. Επίσης διαθέτουν περιορισμένη μνήμη στην οποία έχουν αποθηκευμένο ένα μοναδικό αριθμό που αποτελεί την ταυτότητά τους. Τέτοιες ετικέτες είναι κατάλληλες για χρήση σε αντικείμενα, κιβώτια και παλέτες προϊόντων για την ταυτοποίησή τους κατά την κίνησή τους στην εφοδιαστική αλυσίδα.

Η κατηγορία 2[38] αποτελεί υπερσύνολο της κατηγορίας 1/0 με κάποια επιπρόσθετα λειτουργικά χαρακτηριστικά. Ειδικότερα, σε αυτή την κατηγορία ανήκουν οι επανεγγράψιμες παθητικές ετικέτες, δηλαδή οι ετικέτες οι οποίες εκτός από τη δυνατότητα ανάγνωσης παρέχουν και τη δυνατότητα επανεγγραφής.

[37] Βλ. Engels, D. W., & Sarma, S. E. (2005). Standardization requirements within the RFID class structure framework, ό.π. σελ: 2-3.
[38] Βλ. Engels, D. W., & Sarma, S. E. (2005). Standardization requirements within the RFID class structure framework, ό.π. σελ: 3-4.

Η κατηγορία 3[39] αποτελεί υπερσύνολο της κατηγορίας 2 και οι ετικέτες που ανήκουν σε αυτήν είναι οι ημι-παθητικές ετικέτες. Η σημαντικότερη διαφοροποίησή τους από τις ετικέτες της κατηγορίας 2 είναι ότι έχουν τη δική τους πηγή ενέργειας την οποία μπορούν να χρησιμοποιήσουν προκειμένου να τεθούν σε λειτουργία από μόνες τους, χωρίς την ύπαρξη αναγνώστη. Συνεπώς μπορούν να υποστηρίξουν παθητική επικοινωνία και να λειτουργήσουν ως αισθητήρες περιβάλλοντος καταγράφοντας για παράδειγμα τη θερμοκρασία και την υγρασία του περιβάλλοντος και αποθηκεύοντας αυτές τις πληροφορίες στη μνήμη τους. Σε περίπτωση που τελειώσει η δική τους πηγή ενέργειας, μπορούν να λειτουργήσουν και ως ετικέτες της κατηγορίας 2.

Η κατηγορία 4[40] αποτελεί υπερσύνολο της κατηγορίας 3 και οι ετικέτες που ανήκουν σε αυτήν είναι οι ενεργητικές ετικέτες. Δηλαδή οι ετικέτες που έχουν τη δική τους πηγή ενέργειας και μπορούν να ξεκινήσουν οι ίδιες την επικοινωνία είτε απευθείας με άλλες ενεργητικές ετικέτες που ανήκουν στην ίδια συχνότητα, είτε με αναγνώστες.

Τέλος η κατηγορία 5[41] αποτελεί υπερσύνολο όλων των υπολοίπων κατηγοριών. Στην κατηγορία αυτή ανήκουν και πάλι οι ενεργητικές ετικέτες με σημαντικότερη διαφορά από τις ενεργητικές ετικέτες της κατηγορίας 4 τη δυνατότητα λειτουργίας τους ως αναγνώστες. Συγκεκριμένα μπορούν να ενεργοποιήσουν ετικέτες από τις κατηγορίες 1/0, 2 και 3 καθώς και να επικοινωνήσουν ασύρματα με ετικέτες από την κατηγορία 4.

3.3.2. Αναγνώστες

Το δεύτερο σημαντικότερο στοιχείο ενός τυπικού συστήματος RFID είναι ο αναγνώστης (reader or interrogator) ο οποίος είναι μία ηλεκτρονική συσκευή που επικοινωνεί και ανταλλάσει πληροφορίες με τις ετικέτες και το

[39] Βλ. Engels, D. W., & Sarma, S. E. (2005). Standardization requirements within the RFID class structure framework, ό.π. σελ. 4.
[40] Βλ. Engels, D. W., & Sarma, S. E. (2005). Standardization requirements within the RFID class structure framework, ό.π. σελ. 4.
[41] Βλ. Engels, D. W., & Sarma, S. E. (2005). Standardization requirements within the RFID class structure framework, ό.π. σελ. 5.

υπολογιστικό σύστημα με τη χρήση μίας κεραίας. Η βασική του λειτουργία είναι καταρχήν είτε να στέλνει ενέργεια με τη χρήση ραδιοκυμάτων στην περίπτωση των παθητικών και ημι-παθητικών ετικετών για να τις ενεργοποιήσει[42], είτε να λαμβάνει απευθείας το σήμα στην περίπτωση των ενεργητικών ετικετών[43]. Συγκεκριμένα, αφού λάβει απάντηση από κάποια ετικέτα και λάβει, για παράδειγμα, το μοναδικό αριθμό της ετικέτας ο οποίος την ταυτοποιεί, τον αποθηκεύει στη μνήμη του. Μετέπειτα επικοινωνεί με το υπολογιστικό σύστημα είτε ασύρματα (μέσω wifi, bluethooth, κινητή τηλεφωνία), είτε ενσύρματα (μέσω τοπικού δικτύου LAN) και χρησιμοποιεί το μοναδικό αυτό αριθμό για να ανακτήσει περισσότερες πληροφορίες σχετικά με την ετικέτα. Η ενέργεια του αναγνώστη προέρχεται είτε από ενσωματωμένη μπαταρία, είτε από εξωτερική πηγή ενέργειας.

Ένα από τα σημαντικότερα πλεονεκτήματα των αναγνωστών, το οποίο έπαιξε και κρίσιμο παράγοντα στη χρήση συστημάτων RFID σε πολλές εφαρμογές, είναι η ικανότητά τους να μπορούν να επικοινωνήσουν ταυτόχρονα με περισσότερες από μία ετικέτες χωρίς να είναι απαραίτητο να βρίσκονται σε πεδίο ορατότητας. Ειδικότερα, οι αναγνώστες μπορούν να διαβάσουν ταυτόχρονα όλες τις ετικέτες που βρίσκονται στο πεδίο εκπομπής τους κερδίζοντας έτσι σημαντικό χρόνο στην ολοκλήρωση των διαδικασιών των εφαρμογών[44].

[42] Οι παθητικές ετικέτες δε διαθέτουν δική τους πηγή ενέργειας και επομένως είναι ανενεργές έως ότου λάβουν ενέργεια από τον αναγνώστη. Οι ημι-παθητικές ετικέτες διαθέτουν δική τους πηγή ενέργειας, αλλά πρέπει να λάβουν ενέργεια από τον αναγνώστη για να του αποστείλουν τα ζητούμενα δεδομένα (σχετικά με τις παθητικές και ημι-παθητικές ετικέτες βλ. Μέρος πρώτο, υποκεφάλαιο 3.3.1.1).

[43] Οι ενεργητικές ετικέτες διαθέτουν δική τους πηγή ενέργειας και επομένως έχουν τη δυνατότητα να ξεκινήσουν οι ίδιες την επικοινωνία με τον αναγνώστη (σχετικά με τις ενεργητικές ετικέτες βλ. Μέρος πρώτο, υποκεφάλαιο 3.3.1.1).

[44] Προκειμένου να μπορεί ένας αναγνώστης να επικοινωνήσει με περισσότερες από μία ετικέτες χωρίς να υπάρχει σύγκρουση έχουν προταθεί βασικές τεχνικές απομόνωσης. Δύο βασικές τεχνικές απομόνωσης που χρησιμοποιούνται είναι ο αλγόριθμος διάσχισης δυαδικού δέντρου και μία παραλλαγή του αλγορίθμου ALOHA. Για περισσότερες λεπτομέρειες βλ. Ρεκλείδης, Ε., Ριζομυλιώτης Π., Γκρίτζαλης, Στ. (2010). RFID: Απειλές κατά της Ιδιωτικότητας και Μέτρα Προστασίας, σε Λαμπρινουδάκη, Κ.-Μήτρου, Λ.-Γκρίτζαλη, Σ.-Κάτσικα,Σ., Προστασία της ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, εκδ. Παπασωτηρίου, Αθήνα, σελ: 193-220 και παραπέρα βιβλιογραφία.

Ανάλογα με την εφαρμογή τους οι αναγνώστες μπορεί να είναι σταθεροί, ολοκληρωμένοι, φορητοί και γραφείου[45]. Οι σταθεροί αναγνώστες χρησιμοποιούνται κυρίως στη βιομηχανία, είναι εγκατεστημένοι σε ένα συγκεκριμένο σημείο[46], υποστηρίζονται από εξωτερικές κεραίες και επικοινωνούν με τις ετικέτες που κινούνται μέσα στο πεδίο εκπομπής τους. Οι ολοκληρωμένοι αναγνώστες είναι υποκατηγορία των σταθερών αναγνωστών και αυτό που τους διαφοροποιεί είναι ότι έχουν την κεραία ενσωματωμένη και όχι εξωτερική. Οι φορητοί αναγνώστες (γνωστοί και ως αναγνώστες χειρός, βλ. Εικόνα 9) έχουν τη μορφή υπολογιστή παλάμης (PDA) συνήθως με χειρολαβή και είναι ιδανικοί για τη σάρωση ετικετών εν κινήσει. Διαθέτουν οθόνη και πληκτρολόγιο ώστε να μπορεί ο χρήστης να διαβάζει τα δεδομένα της ετικέτας που σκανάρει εκείνη τη στιγμή αλλά και να στέλνει εντολές στην ετικέτα. Τέλος οι αναγνώστες γραφείου συνδέονται πάνω στους προσωπικούς ηλεκτρονικούς υπολογιστές μέσω μίας θύρας USB επεκτείνοντας έτσι τις λειτουργίες των ηλεκτρονικών υπολογιστών με τη δυνατότητα σάρωσης και επομένως ανάγνωσης ή και εγγραφής ετικετών.

Εικόνα 9 Αναγνώστης χειρός RFID

Πηγή: https://www.zebra.com/us/en/products/rfid/rfid-handhelds.html

[45] Πληροφορίες σχετικά με τους αναγνώστες βλ. https://www.trinitysystems.gr/el/proionta/rfid-anagnostes/

[46] Για παράδειγμα τοποθετούνται στην είσοδο της αποθήκης για τον αυτοματοποιημένο έλεγχο των εμπορευμάτων που εισέρχονται και εξέρχονται.

3.3.3. Ενδιάμεσο λογισμικό

Όπως έχει προαναφερθεί, ο αναγνώστης αφού λάβει το μοναδικό αριθμό από μία ετικέτα, προκειμένου να ανακτήσει περισσότερες πληροφορίες σχετικά με την ετικέτα, επικοινωνεί με ένα υπολογιστικό σύστημα. Σε αυτό το στάδιο, το ενδιάμεσο λογισμικό (middleware) αποτελεί τη γέφυρα επικοινωνίας ανάμεσα στον αναγνώστη και το υπολογιστικό σύστημα και μεταφέρει τα δεδομένα στη σωστή μορφή από τον αναγνώστη προς στο υπολογιστικό σύστημα και το αντίστροφο.

Η βέλτιστη λειτουργία ενός συστήματος RFID εξαρτάται από την αποτελεσματικότητα του ενδιάμεσου λογισμικού που χρησιμοποιεί[47]. Συγκεκριμένα, το ενδιάμεσο λογισμικό είναι αυτό που βοηθάει στην αποτελεσματική ροή της πληροφορίας στο σύστημα εφόσον συνδέει τα βασικά συστατικά μέρη του συστήματος με το υπολογιστικό σύστημα στο οποίο αποθηκεύονται τελικά όλες οι πληροφορίες.

Επίσης, το ενδιάμεσο λογισμικό εκτός από δεδομένα μεταφέρει και εντολές μεταξύ του αναγνώστη και του υπολογιστικού συστήματος. Τέτοιες εντολές μπορεί να είναι είτε σχετικές με τις ετικέτες, όπως η εύρεση μίας ετικέτας, η εγγραφή δεδομένων σε μία ετικέτα και η καταστροφή μίας ετικέτας, είτε σχετικές με τον αναγνώστη, όπως η αλλαγή των ρυθμίσεων του αναγνώστη.

3.3.4. Υπολογιστικό σύστημα βάσης

Το υπολογιστικό σύστημα βάσης (back-end) αποτελεί το τελευταίο μέρος ενός συστήματος RFID. Στο υπολογιστικό σύστημα συλλέγεται, αποθηκεύεται, τίθεται υπό επεξεργασία και αναλύεται όλος ο όγκος των πληροφοριών σχετικά με τις ετικέτες που χρησιμοποιούνται σε κάθε εφαρμογή.

[47] Βλ. OECD (2008). OECD Policy Guidance on Radio Frequency Identification (RFID), Ministerial Meeting on the future of the meeting economy, Seoul, Korea, 17-18 June, σελ. 35.

Όσον αφορά τη σύνδεση των αναγνωστών με το υπολογιστικό σύστημα, οι σταθεροί αναγνώστες μπορούν να συνδεθούν και να επικοινωνήσουν με το υπολογιστικό σύστημα με τη χρήση τοπικών δικτύων (LAN). Στην περίπτωση των αναγνωστών που κινούνται σε μικρή ακτίνα, η σύνδεση με το υπολογιστικό σύστημα γίνεται με τη χρήση ασύρματης τεχνολογίας μικρής εμβέλειας, όπως wi-fi και bluetooth. Ενώ υπάρχει και η δυνατότητα σύνδεσης με τη χρήση της κινητής τηλεφωνίας σε εφαρμογές μεταφορών όπου παρακολουθείται η κίνηση των προϊόντων που φέρουν ετικέτες. Στην τελευταία περίπτωση, μπορεί επιπρόσθετα να χρησιμοποιηθεί και σύστημα εντοπισμού της γεωγραφικής θέσης αυτών των προϊόντων μέσω δορυφόρου (GPS).

3.4. Συχνότητες λειτουργίας συστημάτων RFID

Μία σημαντική παράμετρος η οποία επηρεάζει τη λειτουργικότητα ενός συστήματος RFID είναι οι συχνότητες στις οποίες εκπέμπει. Ένα σύστημα RFID μπορεί να λειτουργήσει σε πολλές διαφορετικές συχνότητες και κατ' επέκταση και σε διαφορετική ζώνη συχνοτήτων[48]. Επειδή όμως η κάθε ζώνη συχνοτήτων θέτει άλλες ικανότητες αλλά και περιορισμούς στο σύστημα, η επιλογή της κατάλληλης συχνότητας είναι σημαντικό να γίνει με βάση τις απαιτήσεις της κάθε εφαρμογής.

Παράλληλα, είναι σημαντικό να ληφθεί υπόψη και το γεγονός ότι για να μπορέσει ένα σύστημα RFID να είναι λειτουργικό σε παγκόσμιο επίπεδο, πρέπει να καθοριστούν παγκοσμίως οι συχνότητες στις οποίες θα εκπέμπει[49]. Μέχρι στιγμής, στις περισσότερες περιοχές του κόσμου έχουν καθοριστεί οι συχνότητες λειτουργίας για τα συστήματα RFID στη χαμηλή και στην υψηλή ζώνη, ενώ στην πολύ υψηλή ζώνη δεν έχει γίνει αποδεκτή ακόμη παγκοσμίως

[48] Το φάσμα συχνοτήτων είναι χωρισμένο σε τέσσερις ζώνες: τη χαμηλή ζώνη (Low frequency, 30-300 kHz), την υψηλή ζώνη (High frequency, 3-30MHz), την πολύ υψηλή ζώνη (Ultra-High frequency, 300 Mhz-3 GHz) και τα μικροκύματα (Microwaves, 2-30 GHz).

[49] Βλ. US Department of Commerce (2005), Radio Frequency Identification. Opportunities and Challenges in Implementation, Department of Commerce, Washington D.C., April 2005, σελ. 19 και Oertel, B., Wölk, M., Hilty, L. (2010). Security aspects and prospective applications of RFID systems. Federal Office for Information Security, σελ. 25.

μία μοναδική τιμή. Στο παρακάτω πίνακα (Πίνακας 3) φαίνονται οι συχνότητες λειτουργίας των συστημάτων RFID όπως έχουν οριστεί ανά τον κόσμο.

Πίνακας 3 Συχνότητες λειτουργίας συστημάτων RFID ανά τον κόσμο
Πηγή: US Department of Commerce (2005, σελ. 21)

Συχνότητες λειτουργίας συστημάτων RFID		
Ζώνες συχνοτήτων	**Συχνότητα**	**Περιοχές/Χώρες**
Χαμηλή	125–134 kHz	ΗΠΑ, Καναδάς, Ιαπωνία & Ευρώπη
Υψηλή	13.56 MHz	ΗΠΑ, Καναδάς, Ιαπωνία & Ευρώπη
Πολύ υψηλή	433.05–434.79 MHz	Ευρώπη, ΗΠΑ & Ιαπωνία (υπό εξέταση)
	865–868 MHz	Ευρώπη
	866–869 & 923–925 MHz	Νότια Κορέα
	902–928 MHz	ΗΠΑ
	952–954 MHz	Ιαπωνία
Μικροκύματα	2400–2500 & 5.725–5.875 GHz	ΗΠΑ, Καναδάς, Ιαπωνία & Ευρώπη

Επίσης, είναι αναγκαίο να οριστούν συγκεκριμένα οι συχνότητες στις οποίες θα εκπέμπει η τεχνολογία RFID[50]. Καταρχήν επειδή το φάσμα συχνοτήτων είναι συγκεκριμένο και περιορισμένο, αλλά και το πιο σημαντικό επειδή υπάρχει κίνδυνος να προκύψουν παρεμβολές με άλλα συστήματα που χρησιμοποιούν συχνότητες για να λειτουργήσουν. Τέτοια παραδείγματα άλλων συστημάτων είναι το ραδιόφωνο, η τηλεόραση, οι ασύρματοι επικοινωνίας που χρησιμοποιούν η αστυνομία και γενικότερα οι υπηρεσίες έκτακτης ανάγκης και οι συχνότητες που χρησιμοποιούν για τις θαλάσσιες και αεροναυτικές επικοινωνίες.

[50] Βλ. OECD (2008). OECD Policy Guidance on Radio Frequency Identification (RFID), ό.π. σελ. 29.

3.4.1. Χαρακτηριστικά συστημάτων RFID ανά ζώνη συχνότητας

Όπως αναφέρθηκε παραπάνω, τα συστήματα RFID λειτουργούν σε διάφορες συχνότητες και η επιλογή της καταλληλότερης συχνότητας πρέπει να γίνεται σύμφωνα με τις απαιτήσεις κάθε εφαρμογής. Στον παρακάτω πίνακα παρουσιάζονται τα χαρακτηριστικά των συστημάτων RFID ανά ζώνη συχνοτήτων.

Πίνακας 4 Χαρακτηριστικά συστημάτων RFID ανά ζώνη συχνοτήτων
Πηγή: OECD (2008c, σελ. 34), OECD (2007, σελ. 18), Dressen D. (2004)

Παράμετροι	Χαμηλή Συχνότητα	Υψηλή Συχνότητα	Πολύ υψηλή Συχνότητα	Μικροκύματα
Εύρος ανάγνωσης	έως 1.2 m	έως 1.2 m	έως 4 m	έως 15 m
Ρυθμός μετάδοσης δεδομένων	αργός	μέτριος	γρήγορος	πολύ γρήγορος
Υγρασία	καμία επίδραση	μικρή επίδραση	αρνητική επίδραση (απορρόφηση)	αρνητική επίδραση (απορρόφηση)
Μέταλλα	καμία επίδραση	καμία επίδραση	αρνητική επίδραση	αρνητική επίδραση
Οπτική επαφή	δεν απαιτείται	δεν απαιτείται	μερικές φορές απαιτείται	απαιτείται
Αποδεκτή συχνότητα παγκοσμίως	ναι	ναι	σε μερικές περιοχές (EU/ΗΠΑ)	σε μερικές περιοχές (εκτός EU)
Κόστος	μικρό ($0.50-$5)	μικρό ($0.23-$10)	μεγάλο ($25-$100+)	μεγάλο ($0.13-$25)
Ετικέτες	παθητικές	παθητικές	παθητικές και ενεργητικές	παθητικές και ενεργητικές

Όσον αφορά τα συστήματα RFID που εκπέμπουν στη ζώνη χαμηλών συχνοτήτων, το εύρος ανάγνωσής τους είναι μικρό και ο ρυθμός μετάδοσης των δεδομένων αργός. Έχουν όμως το πλεονέκτημα ότι έχουν μικρό κόστος, δεν απαιτείται οπτική επαφή μεταξύ της ετικέτας και του αναγνώστη και δεν επηρεάζονται από την υγρασία και τα μεταλλικά αντικείμενα, γεγονός που τα καθιστά κατάλληλα για χρήση σε εφαρμογές όπως την ταυτοποίηση ζώων[51] και την παρακολούθηση αντικειμένων με υψηλή περιεκτικότητα σε νερό, όπως τα φρούτα και τα λαχανικά.

[51] Για την ταυτοποίηση των ζώων χρησιμοποιείται η ετικέτα τύπου ηλεκτρονικού στομαχικού βόλου, δηλαδή βόλου που καταπίνουν τα ζώα και παραμένει στο στομάχι τους για τον εντοπισμό και την ηλεκτρονική τους ταυτοποίηση.

Τα συστήματα RFID που εκπέμπουν στη ζώνη υψηλών συχνοτήτων είναι μία εξίσου οικονομική λύση με παρόμοια και λίγο καλύτερα χαρακτηριστικά με αυτά των συστημάτων της ζώνης χαμηλών συχνοτήτων. Παραδείγματα εφαρμογών τέτοιων συστημάτων είναι εφαρμογές για τον έλεγχο πρόσβασης σε κτίρια, στην εφοδιαστική αλυσίδα για τον εντοπισμό αντικειμένων και τη διαχείριση αποθεμάτων, στην έκδοση εισιτηρίων και στις βιβλιοθήκες για τη διαχείριση των βιβλίων.

Τα συστήματα RFID που εκπέμπουν στη ζώνη πολύ υψηλών συχνοτήτων έχουν άλλα πλεονεκτήματα και άλλους περιορισμούς με τις δύο προηγούμενες περιπτώσεις. Σε αντίθεση λοιπόν με τα προαναφερθέντα, έχουν αρκετά μεγαλύτερο εύρος ανάγνωσης και γρηγορότερο ρυθμό μετάδοσης των δεδομένων. Επιδρά όμως αρνητικά σε αυτά η υγρασία και η παρουσία μεταλλικών αντικειμένων, μερικές φορές απαιτείται οπτική επαφή μεταξύ της ετικέτας και του αναγνώστη και το μεγαλύτερό τους μειονέκτημα είναι ότι δεν υπάρχει ακόμη μία συγκεκριμένη συχνότητα σε αυτό το φάσμα αποδεκτή παγκοσμίως. Παράδειγμα εφαρμογής ενός τέτοιου συστήματος είναι η παρακολούθηση παλετών και κοντέινερ.

Τέλος, τα συστήματα RFID που εκπέμπουν στη ζώνη συχνοτήτων των μικροκυμάτων έχουν ακόμη μεγαλύτερο εύρος ανάγνωσης και ο ρυθμός μετάδοσης των δεδομένων είναι πολύ γρήγορος. Είναι όμως ακριβά και η απόδοσή τους δεν είναι καλή υπό την παρουσία υγρασίας και μεταλλικών αντικειμένων. Παράδειγμα εφαρμογής ενός τέτοιου συστήματος είναι η αυτόματη πληρωμή διοδίων.

3.4.2. Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων

Οι όροι με τους οποίους πρέπει να χρησιμοποιούνται οι μεμονωμένες συχνότητες ή οι ζώνες συχνοτήτων, καθορίζονται από την αντίστοιχη διοικητική αρχή που έχει ορίσει η κάθε χώρα για τη ρύθμιση των ηλεκτρονικών επικοινωνιών. Στην περίπτωση της Ελλάδος, η Εθνική Επιτροπή

Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)[52,53] είναι αυτή η οποία εποπτεύει και ελέγχει την αγορά των ηλεκτρονικών επικοινωνιών.

Η ΕΕΤΤ, λαμβάνοντας υπόψη την απόφαση της Επιτροπής 2006/804/ΕΚ της 23ης Νοεμβρίου 2006 σχετικά με την εναρμόνιση του ραδιοφάσματος για συσκευές ταυτοποίησης ραδιοσυχνοτήτων (RFID) που λειτουργούν στη ζώνη πολύ υψηλών συχνοτήτων (UHF)[54], συμπεριλαμβάνει τις εφαρμογές RFID στον πίνακα κατανομής ζωνών συχνοτήτων, όπως ορίστηκε στον Εθνικό Κανονισμό Κατανομής Ζωνών Συχνοτήτων (ΕΚΚΖΣ)[55]. Και μετέπειτα, με τον Κανονισμό Όρων Χρήσης Μεμονωμένων Ραδιοσυχνοτήτων ή Ζωνών Ραδιοσυχνοτήτων (ΦΕΚ 1713/Β/26-6-2014)[56] καθορίζει ότι η χρήση των συσκευών μικρής εμβέλειας (χαμηλή και υψηλή ζώνη συχνοτήτων) που χρησιμοποιούνται για εφαρμογές ραδιοσυχνικής αναγνώρισης (RFID) δεν απαιτεί χορήγηση ατομικού δικαιώματος χρήσης ραδιοσυχνοτήτων, εφόσον ο κίνδυνος πρόκλησης επιζήμιων παρεμβολών είναι αμελητέος (βλ. Παράρτημα Κανονισμού, σελ. 22187 και 22192).

3.5. Επίπεδο ισχύος

Το επίπεδο ισχύος είναι ένας περιοριστικός παράγοντας όσον αφορά την εμβέλεια του σήματος που θα εκπέμπει ένα σύστημα RFID. Ταυτόχρονα

[52] Περισσότερες πληροφορίες σχετικά με την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) διαθέσιμες στο https://www.eett.gr/opencms/opencms/EETT/EETT/AboutEETT/.

[53] Οι αρμοδιότητες της ΕΕΤΤ καθορίζονται στο άρθρο 12 του Ν.4070/2012 (ΦΕΚ 82/Α/10-04-2012) για τις ηλεκτρονικές επικοινωνίες (όπως τροποποιήθηκε με το Ν.4146/2013, ΦΕΚ 90 Α/18-4-2013, το Ν.4313/2014, ΦΕΚ 261 Α/17-12-2014 και το Ν. 4339/2015, ΦΕΚ 133 Α/29-10-2015), διαθέσιμος στο https://www.eett.gr/opencms/export/sites/default/admin/downloads/telec/elliniki_nomothesia/nomoi/N4070-2012.pdf

[54] Βλ. Απόφαση της Επιτροπής της 23ης Νοεμβρίου 2006 σχετικά με την εναρμόνιση του ραδιοφάσματος για συσκευές ταυτοποίησης ραδιοσυχνοτήτων (RFID) που λειτουργούν στη ζώνη υπερυψηλών συχνοτήτων (UHF) [κοινοποιηθείσα υπό τον αριθμό Ε (2006) 5599] (2006/804/ΕΚ), Επίσημη Εφημερίδα της ΕΕ αριθ. L 329/64 της 25.11.2006, διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32006D0804&from=EN.

[55] Ο Εθνικός Κανονισμός Κατανομής Ζωνών Συχνοτήτων (ΕΚΚΖΣ) είναι διαθέσιμος στο https://www.eett.gr/opencms/export/sites/default/admin/downloads/telec/elliniki_nomothesia/ypourgikes_apofaseis/FEK105_B_EKKZS.pdf. Βλ. πίνακα κατανομής ζωνών συχνοτήτων στη σελ. 1136. Επίσης βλ. Αλεξανδροπούλου–Αιγυπτιάδου, Ε., Μαυρίδης, Ι. (2007). Η Προστασία των Προσωπικών Δεδομένων.., ό.π. σελ: 495.

[56] Βλ. Κανονισμός Όρων Χρήσης Μεμονωμένων Ραδιοσυχνοτήτων ή Ζωνών Ραδιοσυχνοτήτων, ΦΕΚ 1713/Β/26-6-2014, διαθέσιμο στο https://www.eett.gr/opencms/export/sites/default/EETT/Electronic_Communications/Radio_Communications/Rigths_Of_Use/FEK1713_26-6-14.pdf.

λοιπόν με τον καθορισμό των συχνοτήτων λειτουργίας των συστημάτων RFID, κρίνεται αναγκαίο να οριστεί και το επίπεδο ισχύος στο οποίο θα λειτουργεί ένα σύστημα RFID.

Όσο μεγαλύτερο είναι το επίπεδο ισχύος, τόσο μεγαλύτερη είναι και η εμβέλεια του σήματος που εκπέμπει το σύστημα επιτυγχάνοντας μεγαλύτερο εύρος ανάγνωσης και πιο καθαρό σήμα χωρίς εξωτερικούς θορύβους. Όμως το μεγάλο επίπεδο ισχύος έχει αρνητικές επιπτώσεις στην υγεία των ανθρώπων κυρίως όταν βρίσκονται κοντά στην κεραία του συστήματος.

Για την προστασία της υγείας των ανθρώπων οι αντίστοιχες αρμόδιες διοικητικές αρχές της κάθε χώρας θέτουν επιτρεπόμενα όρια στα επίπεδα ακτινοβολίας ισχύος από τις κεραίες των συστημάτων για κάθε συχνότητα λειτουργίας, περιορίζοντας όμως έτσι τους κατασκευαστές και κάνοντας ακόμη δυσκολότερη την επίτευξη της εναρμονισμένης λειτουργίας τους σε παγκόσμιο επίπεδο. Διότι πέρα από την ίδια συχνότητα λειτουργίας τους, που αναφέρθηκε σε παραπάνω υποκεφάλαιο (βλ. Μέρος πρώτο, υποκεφάλαιο 3.4), για να είναι ένα σύστημα λειτουργικό σε παγκόσμιο επίπεδο, πρέπει ταυτόχρονα να έχει και το ανάλογο επίπεδο ισχύος.

3.6. Πρότυπα ISO για τα συστήματα RFID

Ο ISO είναι ένας ανεξάρτητος, μη κυβερνητικός διεθνής οργανισμός τυποποίησης (International Organization for Standardization, ISO) ο οποίος εξειδικεύεται στη δημιουργία προτύπων για την τυποποίηση των λειτουργικών χαρακτηριστικών προϊόντων σε όλους τους τομείς της βιομηχανίας. Προκειμένου να τονιστεί η επιρροή του ISO αξίζει να αναφερθεί ότι μέχρι σήμερα έχει δημοσιεύσει 22.047 διεθνή πρότυπα και έγγραφα[57] τα οποία χρησιμοποιούνται από τις βιομηχανίες κατά βούληση.

Σκοπός του ISO είναι η χρήση των ίδιων προδιαγραφών από τους κατασκευαστές τεχνολογιών σε όλο τον κόσμο για την ανάπτυξη των τεχνολογιών με τέτοιο τρόπο ώστε να είναι εφικτό να μπορούν να

[57] Περισσότερες πληροφορίες σχετικά με τον οργανισμό ISO βλ. https://www.iso.org/about-us.html.

χρησιμοποιηθούν παγκοσμίως. Ταυτόχρονα, με την εφαρμογή προτύπων ISO κατά την ανάπτυξη ενός συστήματος, μειώνονται τα λειτουργικά λάθη και αυξάνεται η εμπιστοσύνη των καταναλωτών, με αποτέλεσμα να αποκτά το σύστημα ακόμη μεγαλύτερο ανταγωνιστικό πλεονέκτημα στην αγορά.

Έτσι και με την τεχνολογία RFID, ο ISO έχει δημιουργήσει ένα μεγάλο αριθμό προτύπων ανά ζώνη συχνοτήτων για τις διάφορες εφαρμογές προκειμένου να διασφαλιστεί η διαλειτουργικότητα των διαφόρων συστατικών μερών των συστημάτων RFID που κατασκευάζονται από διαφορετικούς κατασκευαστές σε όλο τον κόσμο. Στον παρακάτω πίνακα (Πίνακας 5) παρουσιάζονται τα κυριότερα πρότυπα ISO σχετικά με τα συστήματα RFID και τις εφαρμογές τους.

Πίνακας 5 Κυριότερα πρότυπα ISO για τα συστήματα RFID
Πηγή: OECD (2008c, σελ. 70), OECD (2007, σελ. 13)

Πρότυπα ISO	
ISO 11784 ISO 11785 ISO 14223	για τον εντοπισμό και την ταυτοποίηση ζώων
ISO 10536	ανέπαφες έξυπνες κάρτες εγγύτητας με απόσταση ανάγνωσης μικρότερου του 1cm
ISO 14443	ανέπαφες έξυπνες κάρτες εγγύτητας με απόσταση ανάγνωσης τα 10cm, συνήθως με μικροεπεξεργαστή
ISO 15693	ανέπαφες έξυπνες κάρτες εγγύτητας με απόσταση ανάγνωσης το 1m, συνήθως χωρίς μικροεπεξεργαστή
ISO 10374	για την αυτόματη ταυτοποίηση κοντέινερ
ISO 18000	σειρά προτύπων διεπαφής για την αυτόματη αναγνώριση και διαχείριση σε επίπεδο αντικειμένου

Όπως φαίνεται από τον παραπάνω πίνακα, οι τρεις μεγάλες κατηγορίες εφαρμογών για τις οποίες έχουν αναπτυχθεί τα κυριότερα πρότυπα ISO είναι η αυτόματη αναγνώριση των ζώων, οι ασύρματες έξυπνες κάρτες και η διαχείριση της εφοδιαστικής αλυσίδας.

Όσον αφορά την αυτόματη αναγνώριση των ζώων, δηλαδή τον εντοπισμό τους και την ταυτοποίησή τους, έχουν αναπτυχθεί τρία πρότυπα ISO. Το ISO 11784 το οποίο καθορίζει τη δομή του μοναδικού κωδικού ταυτοποίησης των ζώων, το ISO 11785 το οποίο καθορίζει τα χαρακτηριστικά του πρωτόκολλου μετάδοσης ανάμεσα στην ετικέτα και τον αναγνώστη και συγκεκριμένα τον τρόπο ενεργοποίησης των ετικετών και τον τρόπο μετάδοσης των πληροφοριών και το ISO 14223 το οποίο αποτελεί επέκταση των δύο προηγούμενων προτύπων. Τέλος, και τα τρία αυτά πρότυπα αφορούν συστήματα που εκπέμπουν στη χαμηλή ζώνη συχνοτήτων.

Όσον αφορά εφαρμογές ασύρματων έξυπνων καρτών, βάσει της εμβέλειάς τους έχουν αναπτυχθεί τρία πρότυπα ISO. Το ISO 10536 το οποίο αφορά ανέπαφες έξυπνες κάρτες οι οποίες λειτουργούν σε πολύ μικρή απόσταση (μικρότερη του 1cm), το ISO 14443 το οποίο αφορά ανέπαφες έξυπνες κάρτες εγγύτητας συνήθως με μικροεπεξεργαστή και απόσταση ανάγνωσης τα 10cm[58] και το ISO 15693 το οποίο αφορά ανέπαφες έξυπνες κάρτες εγγύτητας συνήθως χωρίς μικροεπεξεργαστή και με απόσταση ανάγνωσης το 1m[59].

Τέλος, όσον αφορά τη διαχείριση της εφοδιαστικής αλυσίδας, δηλαδή τον εντοπισμό και την παρακολούθηση των αγαθών και των αποθεμάτων και συγκεκριμένα σε επίπεδο τεμαχίου, έχει αναπτυχθεί μία σειρά προτύπων (ISO 18000) η οποία καθορίζει πρότυπα για τέτοια συστήματα RFID ανάλογα με τη ζώνη συχνοτήτων στην οποία εκπέμπουν. Συγκεκριμένα, τα πρότυπα αυτής της σειράς είναι το ISO 18000-2 το οποίο αφορά ετικέτες που εκπέμπουν στη χαμηλή ζώνη συχνοτήτων, το ISO 18000-3 το οποίο αφορά ετικέτες που εκπέμπουν στην υψηλή ζώνη συχνοτήτων και ISO 18000-6 το οποίο αφορά ετικέτες που εκπέμπουν στην πολύ υψηλή ζώνη συχνοτήτων.

[58] Συγκεκριμένο παράδειγμα εφαρμογής του ISO 14443 είναι στα ηλεκτρονικά διαβατήρια (ICAO 2004b, σελ. 6 και OECD 2008c, σελ. 69).
[59] Όπως για παράδειγμα οι κάρτες ελεγχόμενης πρόσβασης (OECD 2007, σελ. 12)

3.7. Πρότυπα EPC για τα συστήματα RFID

Σε αυτή την ενότητα παρουσιάζεται ο EPC Global οργανισμός ανάπτυξης προτύπων και πώς με τη δημιουργία του EPC δικτύου μπορεί να επιτευχθεί τελικά η δημιουργία μίας παγκόσμιας εφοδιαστικής αλυσίδας η οποία θα διαμοιράζει πληροφορίες σε επίπεδο τεμαχίου, από όλους τους κατασκευαστές και σε όλους τους τομείς της βιομηχανίας.

3.7.1. EPC Global

Ο EPC Global[60] είναι ένας μη κερδοσκοπικός οργανισμός ανάπτυξης προτύπων, ο οποίος αποτελεί συνεργασία δύο κορυφαίων οργανισμών ανάπτυξης προτύπων, τον EAN International (γνωστό και ως GS1) και το Uniform Code Council (γνωστό και ως GS1 US). Δημιουργήθηκε για να πετύχει καταρχήν την τυποποίηση της τεχνολογίας του Ηλεκτρονικού Κώδικα Προϊόντος (Electronic Product Code, EPC) και την παγκόσμια υιοθέτησή της με σκοπό να εξασφαλιστεί η διαλειτουργικότητα μεταξύ προϊόντων που έχουν κατασκευαστεί από διαφορετικούς προμηθευτές ανά τον κόσμο.

Τα πρότυπα που αναπτύσσει ο EPC Global έχουν τους εξής στόχους[61]: (α) να διευκολύνουν την ανταλλαγή πληροφοριών μεταξύ των εμπόρων (β) να ενθαρρύνουν την ύπαρξη μία ανταγωνιστικής αγοράς και (γ) να προωθούν την καινοτομία.

3.7.2. EPC δίκτυο

Το EPC δίκτυο (EPC Network) δημιουργήθηκε από τον EPC Global ως η λύση στη δημιουργία μίας αποτελεσματικής παγκόσμιας εφοδιαστικής αλυσίδας, αξιοποιώντας τα οφέλη της τεχνολογίας RFID σε συνδυασμό με την τεχνολογία του Ηλεκτρονικού Κώδικα Προϊόντος (EPC). Παρέχει τα

[60] Περισσότερες πληροφορίες σχετικά με τον οργανισμό EPC Global διαθέσιμες στο http://www.gs1gt.org/productos/epc/descargas/epc.pdf

[61] Βλ. Aguirre, J. I. (2007). EPCglobal: a universal standard (Doctoral dissertation, Massachusetts Institute of Technology), σελ. 29.

απαραίτητα πρότυπα εξασφαλίζοντας την επιτυχημένη εφαρμογή τους σε όλους τους τομείς της βιομηχανίας, με αποτέλεσμα να διασφαλίζεται η παγκοσμίως αποδεκτών ανάπτυξη προϊόντων υλικού και λογισμικού.

Το EPC δίκτυο διαχειρίζεται και διαμοιράζεται πληροφορίες προϊόντων σε επίπεδο τεμαχίου, οποιουδήποτε κατασκευαστή σε όλους τους τομείς της βιομηχανίας, τυποποιημένες βάσει του Ηλεκτρονικού Κώδικα Προϊόντος (EPC). Απώτερος στόχος του δικτύου είναι η επισήμανση όλων των αντικειμένων που μετέχουν σε όλα τα στάδια της εφοδιαστικής αλυσίδας με ένα μοναδικό κωδικό, προκειμένου να συγκεντρώνονται πληροφορίες για αυτά αυτόματα, δυναμικά και σε πραγματικό χρόνο, από την παραγωγή έως και τη διανομή και από την αποθήκευση έως και την πώληση[62].

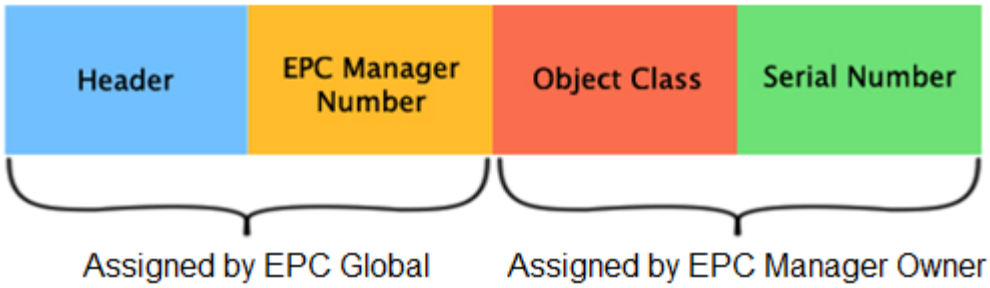
3.7.3. Ηλεκτρονικός Κωδικός Προϊόντος

Το βασικό στοιχείο του EPC δικτύου για να λειτουργήσει αποτελεσματικά είναι η χρήση της τεχνολογίας του Ηλεκτρονικού Κώδικα Προϊόντος (EPC) για τη δημιουργία ενός αναγνωριστικού κωδικού για κάθε αντικείμενο ο οποίος θα το ταυτοποιεί μοναδικά παγκοσμίως. Ο μοναδικός αυτός EPC κωδικός αποθηκεύεται στις ετικέτες των συστημάτων RFID οι οποίες προσκολλώνται ή ενσωματώνονται στα αντικείμενα και χρησιμοποιείται για τον εντοπισμό και την ταυτοποίησή τους.

Ο EPC κωδικός είναι παρόμοιος με τον UPC-A κωδικό που χρησιμοποιείται στους γραμμωτούς κώδικες (βλ. Μέρος πρώτο, Κεφάλαιο 2), αλλά με σημαντική διαφορά το γεγονός ότι χρησιμοποιείται σε επίπεδο τεμαχίου ενώ ο UPC-A κωδικός χρησιμοποιείται σε επίπεδο κατηγορίας προϊόντων. Ο EPC κωδικός λοιπόν έχει τέτοια δομή ώστε να είναι μοναδικός μεταξύ άλλων αντίστοιχων κωδικών αντικειμένων, σε όλους τους τομείς της βιομηχανίας και από οποιοδήποτε κατασκευαστή για πάντα.

[62] Βλ σχετικό κείμενο «About EPC Global», σελ. 2, διαθέσιμο στο http://www.gs1gt.org/productos/epc/descargas/epc.pdf

Όπως φαίνεται στην παρακάτω εικόνα (Εικόνα 10), ο EPC κωδικός αποτελείται από την επικεφαλίδα (header) και τον αριθμό του διαχειριστή του ηλεκτρονικού κωδικού προϊόντος (EPC Manager number) τα οποία αναθέτονται από τον EPC Global και την κλάση του αντικειμένου (object class) και τον σειριακό αριθμό (serial number) τα οποία αναθέτονται από τον διαχειριστή του ηλεκτρονικού κωδικού προϊόντος. Αναλυτικότερα, η επικεφαλίδα (header) ορίζει το μήκος, τον τύπο, τη δομή, την έκδοση και τη γενιά του EPC κωδικού, ο αριθμός του διαχειριστή του ηλεκτρονικού κωδικού προϊόντος (EPC Manager number) προσδιορίζει τον κατασκευαστή του προϊόντος, η κλάση του αντικειμένου (object class) αναφέρεται στην κατηγορία του προϊόντος και ο σειριακός αριθμός (serial number) καθορίζει το συγκεκριμένο τεμάχιο.



Εικόνα 10 Η βασική μορφή του EPC κωδικού

Πηγή: https://www.epc-rfid.info/

Αξίζει να επισημανθεί πως η μοναδικότητα του EPC κωδικού οφείλεται στο δεύτερο τμήμα του κωδικού που προσδιορίζει τον κατασκευαστή του αντικειμένου. Ο EPC Global αναθέτει ένα μοναδικό κωδικό για κάθε κατασκευαστή και έτσι οι κατασκευαστές με τη σειρά τους μπορούν να δημιουργούν νέους EPC κωδικούς (την κλάση του αντικειμένου και τον σειριακό αριθμό) χωρίς να υπάρχει ο φόβος σύγχυσης με αντίστοιχους κωδικούς από άλλους κατασκευαστές[63].

Ο EPC κωδικός μπορεί να αποτελείται από 64 έως 256 bit[64]. Η μορφή των 96-bit είναι η πιο διαδεδομένη στις εφαρμογές της εφοδιαστικής αλυσίδας

[63] Βλ. σχετικό κείμενο «About EPC Global», σελ. 3, διαθέσιμο στο http://www.gs1gt.org/productos/epc/descargas/epc.pdf

[64] Βλ. Aguirre, J. I. (2007). EPCglobal.., ό.π. σελ. 31.

επειδή είναι μία μέση και φθηνή λύση η οποία ταυτόχρονα μπορεί να αναπαράγει μεγάλο αριθμό κωδικών. Για παράδειγμα[65], με τον κωδικό 96-bit μπορούν να παραχθούν κωδικοί για 268 εκατομμύρια κατασκευαστές και κάθε κατασκευαστής θα μπορεί να ορίσει 16 εκατομμύρια τύπους προϊόντων και 68 δισεκατομμύρια σειριακούς αριθμούς για τα τεμάχια σε κάθε τύπο. Νούμερα αριθμητικά αρκετά μεγάλα για να μπορούν να καλύψουν όλα τα προϊόντα ανά κατασκευαστή παγκοσμίως για τα επόμενα χρόνια.

3.7.4. Πρότυπα EPC

Αρχικά, το 2004 εγκρίθηκαν από τον οργανισμό EPC Global τα πρότυπα πρώτης γενιάς, ονομαζόμενα EPCglobal Class-0 και Class-1 Generation-1. Εξαιτίας όμως των περιορισμών που έθεταν αυτά τα πρότυπα και της γρήγορης εξάπλωσης της τεχνολογίας RFID, την ίδια χρονιά εγκρίθηκε και το πρότυπο δεύτερης γενιάς EPCglobal Class-1 Generation-2 (γνωστό και ως Gen 2) το οποίο καθορίζει το πρωτόκολλο επικοινωνίας της διεπαφής αέρα για τις ετικέτες της κατηγορίας 1 που εκπέμπουν στη ζώνη πολύ υψηλής συχνότητας (σχετικά με τις κατηγορίες των ετικετών και τα λειτουργικά τους χαρακτηριστικά βλ. Μέρος πρώτο, υποκεφάλαιο 3.3.1.4).

Σκοπός λοιπόν των ετικετών δεύτερης γενιάς είναι να ξεπεραστούν οι περιορισμοί των ετικετών της πρώτης γενιάς και να δημιουργηθούν ετικέτες παγκοσμίως συμβατές. Συγκεκριμένα, οι ετικέτες δεύτερης γενιάς καταρχήν υπερτερούν στη χωρητικότητα μνήμης η οποία φτάνει τα 256 bits και στην επιμήκυνση του συνθηματικού στα 32 bits, σε αντίθεση με τις ετικέτες πρώτης γενιάς στις οποίες η χωρητικότητα μνήμης φτάνει τα 96 bits και το συνθηματικό τα 8 bits[66]. Έτσι λοιπόν αυξάνονται οι πιθανοί συνδυασμοί των συνθηματικών από 256 σε 4.294.967.296 και ταυτόχρονα μεγαλώνει κατά πολύ ο χρόνος υπολογισμών σε μία πιθανή brute-force attack (επίθεση ωμής

[65] Βλ. http://www.rfidjournal.com/faq/show?105
[66] Βλ. Bolan, C. (2008). A Review of the Electronic Product Code Standards for RFID Technology. In INC, σελ. 173-175.

βίας)[67] κάνοντας τελικά το σύστημα λιγότερο ευάλωτο σε τέτοιες επιθέσεις. Ταυτόχρονα αυξήθηκε και η ζώνη συχνοτήτων κατά 30 MHz, από 860 MHz – 930 MHz σε 860 MHz – 960 MHz, διευκολύνοντας έτσι την επικοινωνία των ετικετών με τους αναγνώστες.

Τέλος, το πρότυπο δεύτερης γενιάς, πέρα από παγκόσμια διαλειτουργικότητα, υπόσχεται ταχύτερο ρυθμό ανάγνωσης ετικετών έως και 10 φορές, μικρότερο μέγεθος της ετικέτας έως και 20%, μεγαλύτερη αξιοπιστία, καλύτερους αλγόριθμους ανάγνωσης, κρυπτογράφηση του κωδικού πρόσβασης και δυνατότητα θανάτωσης της ετικέτας και όχι μόνο απενεργοποίησης αυτής, όπως στα πρότυπα πρώτης γενιάς[68].

4. Σύγκριση της τεχνολογίας RFID με το γραμμωτό κώδικα

Όπως έχει ήδη προαναφερθεί, οι γραμμωτοί κώδικες και η τεχνολογία RFID είναι τεχνολογίες αυτόματης αναγνώρισης. Και στις δύο περιπτώσεις οι ετικέτες τους περιέχουν δεδομένα, συνήθως ένα μοναδικό αριθμό ο οποίος μπορεί να αναγνωστεί από ειδικούς αναγνώστες, και βασίζονται σε ένα υπολογιστικό σύστημα που συνδέεται σε μία βάση δεδομένων προκειμένου να ανακτήσουν τις σχετικές με το προϊόν πληροφορίες[69]. Παρόλο όμως που και οι δύο τεχνολογίες ανήκουν στην ίδια κατηγορία, παρουσιάζουν αρκετές διαφορές (Πίνακας 6).

[67] Με τον όρο brute-force attack εννοείται η επίθεση στην ετικέτα κατά την οποία χρησιμοποιούνται όλοι οι πιθανοί συνδυασμοί για να βρεθεί ο κωδικός της και να διαβαστεί το περιεχόμενό της.
[68] Βλ. Porter, L. (2005). The Gen 2 Standard: What Is It, and What Does It Mean?. Paxar Corporation, σελ. 2.
[69] Βλ. Gaukler, G., Seifert, R.W. (2007). Applications of RFID in supply chains, chapter 2 in Trends in supply chain Design and Management: Technologies and Methodologies, Edited by Hosang Jung, Frank Chen, Bongju Jeong, Springer London Ltd., σελ. 3 και Nikita, M. (2012). RFID in the Supply Chain and the Privacy Concernsό.π., σελ. 1215.

Πίνακας 6 Σύγκριση της τεχνολογίας RFID με το γραμμωτό κώδικα

Χαρακτηριστικά	Barcode	RFID
Οπτική επαφή	Απαιτείται οπτική επαφή	Δεν απαιτείται οπτική επαφή
Ρυθμός ανάγνωσης	Μία ετικέτα τη φορά	Ταυτόχρονα πολλές ετικέτες
Αναγνώριση	Ανά τύπο αντικειμένου	Ανά τεμάχιο
Εμβέλεια	Από χιλιοστά μέχρι κάποια εκατοστά	Μερικά εκατοντάδες μέτρα, ανάλογα το είδος της ετικέτας
Ανθρώπινο δυναμικό	Χρειάζεται ανθρώπινη παρέμβαση	Γίνονται όλα αυτοματοποιημένα
Δυνατότητα επανεγγραφής	Δεν είναι εφικτή	Είναι εφικτή ακόμη και σε πραγματικό χρόνο
Μνήμη	Περιορισμένη	Μεγάλη
Διάρκεια ζωής	Δεν μπορούν να επαναχρησιμοποιηθούν	Μπορούν να επαναχρησιμοποιηθούν
Ανθεκτικότητα	Χαμηλή, απαιτούν καθαρό περιβάλλον και δεν μπορούν να διαβαστούν εάν φθαρούν	Υψηλή
Κόστος	Χαμηλό	Υψηλό
Ασφάλεια	Μικρή προστασία	Υψηλή προστασία

Οι σημαντικότερες διαφορές των δύο αυτών τεχνολογιών[70] οι οποίες ταυτόχρονα αποτελούν και τα πια ανταγωνιστικά πλεονεκτήματα της τεχνολογίας RFID, είναι πως όταν χρησιμοποιείται η τεχνολογία RFID η αναγνώριση των αντικειμένων γίνεται σε επίπεδο τεμαχίου, δεν απαιτείται οπτική επαφή του αναγνώστη με το αντικείμενο και ταυτόχρονα δίνεται η δυνατότητα να αναγνωστούν από έναν αναγνώστη πολλές ετικέτες ταυτόχρονα οι οποίες βρίσκονται στην εμβέλειά του[71]. Έτσι, μειώνεται η ανθρώπινη παρέμβαση άρα και τα ανθρώπινα λάθη και επομένως μειώνεται και ο χρόνος ολοκλήρωσης των εργασιών. Σε αντίθεση με τις ετικέτες των γραμμωτών κωδικών στις οποίες η αναγνώριση γίνεται σε επίπεδο κατηγορίας προϊόντων, απαιτούν οπτική επαφή με το σαρωτή σε απόσταση μερικών εκατοστών και μπορεί να αναγνωστεί μόνο μία ετικέτα ανά σάρωση.

Επίσης, οι ετικέτες RFID έχουν μεγαλύτερη μνήμη συγκριτικά με αυτές των γραμμωτών κωδικών με αποτέλεσμα να επιτρέπουν την αποθήκευση

[70] Βλ. Katina, M., McCathie, L. (2005). The pros and cons of RFID in Supply Chain Management, Proceedings of the International Conference on Mobile Business (ICMB'05), IEEE Computer Society, σελ. 623 και Nikita, M. (2012). RFID in the Supply Chain and the Privacy Concernsό.π., σελ. 1215.
[71] Βλ. White, G., Gardiner, G., Prabhakar, G. P., & Abd Razak, A. (2007). A comparison of barcoding and RFID technologies in practice. Journal of information, information technology and organizations, Vol. 2, σελ. 128.

περισσότερων δεδομένων και σε ορισμένες περιπτώσεις ανάλογα με το είδος της ετικέτας να παρέχουν τη δυνατότητα επανεγγραφής ή ενημέρωσης των αποθηκευμένων σε αυτές δεδομένων ακόμη και σε πραγματικό χρόνο (σχετικά με τις κατηγορίες ετικετών RFID βάσει της δυνατότητας ανάγνωσης-εγγραφής βλ. Μέρος πρώτο, υποκεφάλαιο 3.3.1.2). Παράλληλα, οι ετικέτες RFID μπορούν να λειτουργήσουν και ως αισθητήρες περιβάλλοντος καταγράφοντας και αποθηκεύοντας στη μνήμη τους δεδομένα από το περιβάλλον, όπως τη θερμοκρασία και την υγρασία, σε όλη τη διάρκεια ζωής του προϊόντος και αργότερα όταν αναγνωστούν να αποθηκευτούν αυτές οι πληροφορίες στη βάση δεδομένων. Αυτή η ιδιότητα των ετικετών RFID είναι πολύ χρήσιμη κυρίως για την παρακολούθηση ευαίσθητων προϊόντων, όπως τα τρόφιμα[72].

Ακόμη, οι ετικέτες RFID υπερτερούν και στη διάρκεια ζωής. Συγκεκριμένα, εφόσον μπορούν να ενημερωθούν τα αποθηκευμένα σε αυτές δεδομένα μπορούν ευκολότερα να επαναχρησιμοποιηθούν. Ταυτόχρονα είναι και πιο ανθεκτικές δίνοντας τη δυνατότητα να χρησιμοποιηθούν σε περιπτώσεις όπου οι γραμμωτοί κώδικες δε μπορούν διότι εάν λερωθούν, τσαλακωθούν ή σκιστούν θα αχρηστευθούν[73].

Βέβαια η τεχνολογία RFID έχει και μειονεκτήματα συγκριτικά με τους γραμμωτούς κώδικες. Ένας από τους σημαντικότερους λόγους για τους οποίους οι ετικέτες RFID δεν έχουν αντικαταστήσει σε μεγάλη κλίμακα τις ετικέτες των γραμμωτών κωδικών είναι το κόστος της ετικέτας. Το κόστος εκτύπωσης της ετικέτας των γραμμωτών κωδικών είναι τόσο χαμηλό όσο το κόστος εκτύπωσης στον εκτυπωτή του σπιτιού, γεγονός που κάνει τις ετικέτες των γραμμωτών κωδικών πολύ ανταγωνιστικές κυρίως στο λιανικό εμπόριο όταν και το κόστος του ίδιου του προϊόντος είναι πολύ χαμηλό.

Επίσης, μεταλλικές επιφάνειες και υγρά δυσχεραίνουν την ανάγνωση των ετικετών RFID που εκπέμπουν κυρίως στη ζώνη πολύ υψηλών

[72] Βλ. Psion Teklogix (2004). Understanding RFID and Associated Applications, σελ. 4, online at http://barcodingworks.com//?module=file&act=procFileDownload&file_srl=834&sid=f4c018c2525553c93e3b669d3ddd518d.

[73] Στην περίπτωση των γραμμωτών κωδικών δεν μπορεί να χρησιμοποιηθεί κάποιο προστατευτικό κάλυμμα διότι απαιτείται οπτική επαφή με τον σαρωτή προκειμένου να αναγνωστούν.

συχνοτήτων. Βέβαια και σε τέτοιες περιπτώσεις, για παράδειγμα την αναγνώριση αντικειμένων με υψηλή περιεκτικότητα σε νερό όπως τα φρούτα και τα λαχανικά, μπορούν να χρησιμοποιηθούν ετικέτες RFID που εκπέμπουν στη ζώνη χαμηλών συχνοτήτων με το μειονέκτημα ότι το εύρος ανάγνωσής τους είναι μικρότερο και ο ρυθμός μετάδοσης των δεδομένων αργός (βλ. Μέρος πρώτο, υποκεφάλαιο 3.4.1).

Ένα ακόμη μειονέκτημα της τεχνολογίας RFID το οποίο είναι μεγάλης σημασίας και καθυστερεί σημαντικά την εξάπλωσή της είναι τα προβλήματα εμπιστοσύνης των καταναλωτών σε θέματα ιδιωτικότητας, τα οποία θα μελετηθούν εκτενώς παρακάτω. Συγκεκριμένα, το μεγαλύτερο πλεονέκτημα της τεχνολογίας RFID, δηλαδή η δυνατότητα ανάγνωσης χωρίς οπτική επαφή και από απόσταση ανά πάσα στιγμή χωρίς τη γνώση των καταναλωτών, δημιουργεί ανασφάλεια και εγείρει σημαντικά ερωτήματα σχετικά με την παραβίαση της ιδιωτικότητας.

5. Παραδείγματα εφαρμογών της τεχνολογίας RFID

Η τεχνολογία RFID ήδη μέχρι σήμερα εφαρμόζεται και χρησιμοποιείται με επιτυχία σε πληθώρα εφαρμογών και σε διαφορετικούς τομείς[74]. Προκειμένου λοιπόν να κατηγοριοποιηθεί το μεγάλο αυτό εύρος των εφαρμογών, σε αυτό το κεφάλαιο ομαδοποιούνται οι εφαρμογές ανά κατηγορία φορέων των ετικετών. Συγκεκριμένα, ανάλογα με τα χαρακτηριστικά που έχουν κάθε φορά οι ετικέτες (σχετικά με την κατηγοριοποίηση των ετικετών βλ. Μέρος πρώτο, υποκεφάλαιο 3.3.1) προορίζονται για άλλη χρήση και οι φορείς των ετικετών μπορεί να είναι είτε αντικείμενα, είτε ζώα, είτε ο ίδιος ο άνθρωπος.

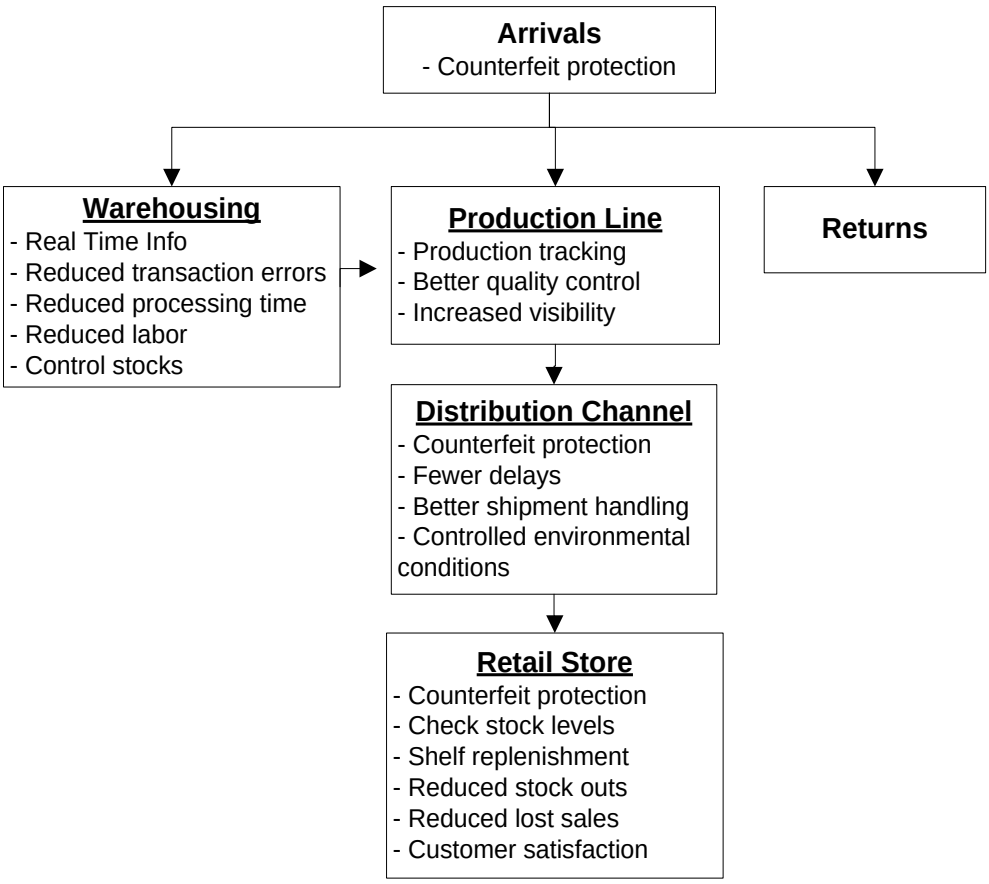
[74] Σχετικά με τις εφαρμογές της τεχνολογίας RFID στους διάφορους τομείς βλ. Ilie-Zudor, E., Kemény, Z., Van Blommestein, F., Monostori, L., Van Der Meulen, A. (2011). A survey of applications and requirements of unique identification systems and RFID techniques, Computers in Industry, 62 (3), pp. 227-252, Ahsan, K., Shah, H., Kingston, P. (2010). RFID applications: An introductory and exploratory study, International Journal of Computer Science Issues, 7 (1), No. 3, διαθέσιμο στο https://arxiv.org/ftp/arxiv/papers/1002/1002.1179.pdf, Domdouzis, K., Kumar, B., Anumba, C. (2007). Radio-Frequency Identification (RFID) applications: A brief introduction. Advanced Engineering Informatics, 21(4), 350-355, doi: 10.1016/j.aei.2006.09.001.

5.1. Φορείς αντικείμενα

Στη σημερινή εποχή, το μεγαλύτερο εύρος εφαρμογών της τεχνολογίας RFID εντοπίζεται κυρίως στην αναγνώριση των αντικειμένων και συγκεκριμένα στη βιομηχανία. Το πιο χαρακτηριστικό παράδειγμα είναι η εκτεταμένη χρήση της τεχνολογίας στη διαχείριση της εφοδιαστικής αλυσίδας για τον εντοπισμό αντικειμένων καθ' όλη τη διαδρομή τους και μάλιστα σε επίπεδο τεμαχίου (βλ. Μέρος τρίτο, Κεφάλαιο 3). Δηλαδή, με τη βοήθεια της τεχνολογίας RFID εντοπίζεται καταρχήν σε πραγματικό χρόνο η πρώτη ύλη από τη στιγμή που εισέρχεται στην εφοδιαστική αλυσίδα και κατά την αποθήκευσή της και αργότερα εντοπίζονται τα τελικά προϊόντα κατά την παραγωγή και τη διανομή τους στα καταστήματα λιανικής πώλησης. Μετέπειτα, στα καταστήματα λιανικής πώλησης διενεργείται ευκολότερη διαχείριση και οργάνωση των εμπορευμάτων με στόχο να είναι διαθέσιμο στα ράφια των καταστημάτων για τους πελάτες το σωστό προϊόν, στη σωστή θέση και στο σωστό χρόνο. Επομένως, με τη βοήθεια της τεχνολογίας RFID ελέγχονται πάντοτε σε πραγματικό χρόνο τα αποθέματα, βελτιστοποιείται και επιταχύνεται η γραμμή παραγωγής, μειώνονται τα ανθρώπινα λάθη και επομένως και το λειτουργικό κόστος και τελικά επιτυγχάνεται η ικανοποίηση του καταναλωτή στο μέγιστο, γεγονός που επισημαίνει και την επιτυχημένη διαχείριση της εφοδιαστικής αλυσίδας[75].

Η πληθώρα των πλεονεκτημάτων που προκύπτουν από την εφαρμογή της τεχνολογίας RFID στη διαχείριση της εφοδιαστικής αλυσίδας (βλ. Εικόνα 11) έχει ως αποτέλεσμα να τείνει να αντικαταστήσει το γραμμωτό κώδικα. Επίσης έχει αναπτυχθεί η ISO 18000 σειρά προτύπων (βλ. Μέρος πρώτο, υποκεφάλαιο 3.6) για την αποτελεσματικότερη διαχείριση της εφοδιαστικής αλυσίδας και παράλληλα έχει δημιουργηθεί το EPC δίκτυο (βλ. Μέρος πρώτο, υποκεφάλαιο 3.7.2) με στόχο τη δημιουργία μίας παγκόσμιας εφοδιαστικής αλυσίδας η οποία θα διαμοιράζεται πληροφορίες σε επίπεδο τεμαχίου από όλους τους κατασκευαστές και σε όλους τους τομείς της βιομηχανίας.

[75] Βλ. Nikita, M. (2012). RFID in the Supply Chain and the Privacy Concerns, ό.π..



Εικόνα 11 Πλεονεκτήματα της τεχνολογίας RFID στην εφοδιαστική αλυσίδα

Πηγή: Nikita, M. (2012). RFID in the Supply Chain and the Privacy Concerns, in Bottis, M., Alexandropoulou,E., Iglezakis,I., (edit.). Values and Freedoms in Modern Information Law & Ethics, Proceedings of the 4th International Conference of Information Law and Ethics, University of Macedonia, 20-22 May 2011, ed. Nomiki Bibliothiki Group, Athens 2012, σελ. 1218.

Αντίστοιχα, σε επίπεδο αναγνώρισης αντικειμένων, η τεχνολογία RFID εφαρμόζεται και στη φαρμακοβιομηχανία[76] στην οποία πέρα από τη διαχείριση της εφοδιαστικής αλυσίδας χρησιμοποιείται και για τη συντήρηση των φαρμάκων[77], τον εντοπισμό ληγμένων φαρμάκων αλλά και τον εντοπισμό

[76] Αναφορικά με την εφαρμογή της τεχνολογίας RFID στη φαρμακοβιομηχανία βλ. Coustasse, A., Kimble, C. A., Stanton, R. B., Naylor, M. (2016). Could the Pharmaceutical Industry Benefit from Full-Scale Adoption of Radio-Frequency Identification (RFID) Technology with New Regulations?, Perspectives in health information management, 13 (Fall), διαθέσιμο στο https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5075230/.

[77] Υπάρχουν ετικέτες οι οποίες μπορούν να λειτουργήσουν ως αισθητήρες περιβάλλοντος και να καταγράφουν δεδομένα από το περιβάλλον, όπως τη θερμοκρασία και την υγρασία, σε όλη τη διάρκεια ζωής του προϊόντος που τις φέρουν. Αυτή τους η ιδιότητα μπορεί να χρησιμεύσει στην περίπτωση των φαρμάκων τα οποία χρήζουν ιδιαίτερη φροντίδα στον τρόπο αποθήκευσης και συντήρησης.

απομιμήσεων. Επίσης, στις βιβλιοθήκες[78] αλλά και στις διάφορες δημόσιες υπηρεσίες χρησιμοποιείται η τεχνολογία RFID σε επίπεδο εγγράφων ως σύστημα εντοπισμού αυτών[79]. Ο έγκαιρος εντοπισμός των εγγράφων είναι προαπαιτούμενο για την εύρυθμη λειτουργία των υπηρεσιών μειώνοντας τη γραφειοκρατία και το χρόνο διεκπεραίωσης των υποθέσεων και ταυτόχρονα εξασφαλίζοντας τη βιωσιμότητα των εγγράφων, την αποφυγή περιπτώσεων απώλειας εξαιτίας παρατοποθέτησης και την αποτροπή εσκεμμένων διαρροών[80].

Άλλες εφαρμογές όπου η τεχνολογία RFID χρησιμοποιείται για την αναγνώριση και τον εντοπισμό αντικειμένων είναι ο χειρισμός των αποσκευών από τις αεροπορικές εταιρείες, η ανακύκλωση, η μεταφορά των αποβλήτων, οι αυτοματοποιημένες πληρωμές του αντιτίμου από τα διερχόμενα οχήματα στα διόδια, ο έλεγχος γνησιότητας των χαρτονομισμάτων καθώς και πολλές άλλες.

5.2. Φορείς άνθρωποι

Όσον αφορά περιπτώσεις όπου φορέας της τεχνολογίας RFID είναι ο άνθρωπος, η τεχνολογία RFID χρησιμοποιείται καταρχήν για τον έλεγχο πρόσβασης των ανθρώπων σε κτίρια και εγκαταστάσεις, όπως στα αεροδρόμια, στα εργαστήρια και στο χώρο εργασίας. Πέρα από τον απλό έλεγχο πρόσβασης ενός ανθρώπου σε μία ελεγχόμενη περιοχή με τη βοήθεια

[78] Αναφορικά με την εφαρμογή της τεχνολογίας RFID στις βιβλιοθήκες βλ. Coyle, K. (2005). Management of RFID in Libraries, The Journal of Academic Librarianship, 31(5), pp. 486-489, διαθέσιμο στο http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.454.9531&rep=rep1&type=pdf

[79] Ένα από τα χαρακτηριστικότερα παραδείγματα χρήσης συστήματος εντοπισμού εγγραφών είναι αυτό του Florida State University , όπου εγκαταστάθηκε ένα τέτοιο σύστημα στα Offices of Sponsored Research Services and Sponsored Research Accounting Services με σκοπό τη βελτιστοποίηση διαχείρισης των 3.500 φακέλων που επί καθημερινής βάσης διαχειριζόταν τα δύο γραφεία. Βλ. O' Connor, M. C. (2006). RFID Brings Order to a Chaotic Office, RFID Journal, RFID Journal LLC, διαθέσιμο στο http://www.rfidjournal.com/articles/view?2374 και Μυλώση Μ., Γιαννουκάκου Αι., Νικήτα Μ. (2013). Ιδιωτικότητα και Διαφάνεια στη Δημόσια Διοίκηση: προσωπικά δεδομένα και διάχυση, Νομικές και Κοινωνικές Προεκτάσεις του Διαδικτύου σήμερα, Πανελλήνιο Συνέδριο, Νομική Βιβλιοθήκη, Θεσσαλονίκη, Ιούνιος 2013, σελ. 190.

[80] Βλ. Μυλώση, Μ., Γιαννουκάκου, Α., Νικήτα, Μ. (2013). Ιδιωτικότητα και Διαφάνεια στη Δημόσια Διοίκηση: προσωπικά δεδομένα και διάχυση", Νομικές και Κοινωνικές Προεκτάσεις του Διαδικτύου σήμερα, Πανελλήνιο Συνέδριο, Νομική Βιβλιοθήκη, Θεσσαλονίκη, Ιούνιος 2013, σελ: 175-194.

μίας κάρτας η οποία θα του εξασφαλίσει την είσοδο, η τεχνολογία RFID χρησιμοποιείται και για τον έλεγχο πρόσβασης σε εγκαταστάσεις όπου απαιτείται υψηλή ασφάλεια. Συγκεκριμένα, η τεχνολογία RFID επιλέχθηκε και χρησιμοποιείται στα ηλεκτρονικά διαβατήρια[81] καθώς με τη χρήση της μπορούν τα διαβατήρια να προσφέρουν μεγαλύτερη αξιοπιστία για την αυθεντικότητά τους και ταυτόχρονα αλάνθαστη ταυτοποίηση των υποκειμένων (βλ. Μέρος τρίτο, Κεφάλαιο 2). Παρόμοιες εφαρμογές είναι η ψηφιακή ταυτότητα και το ψηφιακό δίπλωμα οδήγησης όπου η χρήση της τεχνολογίας RFID επιτυγχάνει γρήγορη και αξιόπιστη ταυτοποίηση των υποκειμένων.

Επίσης, η τεχνολογία RFID εφαρμόζεται και στους ασθενείς στο χώρο της υγείας[82]. Για παράδειγμα, ασθενείς που βρίσκονται στο χώρο των νοσοκομείων και ασθενείς με ψυχολογικά προβλήματα ή με τη νόσο Alzheimer οι οποίοι είναι ανίκανοι να φροντίσουν τον εαυτό τους επωφελούνται από τη τεχνολογία RFID είτε με εμφύτευση της ετικέτας, είτε φορώντας την στο χέρι ως βραχιόλι. Σε αυτές τις περιπτώσεις στην ετικέτα RFID αποθηκεύονται τα στοιχεία του ασθενούς, το ιατρικό ιστορικό, η φαρμακευτική αγωγή και στοιχεία επικοινωνίας κοντινού προσώπου σε περιπτώσεις εκτάκτου ανάγκης διευκολύνοντας έτσι το ιατρικό προσωπικό να εκτελέσει γρήγορα και με ασφάλεια τα ιατρικά του καθήκοντα, αξιοποιώντας αποτελεσματικά τον ιατρικό εξοπλισμό και βελτιώνοντας τη φροντίδα των ασθενών.

Άλλες εφαρμογές της τεχνολογίας RFID όπου φορέας είναι ο άνθρωπος είναι στις φυλακές και στα σχολεία για την παρακολούθηση των

[81] Αναφορικά με την εφαρμογή της τεχνολογίας RFID στα ηλεκτρονικά διαβατήρια βλ. Nikita, M., (2012). RFID chips and EU e-passports: the end of privacy?, in Bottis,M., (edit.). Privacy and Surveillance-current aspects and future perspectives, Proceedings of the Liss-Cost seminar in Athens, Greece "Surveillance in Academia", 2012 plus selected papers from ICIL 2011 and 2012 in Corfu, Greece, ed. Nomiki Bibliothiki Group, p. 199-211.

[82] Αναφορικά με την εφαρμογή της τεχνολογίας RFID στο χώρο της υγείας στους ασθενείς βλ. Prasad, N. S. R. K., Rajesh, A. (2012). RFID-based hospital real time patient management system, International Journal of Computer Trends and Technology, Vol. 3 (3), pp. 1011-1016, διαθέσιμο στο http://ijcttjournal.org/Volume3/issue-3/IJCTT-V3I3P134.pdf και Bottis, M. (2013). Not a Scalpel: RFID Implants for Patients and Personnel in Hospitals, in Bottis M. (ed.), Privacy and Surveillance-current aspects and future perspectives, Nomiki Bibliothiki, pp. 113-124.

κινήσεων των φυλακισμένων[83] και των παιδιών αντίστοιχα για λόγους ασφαλείας και στις δύο περιπτώσεις[84]. Καθώς και στον αθλητισμό[85] για την καταμέτρηση των επιδόσεων των αθλητών και την έκδοση αμερόληπτων αποτελεσμάτων.

5.3. Φορείς ζώα

Όσον αφορά περιπτώσεις όπου φορέας της τεχνολογίας RFID είναι ένα ζώο, η τεχνολογία RFID εφαρμόζεται στα ζώα στην κτηνοτροφία, στα κατοικίδια ζώα και στα ζώα υπό εξαφάνιση. Σε όλες τις περιπτώσεις πραγματοποιείται σήμανση και καταγραφή των ζώων είτε με εμφύτευση της ετικέτας RFID, είτε φορώντας την στα πόδια των ζώων ως βραχιόλι.

Στην κτηνοτροφία[86] με τη βοήθεια της τεχνολογίας RFID παρακολουθούνται τα ζώα που είτε τα ίδια, είτε παράγωγά τους πρόκειται να εισέρθουν στην τροφική αλυσίδα. Συγκεκριμένα, τα ζώα από τη στιγμή της γέννησής τους φέρουν την ετικέτα RFID και οι κτηνίατροι καταγράφουν σε αυτήν εφόσον σε ένα ζώο του έχουν χορηγηθεί φάρμακα. Με αυτό τον τρόπο διευκολύνεται η παρακολούθηση της ιατρικής κατάστασης του ζώου, παρακολουθούνται οι ασθένειες και τα φάρμακα που δόθηκαν και παίρνονται ορθές αποφάσεις σχετικά με το εάν τελικά είναι ασφαλές για τον άνθρωπο να εισέρθει αυτό το ζώο ή τα παράγωγά του στην τροφική αλυσίδα. Επίσης

[83] Στην Ελλάδα έχει εκδοθεί νόμος για την ηλεκτρονική επιτήρηση υπόδικων, κατάδικων και κρατούμενων σε άδεια (Ν. 4205/2013, ΦΕΚ 242/Α΄/611.2013), διαθέσιμος στο http://www.ministryofjustice.gr/site/Portals/0/uploaded_files/uploaded_11/N_4205-2013.pdf. Επίσης βλ. σχετικό δελτίο τύπου στην ελληνική ένωση για τα δικαιώματα του ανθρώπου διαθέσιμο στο https://www.hlhr.gr/%CE%B5%CF%80%CE%B9%CF%84%CE%B7%CF%81%CE%B7%CF%83%CE%B7-%CF%85%CF%80%CE%BF%CE%B4%CE%B9%CE%BA%CF%89%CE%BD/.

[84] Αναφορικά με την εφαρμογή της τεχνολογίας RFID ως μέσο παρακολούθησης ανθρώπων βλ. Singh, I., Patil, H. (2010). RFID: Dynamic Surveillance Approach, International Journal of Computer Science Issues (IJCSI), Vol. 7(3), pp. 24-28, διαθέσιμο στο https://www.researchgate.net/profile/Mustafa_Al-Fayoumi/publication/46093584_Practical_E-Payment_Scheme/links/00b49525be8ab3cc11000000.pdf#page=38

[85] Αναφορικά με την εφαρμογή της τεχνολογίας RFID στον αθλητισμό βλ. Woellik, H., Mueller, A., & Herriger, J. (2014). Permanent RFID timing system in a track and field athletic stadium for training and analysing purposes. Procedia Engineering, Vol. 72, pp. 202-207.

[86] Αναφορικά με την εφαρμογή της τεχνολογίας RFID στην κτηνοτροφία βλ. Ruiz-Garcia, L., Lunadei, L. (2011). The role of RFID in agriculture: Applications, limitations and challenges. Computers and Electronics in Agriculture, Vol. 79(1), pp. 42-50.

μπορεί να χρησιμοποιηθεί και από τους κτηνοτρόφους για την παρακολούθηση και την εφαρμογή αυτοματοποιημένης σίτισης των ζώων.

Όσον αφορά τα ζώα που βρίσκονται υπό εξαφάνιση[87], με τη βοήθεια της τεχνολογίας RFID μπορούν να παρακολουθούνται οι κινήσεις τους σε πραγματικό χρόνο και επομένως να εντοπιστούν. Με αυτό τον τρόπο μπορεί να αποτραπεί η λαθροθηρία και η διευκόλυνση των ομάδων διάσωσης να εντοπίσουν τέτοια γεγονότα και να αντιδράσουν άμεσα.

Τέλος, στα κατοικίδια ζώα[88] η εφαρμογή της τεχνολογίας RFID συμβάλλει στη μείωση των αδέσποτων. Όταν ένα κατοικίδιο ζώο περνάει στην κατοχή κάποιου ανθρώπου, τότε ο κτηνίατρος που παρακολουθεί το ζώο ενημερώνει την ετικέτα RFID του ζώου με τα στοιχεία του ιδιοκτήτη. Έτσι, εάν για κάποιο λόγο το ζώο απομακρυνθεί από τον ιδιοκτήτη του και βρεθεί από κάποιον τρίτο, μπορεί εύκολα με τη βοήθεια ενός κτηνιάτρου να εντοπιστεί ο ιδιοκτήτης του ανακτώντας τα στοιχεία από την ετικέτα RFID.

6. Ζητήματα ασφαλείας της τεχνολογίας RFID και προστασίας της ιδιωτικότητας

Στο παραπάνω κεφάλαιο παρουσιάστηκαν οι επιτυχημένες εφαρμογές της τεχνολογίας RFID. Όμως πέρα από τα πλεονεκτήματα και τις διευκολύνσεις που προσφέρει η εφαρμογή της τεχνολογίας RFID, πρέπει να ληφθούν υπόψη και τα ζητήματα ασφαλείας της τεχνολογίας και προστασίας της ιδιωτικότητας που προκύπτουν από τη χρήση της. Προκειμένου να εφαρμόζεται η τεχνολογία RFID χωρίς προβλήματα, τα εμπλεκόμενα μέρη,

[87] Αναφορικά με την εφαρμογή της τεχνολογίας RFID ως μέσο παρακολούθησης των ζώων υπό εξαφάνιση βλ. O' Donoghue, P., Rutz, C. (2016). Real-time anti-poaching tags could help prevent imminent species extinctions, Journal of Applied Ecology, Vol. 53(1), pp. 5-10, διαθέσιμο στο https://besjournals.onlinelibrary.wiley.com/doi/pdf/10.1111/1365-2664.12452

[88] Στην Ελλάδα έχει εκδοθεί νόμος για τη δημιουργία Διαδικτυακής Ηλεκτρονικής Βάσης σήμανσης και καταγραφής των ζώων συντροφιάς και των ιδιοκτητών τους (Ν. 4039/2012, ΦΕΚ Α 15/02.02.2012). Συγκεκριμένα, στο άρθρο 4 του νόμου εκτός άλλων ορίζεται ότι στη βάση αυτή θα καταχωρίζονται από τους κτηνιάτρους (α) τα στοιχεία, που αφορούν στην αναγνώριση των ζώων συντροφιάς (όπως φύλο, χρώμα, ράτσα, απώλεια, παράδοση σε άλλον ιδιοκτήτη, θάνατος) και (β) τα στοιχεία αναγνώρισης του ιδιοκτήτη τους (όπως ονοματεπώνυμο, διεύθυνση, τηλέφωνο και αριθμό ταυτότητας ή διαβατηρίου ή ισοδύναμου εγγράφου, όπως δίπλωμα οδήγησης ή ασφαλιστικό βιβλιάριο).

δηλαδή οι ετικέτες RFID και οι αναγνώστες, πρέπει να λειτουργούν με ασφαλή τρόπο και σύμφωνα με το πνεύμα της προστασίας της ιδιωτικότητας[89]. Το γεγονός ότι το άτομο που φέρει μία ετικέτα RFID καθίσταται διαρκής πομπός δεδομένων[90] τα οποία δεδομένα μπορούν να αναγνωστούν και από τρίτους χωρίς να το γνωρίζει, εισάγει ένα σημαντικό αριθμό προβλημάτων καθιστώντας αναγκαία τη λήψη μέτρων για την ασφάλειά του.

Σε αυτό το κεφάλαιο παρουσιάζονται οι σημαντικότεροι κίνδυνοι στην ιδιωτικότητα που προκύπτουν από τη χρήση της τεχνολογίας RFID, οι βασικοί τύποι επιθέσεων κατά της τεχνολογίας RFID και τα υπάρχοντα μέτρα προστασίας της ιδιωτικότητας.

6.1. Κίνδυνοι για την ιδιωτικότητα από τη χρήση της τεχνολογίας RFID

Οι κίνδυνοι για την ιδιωτικότητα που προκύπτουν από τη χρήση της τεχνολογίας RFID είναι ένα θέμα το οποίο έχει απασχολήσει αρκετά τους ερευνητές. Οι σημαντικότεροι κίνδυνοι όπως έχουν παρουσιαστεί στη βιβλιογραφία[91] είναι (α) αόρατη συλλογή δεδομένων εν αγνοία του χρήστη, (β) η δημιουργία μεγάλων βάσεων δεδομένων, (γ) η χρήση κοινών μοναδικών αναγνωριστικών χαρακτηριστικών για κάθε αντικείμενο παγκοσμίως, (δ) η αποκάλυψη στοιχείων της ιδιωτικής ζωής και (ε) της τοποθεσίας του κατόχου και (στ) η συσχέτιση μίας συγκεκριμένης ετικέτας RFID με τον κάτοχό της. Αναλυτικότερα για κάθε κίνδυνο αναφέρονται τα παρακάτω.

(α) Συλλογή δεδομένων εν αγνοία του χρήστη

[89] Βλ. Αλεξανδροπούλου–Αιγυπτιάδου, Ε., Μαυρίδης, Ι. (2007). Η Προστασία των Προσωπικών Δεδομένων.., ό.π. σελ: 497.

[90] Βλ. Συνοδινού, Τ.-Ε. (2005). Η ανίχνευση της ιδιωτικότητας μέσα από τις ραδιοσυχνότητες: Προστασία προσωπικών δεδομένων και τεχνολογιών αναγνώρισης μέσω ραδιοσυχνοτήτων (RFID), Αρμ ΝΘ', σελ. 1365.

[91] Σχετικά με τους κινδύνους και τις απειλές στην ιδιωτικότητα από τη χρήση της τεχνολογίας RFID βλ. OECD (2008). OECD Policy Guidance on Radio Frequency Identification (RFID), Ministerial Meeting on the future of the meeting economy, Seoul, Korea, 17-18 June, σελ. 52-56, διαθέσιμο σε http://www.oecd.org/sti/ieconomy/oecdpolicyguidanceonradiofrequencyidentificationrfid.htm, Position Statement on the Use of RFID on Consumer Products (2003), σελ. 2, διαθέσιμο στο https://www.cdt.org/files/privacy/031114rfid.pdf και Ρεκλείδης, Ε., Ριζομυλιώτης Π., Γκρίτζαλης, Στ. (2010). RFID: Απειλές κατά της Ιδιωτικότητας και Μέτρα Προστασίας, ό.π., σελ: 203-206.

Ένας από τους σημαντικότερους κινδύνους στην ιδιωτικότητα είναι η συλλογή των δεδομένων της ετικέτας RFID εν αγνοία του κατόχου της. Συγκεκριμένα, η πρόσβαση στα δεδομένα μπορεί να επιτευχθεί από απόσταση, με την ύπαρξη εμποδίων και χωρίς οπτική επαφή.

(β) Δημιουργία μεγάλων βάσεων δεδομένων

Η χρήση της τεχνολογίας RFID απαιτεί τη δημιουργία μεγάλων βάσεων δεδομένων στις οποίες αποθηκεύονται τα μοναδικά χαρακτηριστικά της κάθε ετικέτας RFID. Εάν αυτές οι εγγραφές, με περαιτέρω επεξεργασία και διασταυρούμενη συγκέντρωση και ανάλυση, συνδεθούν με προσωπικά δεδομένα τότε απειλείται σημαντικά η ιδιωτικότητα.

(γ) Χρήση μοναδικών αναγνωριστικών χαρακτηριστικών για κάθε αντικείμενο παγκοσμίως

Η χρήση της τεχνολογίας του Ηλεκτρονικού Κώδικα Προϊόντος (EPC) για τη δημιουργία ενός αναγνωριστικού κωδικού για κάθε αντικείμενο ο οποίος θα το ταυτοποιεί μοναδικά παγκοσμίως (βλ. Μέρος πρώτο, υποκεφάλαιο 3.7.3), ενδέχεται να οδηγήσει στη δημιουργία ενός συστήματος καταχώρισης όπου κάθε αντικείμενο θα συνδέεται με τον κάτοχό του στο σημείο πώλησης.

(δ) Αποκάλυψη στοιχείων της ιδιωτικής ζωής

Η πρόσβαση στις πληροφορίες μίας ετικέτας RFID μπορεί να οδηγήσει στην αποκάλυψη στοιχείων της ιδιωτικής ζωής του κατόχου, όπως καταναλωτικές προτιμήσεις[92], ιατρικές πληροφορίες[93] αλλά και πληροφορίες για την οικονομική κατάσταση[94]. Δεδομένου ότι η τεχνολογία RFID αναμένεται να ενσωματωθεί σε όλα τα προϊόντα καθημερινής χρήσης έχει ως αποτέλεσμα να απειλείται σημαντικά η ιδιωτικότητα.

(ε) Αποκάλυψη της τοποθεσίας

[92] Η διαφορά με τις κάρτες πιστότητας είναι ότι η χρήση των καρτών πιστότητας γίνεται με τη συγκατάθεση του ατόμου και όσο συχνά το επιθυμεί.
[93] Ιατρικές πληροφορίες μπορούν να αποκαλυφθούν από την πρόσβαση στις πληροφορίες ετικετών φαρμακευτικών προϊόντων.
[94] Πληροφορίες για την οικονομική κατάσταση μπορούν να αποκαλυφθούν από την πρόσβαση στις πληροφορίες ετικετών από αντικείμενα μεγάλης αξίας.

Πέρα από την αποκάλυψη των προτιμήσεων του κατόχου της ετικέτας RFID μπορεί να αποκαλυφθεί και η τοποθεσία. Οι ετικέτες RFID διαβάζονται από τους αναγνώστες των οποίων η τοποθεσία είναι γνωστή αφήνοντας έτσι ψηφιακά αποτυπώματα σε πραγματικό χρόνο. Επίσης, πέρα από την τοποθεσία, με το σύνολο των ετικετών που έχει κάποιος υπό την κατοχή του[95] μπορεί να αποκαλυφθούν ακόμη και οι κινήσεις του κατόχου με μεγάλη ακρίβεια.

(στ) Συσχέτιση μίας συγκεκριμένης ετικέτας RFID με τον κάτοχό της

Η συσχέτιση ανάμεσα στον κάτοχο ενός προϊόντος το οποίο φέρει ετικέτα RFID με αυτήν την ετικέτα είναι ισχυρή καθώς ο κάτοχός της συσχετίζεται με το συγκεκριμένο προϊόν και όχι μόνο με τον τύπο του προϊόντος, όπως συμβαίνει με τις κάρτες πιστότητας πελατών[96]. Για παράδειγμα, αγοράζοντας ένα ρολόι το οποίο έχει ενσωματωμένη ετικέτα RFID[97] μπορεί ο κάτοχός του να συσχετιστεί με το συγκεκριμένο αντικείμενο και να καταγράφονται οι καταναλωτικές συνήθειες και κινήσεις όταν βρίσκεται στην εμβέλεια αναγνωστών. Επιπλέον, εάν κάποια στιγμή χρησιμοποιηθεί από τον κάτοχο του προϊόντος πιστωτική κάρτα, η ταυτοποίηση και η συσχέτιση θα γίνει ακόμη πιο ισχυρή[98].

Οι παραπάνω κίνδυνοι της τεχνολογίας RFID μπορούν να υποβαθμιστούν από τέσσερις «παγίδες»[99] οι οποίες αφορούν διαδεδομένες κοινωνικές αντιλήψεις και δεν ανταποκρίνονται στην πραγματικότητα[100]. Μία παγίδα είναι ότι ο σειριακός αριθμός που αποθηκεύεται στις ετικέτες RFID είναι χωρίς σημασία, περίπτωση στην οποία δε λαμβάνεται υπόψη η

[95] Το σύνολο των ετικετών που φέρει ένα άτομο σχηματίζει ένα μοναδικό αστερισμό (constellation). Βλ. Ρεκλείδης, Ε., Ριζομυλιώτης Π., Γκρίτζαλης, Στ. (2010). RFID: Απειλές κατά της Ιδιωτικότητας και Μέτρα Προστασίας, ό.π., σελ: 206.

[96] Οι κάρτες πιστότητας πελατών (loyalty cards) χρησιμοποιούνται από τα καταστήματα για την παροχή προνομίων στους πελάτες τους, όπως εκπτώσεις σε προϊόντα, με σκοπό τη συλλογή πληροφοριών σχετικά με την καταναλωτική τους συμπεριφορά.

[97] Στα ρολόγια ενσωματώνεται πολλές φορές η τεχνολογία RFID μέσα στο προϊόν και χρησιμοποιείται ως ενδεικτικό για την εγγύηση του προϊόντος.

[98] Βλ. Ρεκλείδης, Ε., Ριζομυλιώτης Π., Γκρίτζαλης, Στ. (2010). RFID: Απειλές κατά της Ιδιωτικότητας και Μέτρα Προστασίας, ό.π., σελ: 204-205.

[99] Σχετικά με τις «παγίδες» βλ. Communication de M. Philippe Lemoine relative à la Radio-Identification (Radio-Tags ou RFIds), σελ. 7, διαθέσιμο στο https://dominfo.files.wordpress.com/2009/10/rfid_communication.pdf.

[100] Βλ. Αλεξανδροπούλου–Αιγυπτιάδου, Ε., Μαυρίδης, Ι. (2007). Η Προστασία των Προσωπικών Δεδομένων.., ό.π. σελ: 498.

δυνατότητα οποιουδήποτε να αποκτήσει πλήθος πληροφοριών ύστερα από διασταυρούμενη συγκέντρωση και ανάλυση πληροφοριών από όλες τις ετικέτες που φέρει το συγκεκριμένο άτομο. Μία δεύτερη παγίδα είναι ότι οι ετικέτες τοποθετούνται μόνο σε αντικείμενα αγνοώντας τις εφαρμογές που έχουν ήδη γίνει στον άνθρωπο με εμφύτευση (βλ. Μέρος τρίτο, Κεφάλαιο 1). Μία τρίτη παγίδα είναι ότι η έρευνα για τις εφαρμογές RFID πραγματοποιείται κυρίως στις Ηνωμένες Πολιτείες όπου το επίπεδο προστασίας της ιδιωτικότητας δεν είναι τόσο υψηλό όσο στην Ευρώπη, παραβλέποντας ότι η εξάπλωση της τεχνολογίας στην Ευρώπη γίνεται ραγδαία χωρίς να προλάβει να περιβληθεί από τα υψηλά πρότυπα προστασίας των προσωπικών δεδομένων της ευρωπαϊκής νομοθεσίας. Τέλος, μία τέταρτη παγίδα είναι η αυτόματη ενεργοποίηση των ετικετών RFID και η μετάδοση των δεδομένων ασύρματα, αόρατα και από απόσταση χωρίς να απαιτείται οπτική επαφή, η οποία έχει ως επακόλουθο την έλλειψη της ατομικής εγρήγορσης του ατόμου του οποίου τα δεδομένα υφίστανται επεξεργασία.

6.2. Επιθέσεις κατά της τεχνολογίας RFID

Σύμφωνα με μελέτη του Γερμανικού Ομοσπονδιακού Γραφείου για την Ασφάλεια των πληροφοριών, οι βασικοί τύποι επιθέσεων κατά της τεχνολογίας RFID είναι οχτώ και προκύπτουν (α) από τη σχέση μεταξύ της ετικέτας και των δεδομένων που είναι αποθηκευμένα σε αυτή, (β) από τη σχέση μεταξύ της ετικέτας και του φορέα της ετικέτας και (γ) τη σχέση μεταξύ της ετικέτας και του αναγνώστη[101]. Οι οχτώ αυτοί βασικοί τύποι επιθέσεων κατά της τεχνολογίας RFID όπως έχουν παρουσιαστεί στη βιβλιογραφία είναι οι παρακάτω[102].

[101] Βλ. Oertel, B., Wölk, M., Hilty, L. (2010). Security aspects and prospective applications of RFID systems. Federal Office for Information Security, σελ. 33, διαθέσιμο στο https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/RFID/RIKCHA_english_pdf.pdf;jsessionid=55D39D5AAE789967CA35785CAB644C38.2_cid351?__blob=publicationFile&v=1

[102] Σχετικά με τις επιθέσεις κατά της τεχνολογίας RFID βλ. Bundesamt für Sicherheit in der Informationstechnik (2005). Security Aspects and Prospective Applications of RFID Systems, σελ. 33-34, διαθέσιμο στο https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/RFID/RIKCHA_english_pdf.pdf?__blob=publicationFile&v=1, Ρεκλείδης, Ε., Ριζομυλιώτης Π., Γκρίτζαλης, Στ. (2010).

1. Η παραποίηση των περιεχομένων της ετικέτας RFID (falsification of contents).

Σε αυτή την περίπτωση προστίθενται επιπλέον δεδομένα εφόσον αποκτηθεί μη εξουσιοδοτημένη πρόσβαση με δυνατότητα εγγραφής σε μία ετικέτα.

2. Η πλαστογράφηση της ταυτότητας της ετικέτας RFID (falsification of transponder's identity).

Ο εισβολέας σε αυτή την περίπτωση αποκτά το σειριακό αριθμό και οποιαδήποτε άλλη πληροφορία ασφάλειας της ετικέτας RFID είναι απαραίτητη προκειμένου να εξαπατήσει τον αναγνώστη. Πλαστογραφεί δηλαδή την ταυτότητα της ετικέτας RFID για να αυθεντικοποιηθεί στον αναγνώστη.

3. Η απενεργοποίηση ετικέτας RFID (deactivating the tag).

Με την απενεργοποίηση της ετικέτας είτε με τη φυσική καταστροφή της ετικέτας, είτε με εντολή διαγραφής (delete command) ή εντολή οριστικής καταστροφής (kill command) από τον αναγνώστη η ετικέτα καθίσταται άχρηστη και ο αναγνώστης δεν μπορεί να επικοινωνήσει μαζί της.

4. Η αποκόλληση της ετικέτας RFID (detaching the tag).

Σε αυτήν την περίπτωση η ετικέτα RFID μπορεί να αποκολληθεί από το αντικείμενο που ταυτοποιεί και να προσκολληθεί και να συσχετιστεί με ένα άλλο αντικείμενο.

5. Η υποκλοπή των ραδιοσημάτων (eavesdropping).

Σε αυτή την περίπτωση ο εισβολέας κατά τη διάρκεια της επικοινωνίας της ετικέτας RFID με τον αναγνώστη μέσω της διεπαφής αέρα προσπαθεί να υποκλέψει τα ραδιοσήματα που ανταλλάσσονται.

6. Η παρεμπόδιση επικοινωνίας (blocking).

RFID: Απειλές κατά της Ιδιωτικότητας και Μέτρα Προστασίας, ό.π., σελ: 206-208 και Graveling R., Winski Th., Dixon K. (2018). The use of chip implants for workers, PE 614.209, IP/A/EMPL/2017-12, σελ. 35, διαθέσιμο στο http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)614209.

Η παρεμπόδιση της επικοινωνίας επιτυγχάνεται με τη χρήση μίας ετικέτας αποκλεισμού (bloker tag)[103] η οποία αποτρέπει τη μη εξουσιοδοτημένη επικοινωνία του αναγνώστη με τις ετικέτες.

7. Η παρεμβολή σήματος (jamming).

Η ανταλλαγή δεδομένων μέσω της διεπαφής αέρα μπορεί να διακοπεί ακόμη και με απλά παθητικά μέσα, όπως ο κλωβός Faraday cage.

8. Η πλαστογράφηση της ταυτότητας του αναγνώστη (falsifying reader's identity).

Ιδανικά, σε ένα ασφαλές σύστημα ο αναγνώστης πρέπει να αποδεικνύει την ταυτότητά του στην ετικέτα RFID, ώστε εάν ένας εισβολέας θελήσει να επικοινωνήσει με την ετικέτα πρέπει να πλαστογραφήσει την ταυτότητα του αναγνώστη. Σε πολλές εφαρμογές όμως η ταυτοποίηση των αναγνωστών παραλείπεται καθώς είναι πολύπλοκη και ακριβή διαδικασία[104].

Ο τύπος επίθεσης από τους εισβολείς επιλέγεται κάθε φορά ανάλογα με τον τιθέμενο προς επίτευξη στόχο. Σύμφωνα με τη μελέτη του Γερμανικού Ομοσπονδιακού Γραφείου για την Ασφάλεια των πληροφοριών[105] τέσσερις είναι οι λόγοι για τους οποίους ένας εισβολέας επιτίθεται σε ένα σύστημα RFID: (α) για λόγους κατασκοπείας με την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες (spying), (β) για την απόκρυψη πληροφοριών με αποτέλεσμα την εξαπάτηση του χρήστη παρέχοντας λανθασμένες πληροφορίες (deception), (γ) για την άρνηση εξυπηρέτησης οπότε η διαθεσιμότητα των λειτουργιών του συστήματος RFID είναι σε κίνδυνο (denial of service) και (δ) για την προστασία της ιδιωτικότητας όταν η ιδιωτική του ζωή απειλείται από το σύστημα RFID και προστατεύεται με επίθεση στο σύστημα. Στον παρακάτω παρουσιάζονται οι οχτώ τύποι επιθέσεων και οι πιθανοί στόχοι του εισβολέα σε κάθε περίπτωση.

---

[103] Η μέθοδος blocker tag είναι μία μέθοδος προστασίας της ιδιωτικότητας η οποία βασίζεται στην τεχνική άρνησης εξυπηρέτησης. Βλ. Ρεκλείδης, Ε., Ριζομυλιώτης Π., Γκρίτζαλης, Στ. (2010). RFID: Απειλές κατά της Ιδιωτικότητας και Μέτρα Προστασίας, ό.π., σελ: 211.

[104] Βλ. Ρεκλείδης, Ε., Ριζομυλιώτης Π., Γκρίτζαλης, Στ. (2010). RFID: Απειλές κατά της Ιδιωτικότητας και Μέτρα Προστασίας, ό.π., σελ: 208.

[105] Βλ. Oertel, B., Wölk, M., Hilty, L. (2010). Security aspects and prospective applications of RFID systems, ό.π. σελ. 34-35

Πίνακας 7 Τύποι επιθέσεων σε συστήματα RFID και οι πιθανοί στόχοι του εισβολέα

Πηγή: Oertel, B., Wölk, M., Hilty, L. (2010). Security aspects and prospective applications of RFID systems. Federal Office for Information Security, σελ. 35.

	Κατασκοπεία	Εξαπάτηση	Άρνηση Εξυπηρέτησης	Προστασία της ιδιωτικότητας
παραποίηση περιεχομένων ετικέτας		πιθανός στόχος		
πλαστογράφηση ταυτότητας της ετικέτας		πιθανός στόχος		
απενεργοποίηση ετικέτας		πιθανός στόχος	πιθανός στόχος	πιθανός στόχος
αποκόλληση ετικέτας		πιθανός στόχος		πιθανός στόχος
υποκλοπή ραδιοσημάτων	πιθανός στόχος			
παρεμπόδιση επικοινωνίας		πιθανός στόχος	πιθανός στόχος	πιθανός στόχος
παρεμβολή σήματος		πιθανός στόχος	πιθανός στόχος	πιθανός στόχος
πλαστογράφηση ταυτότητας αναγνώστη	πιθανός στόχος			

6.3. Μέτρα προστασίας της ιδιωτικότητας

Από τις παραπάνω υποενότητες γίνεται σαφές πως τα συστήματα RFID έρχονται αντιμέτωπα με διάφορες απειλές και επιθέσεις επομένως η ανάγκη για χρήση μεθόδων και τεχνικών αυθεντικοποίησης, ελεγχόμενης πρόσβασης και προστασίας της εμπιστευτικότητας και της ακεραιότητας του περιεχομένου των ετικετών είναι μεγάλη[106]. Σε αυτό το υποκεφάλαιο παρουσιάζονται οι διάφορες τεχνικές που έχουν προταθεί στη βιβλιογραφία για την αντιμετώπιση των παραπάνω προβλημάτων.

Η χρήση του κλωβού Faraday (Faraday cage)[107] είναι μία απλή μέθοδος με την οποία μπορεί να αποτραπεί η συλλογή των δεδομένων από

[106] Βλ. Αλεξανδροπούλου–Αιγυπτιάδου, Ε., Μαυρίδης, Ι. (2007). Η Προστασία των Προσωπικών Δεδομένων.., ό.π. σελ: 498.

[107] Η χρήση του κλωβού Faraday έχει προταθεί από τον ICAO (2004b) ως αντίμετρο για την προστασία των διαβατηρίων όταν δε χρησιμοποιούνται από την παράνομη σάρωση. Βλ. Nikita, M., (2012). RFID chips and EU e-passports: the end of privacy?, ό.π. σελ. 206 και Juels, A., Rivest, R. L., & Szydlo, M. (2003). The blocker tag: Selective blocking of RFID tags for consumer privacy. In

μία ετικέτα RFID εν αγνοία του κατόχου της. Αρκεί να τοποθετηθεί το αντικείμενο το οποίο φέρει την ετικέτα μέσα σε μία θήκη κατασκευασμένη από μεταλλικό πλέγμα ή φύλλο αλουμινίου η οποία θήκη παρεμποδίζει το σήμα της ετικέτας και επομένως αποκλείει την επικοινωνία της ετικέτας με οποιοδήποτε αναγνώστη. Η προστασία όμως που προσφέρει αυτή η μέθοδος είναι περιορισμένη καθώς μόλις ο κάτοχος του αντικειμένου αφαιρέσει τη θήκη είναι και πάλι ευάλωτος. Επίσης αυτή η μέθοδος δεν είναι εφικτό να χρησιμοποιηθεί σε πολύ μεγάλα αντικείμενα και ούτε για μεγάλο πλήθος αντικειμένων.

Η χρήση της μεθόδου των ενεργών παρεμβολών (active jamming)[108] είναι μία εναλλακτική μέθοδος του κλωβού Faraday η οποία δεν επιβαρύνει την ετικέτα RFID και εκμεταλλεύεται τις φυσικές ιδιότητες των σημάτων. Με αυτή τη μέθοδο, χρησιμοποιείται μία συσκευή εκπομπής θορύβου η οποία δημιουργεί παρεμβολές και εμποδίζει την επικοινωνία με την ετικέτα. Ταυτόχρονα όμως μπορεί να προκαλέσει και προβλήματα καθώς ενδέχεται να δημιουργήσει παρεμβολές και σε άλλα νόμιμα συστήματα, όπως τους ασυρμάτους επικοινωνίας που χρησιμοποιούν η αστυνομία και γενικότερα οι υπηρεσίες έκτακτης ανάγκης, που βρίσκονται στην εμβέλεια των παρεμβολών.

Η απενεργοποίηση της ετικέτας RFID είναι ένα ακόμη προτεινόμενο αντίμετρο το οποίο όμως επηρεάζει τον τρόπο λειτουργίας της. Η απενεργοποίηση μπορεί να επιτευχθεί με δύο εντολές τις οποίες λαμβάνει η ετικέτα από τον αναγνώστη, την εντολή τερματισμού (kill command) και την εντολή της ύπνωσης (sleep command). Με την εντολή του τερματισμού απενεργοποιείται η ετικέτα και επομένως δεν μπορεί ποτέ ξανά να επικοινωνήσει μαζί της κάποιος αναγνώστης, γεγονός που καθιστά αυτή τη μέθοδο αποτελεσματικό μέτρο προστασίας της ιδιωτικότητας. Με την εντολή της ύπνωσης η ετικέτα βρίσκεται σε αναμονή και δεν επικοινωνεί με κάποιον

Proceedings of the 10th ACM conference on Computer and communications security, ACM, σελ: 104-105.

[108] Βλ. Juels, A., Rivest, R. L., & Szydlo, M. (2003). The blocker tag: Selective blocking of RFID tags for consumer privacy, ό.π., σελ. 105 και Ρεκλείδης, Ε., Ριζομυλιώτης Π., Γκρίτζαλης, Στ. (2010). RFID: Απειλές κατά της Ιδιωτικότητας και Μέτρα Προστασίας, ό.π., σελ: 210.

αναγνώστη έως ότου λάβει την εντολή αφύπνισης (wake command)[109]. Η υλοποίηση της εν λόγω μεθόδου απενεργοποίησης της ετικέτας είναι εύκολη, αλλά σε ορισμένες περιπτώσεις περιορίζει τις δυνατότητες της τεχνολογίας RFID[110] και σε άλλες περιπτώσεις δεν είναι δυνατόν να εφαρμοστεί γιατί είναι απαραίτητο οι ετικέτες να παραμένουν συνεχώς ενεργές[111]. Επίσης, αν και αποτελεί αποτελεσματικό μέτρο προστασίας της ιδιωτικότητας, το γεγονός ότι χρήστης δεν μπορεί να επαληθεύσει εύκολα εάν όντως η ετικέτα έχει απενεργοποιηθεί είτε γιατί δεν εκτελέστηκε σωστά η εντολή, είτε εσκεμμένα[112] την καθιστά αναξιόπιστο μέτρο.

Άλλη μία μέθοδος προστασίας της εμπιστευτικότητας και της ακεραιότητας του περιεχομένου των ετικετών RFID είναι η ανάλυση της ενέργειας της κεραίας του αναγνώστη[113]. Επειδή οι επιθέσεις στην ετικέτα συνήθως πραγματοποιούνται από απόσταση, η ποιότητα του σήματος του αναγνώστη σε αυτές τις περιπτώσεις είναι ελαττωμένη. Επομένως, η ετικέτα μετρώντας το λόγο του σήματος του αναγνώστη προς το θόρυβο μπορεί να ελέγξει την αυθεντικότητα του αναγνώστη. Βέβαια η μέθοδος αυτή από μόνη της δε προσφέρει αποτελεσματική ασφάλεια και προτείνεται ως συμπληρωματική.

Τέλος, μία ακόμη κατηγορία αντιμέτρων που προτείνεται στη βιβλιογραφία είναι αυτή που βασίζεται στη χρήση κρυπτογραφικών αλγορίθμων. Ένα χαρακτηριστικό παράδειγμα κρυπτογραφικού πρωτοκόλλου αυθεντικοποίησης είναι η οικογένεια πρωτοκόλλων HB[114,115] η οποία έχει

[109] Και στις δύο περιπτώσεις, οι εντολές τερματισμού και ύπνωσης της ετικέτας, προστατεύονται με τη χρήση συνθηματικού. Βλ. Juels, A. (2006). R.F.I.D. Security and Privacy: A Research Survey, IEEE Journal on Selected Areas in Communications, Vol. 24 (2), σελ. 386 και Ρεκλείδης, Ε., Ριζομυλιώτης Π., Γκρίτζαλης, Στ. (2010). RFID: Απειλές κατά της Ιδιωτικότητας και Μέτρα Προστασίας, ό.π., σελ: 210-211.

[110] Τέτοιες είναι οι περιπτώσεις που χρησιμοποιείται ως ενδεικτικό για την εγγύηση του προϊόντος.

[111] Τέτοιες είναι οι περιπτώσεις που χρησιμοποιείται στις βιβλιοθήκες για τη διαχείριση των βιβλίων και στις δημόσιες υπηρεσίες για τον εντοπισμό των δημόσιων εγγράφων.

[112] Βλ. Fishkin, K. P., Roy, S., Jiang, B. (2004). Some methods for privacy in RFID communication, in European Workshop on Security in Ad-hoc and Sensor Networks, Springer, Berlin, Heidelberg, pp. 44.

[113] Βλ. Ρεκλείδης, Ε., Ριζομυλιώτης Π., Γκρίτζαλης, Στ. (2010). RFID: Απειλές κατά της Ιδιωτικότητας και Μέτρα Προστασίας, ό.π., σελ: 212.

[114] Το πρωτόκολλο HB πήρε το όνομά του από τους σχεδιαστές του Hopper και Blum. Βλ. Hopper, N. J., Blum, M. (2000). A Secure Human-Computer Authentication Scheme, Tech. Rep. CMU-CS-00-139, Carnegie Mellon University, 2000, διαθέσιμο στο https://apps.dtic.mil/dtic/tr/fulltext/u2/a382135.pdf και Hopper, N. J., Blum, M. (2001). Secure Human

προταθεί για την αυθεντικοποίηση ανθρώπου με μηχανή. Μία ακόμη μέθοδος η οποία ανήκει σε αυτή την κατηγορία είναι η μέθοδος Hash Lock η οποία ελέγχει την πρόσβαση στα δεδομένα της ετικέτας RFID και με τον τρόπο αυτό δεν αποκαλύπτονται πληροφορίες έως ότου ο αναγνώστης στείλει το σωστό κλειδί[116]. Όμως η χρήση κρυπτογραφικών αλγορίθμων αυξάνει σημαντικά το κόστος των ετικετών αναλογικά με την πολυπλοκότητα των πράξεων που εκτελούν και της απαιτούμενης υπολογιστικής μνήμης με αποτέλεσμα να απορρίπτεται από τους κατασκευαστές.

Ολοκληρώνοντας, διαπιστώνεται ότι σχετικά με την αντιμετώπιση των ζητημάτων ασφαλείας και προστασίας της ιδιωτικότητας έχουν προταθεί διάφορα μέτρα προστασίας τα οποία όμως παρουσιάζουν αδυναμίες και δεν επαρκούν από μόνα τους. Καταλυτικός είναι ταυτόχρονα και ο ρόλος της νομοθεσίας για τη διασφάλιση των δικαιωμάτων του υποκειμένου, η οποία θα εξετασθεί στο επόμενο μέρος της παρούσας διατριβής.

Identification Protocols, In: Boyd C. (eds) Advances in Cryptology – ASIACRYPT (2001), Vol. 2248, pp. 52–66.

[115] Μία βελτιωμένη μορφή του πρωτοκόλλου HB, η HB+, προτάθηκε από τους Juels A. και Weis A. St. Βλ. Juels, A., Weis, A., St. (2005). Authenticating pervasive devices with human protocols, In: Shoup V. (eds) Advances in Cryptology – CRYPTO 2005. CRYPTO 2005. Lecture Notes in Computer Science, Vol. 3621. Springer, Berlin, Heidelberg, σελ: 293-308.

[116] Βλ. Dixit, V., Verma, H., K., Singh, A., K. (2011), Comparison of various Security Protocols in RFID, International Journal of Computer Applications, Vol. 24(7), σελ. 19.

III.ΜΕΡΟΣ ΔΕΥΤΕΡΟ

Νομική ρύθμιση της τεχνολογίας RFID

Η πληθώρα των εφαρμογών της τεχνολογίας RFID, όπως έχουν ήδη παρουσιαστεί σε παραπάνω κεφάλαιο (βλ. Μέρος πρώτο, Κεφάλαιο 5), είναι αδιαμφισβήτητο πως διευκολύνουν τον άνθρωπο σε πολλές πτυχές της καθημερινότητάς του καθιστώντας την τεχνολογία σημαντικό εργαλείο για αυτόν. Έχει όμως παρατηρηθεί πως η δυναμική της εξέλιξη παράλληλα δημιουργεί προκλήσεις και νέους κινδύνους καθώς πολλές φορές συνδέεται είτε άμεσα, είτε έμμεσα με προσωπικά δεδομένα εγείροντας σημαντικά ερωτήματα και έντονο προβληματισμό σχετικά με την προστασία αυτών. Βέβαια όταν σε ένα αντικείμενο προσκολλάται μία ετικέτα RFID δε σημαίνει ότι πάντα θα προκύπτουν ζητήματα ιδιωτικότητας, αλλά ανάλογα με το περιβάλλον στο οποίο εφαρμόζονται και εφόσον χρησιμοποιούνται για τη συλλογή πληροφοριών σχετικά με ένα φυσικό πρόσωπο, τότε μόνο σχετίζονται με την επεξεργασία προσωπικών δεδομένων[117].

Όσον αφορά την έννοια της ιδιωτικότητας[118] (ή αλλιώς της ιδιωτικής ζωής) συχνά αναφέρεται ως το δικαίωμα του ατόμου στην απομόνωση και σε μία ανενόχλητη ζωή (the right to be let alone). Ενώ όσον αφορά την έννοια των προσωπικών δεδομένων[119] είναι ευρύτατη και βασικό του στοιχείο είναι ότι συνδέεται με συγκεκριμένο πρόσωπο έτσι ώστε να προκύπτει η ταυτότητα

[117] Βλ. Κώστα, Ε. (2010). Ζητήματα ιδιωτικότητας και νέες τεχνολογίες: το παράδειγμα της τεχνολογίας RFID, σε Λαμπρινουδάκη, Κ.-Μήτρου, Λ.-Γκρίτζαλη, Σ.-Κάτσικα,Σ., Προστασία της ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, εκδ. Παπασωτηρίου, Αθήνα 2010, σελ: 583-602.

[118] Η έννοια της ιδιωτικότητας, σύμφωνα με τη Μήτρου Λ. (2010, σελ. 508-509), με την πάροδο των χρόνων και την επίδραση των τεχνολογικών εξελίξεων έχει εμπλουτιστεί με επιμέρους δικαιώματα όπως το δικαίωμα σε ιδιωτική ζωή, ο περιορισμός της προσβασιμότητας, ο αποκλειστικός έλεγχος της πρόσβασης στον ιδιωτικό χώρο (ή άσυλο της κατοικίας), η ελαχιστοποίηση των "παρεμβάσεων", η προσδοκία της εχεμύθειας, το δικαίωμα στο απόρρητο και το δικαίωμα στην απόλαυση της μοναξιάς, της –υπό στενή έννοια- ιδιωτικότητας, της ανωνυμίας και της απόσυρσης.

[119] Ως προσωπικά δεδομένα, ή αλλιώς δεδομένα προσωπικού χαρακτήρα όπως χαρακτηρίζονται σε πολλά νομοθετικά κείμενα, σύμφωνα με το άρθρο 4 του Κανονισμού 2016/679 ορίζεται πως είναι "κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου".

του τελευταίου είτε άμεσα, είτε έμμεσα[120]. Επειδή λοιπόν τα προσωπικά δεδομένα αποτελούν στην ουσία στοιχεία της ιδιωτικότητας, η προστασία της ιδιωτικότητας με την προστασία των προσωπικών δεδομένων πολλές φορές ταυτίζονται.

Εξαιτίας όμως του εύρους του ορισμού του όρου προσωπικά δεδομένα, για την επίλυση των ζητημάτων που δημιουργούνται σε σχέση με την επεξεργασία προσωπικών δεδομένων σε εφαρμογές της τεχνολογίας RFID στον ευρωπαϊκό χώρο, προϋποτίθεται τουλάχιστον μία κοινή αντίληψη του ποιες πληροφορίες νοούνται ως προσωπικά δεδομένα[121].

Η Ομάδα εργασίας του άρθρου 29 σε γνώμη της[122] παρέχει κατευθύνσεις για τον τρόπο με τον οποίο πρέπει να γίνεται αντιληπτή η έννοια των προσωπικών δεδομένων ώστε να διαμορφωθεί μία κοινή αντίληψη, ενώ προηγουμένως σε κείμενό[123] της σχετικά με τα ζητήματα προστασίας δεδομένων που προκύπτουν από τη χρήση της τεχνολογίας RFID, αναφέρθηκε σε τρεις περιπτώσεις οι οποίες έχουν επιπτώσεις στην προστασία των προσωπικών δεδομένων εξαιτίας της χρήσης της. Αυτές είναι η περίπτωση όπου συλλέγονται πληροφορίες οι οποίες συνδέονται άμεσα ή έμμεσα με προσωπικά δεδομένα, η περίπτωση όπου αποθηκεύονται προσωπικά δεδομένα απευθείας στις ετικέτες RFID και η περίπτωση όπου συνδέονται οι καταναλωτές με τα προϊόντα που αγοράζουν.

Για τους παραπάνω λόγους, στο αναθεωρημένο πλαίσιο εκτίμησης των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων για τις εφαρμογές RFID το οποίο προτάθηκε το 2011 από μία ομάδα εργασίας RFID (αναλυτικά βλ. Μέρος δεύτερο, Κεφάλαιο 5), παρατηρείται ότι οι ερωτήσεις που προτείνονται (βλ. Εικόνα 13) είναι

[120] Βλ. Αλεξανδροπούλου–Αιγυπτιάδου, Ε. (2007). Προσωπικά δεδομένα: Η νομική ρύθμιση της ηλεκτρονικής επεξεργασίας τους, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα- Κομοτηνή, σελ. 33.
[121] Βλ. Κώστα, Ε. (2010). Ζητήματα ιδιωτικότητας και νέες τεχνολογίες.., ό.π. σελ. 586.
[122] Βλ. Ομάδα εργασίας του άρθρου 29, Γνώμη 4/2007 σχετικά με την έννοια του όρου 'δεδομένα προσωπικού χαρακτήρα', 01248/07/EL WP 136, 20 Ιουνίου, διαθέσιμη στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_el.pdf
[123] Βλ. Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology", (10107/05/EN, WP 105), January 19, 2005, διαθέσιμο στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf

διαμορφωμένες με τέτοιο τρόπο ώστε να καθοδηγήσουν τους φορείς εκμετάλλευσης της τεχνολογίας να εντοπίσουν σε ποια από αυτές τις περιπτώσεις ανήκουν και εν τέλει να αποφασιστεί σε ποιο βαθμό προκαλούν προβλήματα ιδιωτικότητας.

Η χρήση της τεχνολογίας RFID είναι σαφές πως θα βοηθήσει την ανθρωπότητα σε πολλούς τομείς, αρκεί όμως να γίνουν πρώτα οι σωστές επιλογές κατά τη σχεδίαση και την ανάπτυξή της ώστε πάντοτε τα εμπλεκόμενα μέρη να λειτουργούν με ασφαλή τρόπο και σύμφωνα με το πνεύμα της προστασίας της ιδιωτικότητας. Για την επίτευξη των ανωτέρω, η χρήσης της τεχνολογίας επιβάλλεται να τεθεί σε ειδικό νομικό πλαίσιο. Μάλιστα εύλογο θα ήταν να μελετηθεί η εφαρμογή της τεχνολογίας σε κάθε τομέα ξεχωριστά ανάλογα με τους κινδύνους που προκαλεί και να προταθούν ειδικές ρυθμίσεις προσαρμοσμένες σε κάθε περίπτωση για την καλύτερη προστασίας της ιδιωτικότητας.

Σε αυτό το μέρος της διατριβής αρχικά παρουσιάζεται συνοπτικά η εφαρμογή του δικαίου της ΕΕ στην επεξεργασία των προσωπικών δεδομένων. Έπειτα γίνεται αναφορά στη γνώμη της Ομάδας εργασίας του άρθρου 29 σχετικά με τις πρόσφατες εξελίξεις στο ΔτΠ, καθώς η τεχνολογία RFID είναι μία από τις υφιστάμενες εφαρμογές του ΔτΠ. Σε επόμενα κεφάλαια μελετάται η συμβολή του Ο.Ο.Σ.Α. (OECD) στην υιοθέτηση ενός αποδεκτού πλαισίου για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων από εφαρμογές των συστημάτων RFID στον ευρωπαϊκό χώρο, τα βήματα που έγιναν προς τη δημιουργία αυτού του πλαισίου και η παρουσίαση του προτεινόμενου πλαισίου για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID. Ολοκληρώνοντας το δεύτερο μέρος της διατριβής, γίνεται παρουσίαση του ελληνικού νομοθετικού πλαισίου για την προστασία των προσωπικών δεδομένων.

1. Το δίκαιο της ΕΕ για την επεξεργασία των προσωπικών δεδομένων

Οι ραγδαίες τεχνολογικές εξελίξεις και η παγκοσμιοποίηση δημιουργούν νέες ευκαιρίες και προοπτικές στην κοινωνική και οικονομική ζωή, ενώ ταυτόχρονα εγκυμονούν και σοβαρούς κινδύνους προσβολής της ιδιωτικότητας του ατόμου. Γι' αυτό το λόγο, οι νομικές ρυθμίσεις που προέκυπταν κατά την πάροδο των χρόνων για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα ήταν πάντοτε επηρεασμένες από τις εξελίξεις στο χώρο των νέων τεχνολογιών.

Από το 1970 μέχρι και σήμερα, παρατηρείται αλλαγή στην αντιμετώπιση και στη στάση του νομοθέτη απέναντι στην ηλεκτρονική επεξεργασία των προσωπικών δεδομένων. Μάλιστα, τα νομοθετήματα της δεκαετίας του 1970 και 1980 χαρακτηρίστηκαν «νομοθετήματα πρώτης γενιάς» και «νομοθετήματα δεύτερης γενιάς» αντίστοιχα[124]. Σε σχέση με τα νομοθετήματα της πρώτης γενιάς, τα «νομοθετήματα δεύτερης γενιάς» «*εισάγουν χαλαρότερες νομικές ρυθμίσεις στον χώρο της ηλεκτρονικής επεξεργασίας των προσωπικών δεδομένων, στο μέτρο που έχει γίνει πλέον αντιληπτή η αναγκαιότητα της τεχνολογίας για την κοινωνικοοικονομική ανάπτυξη, παρά τους κινδύνους που η αλόγιστη χρήση της εγκυμονεί για το δικαίωμα του ατόμου στον πληροφοριακό του αυτοκαθορισμό*»[125].

Από τη δεκαετία του 1990 και μετέπειτα ακολούθησαν τα «νομοθετήματα τρίτης γενιάς»[126] τα οποία αποτελούν και ορόσημο για την προστασία των προσωπικών δεδομένων και στον ελληνικό χώρο. Συγκεκριμένα, εκδόθηκε η Οδηγία 95/46/Ε.Κ. της 24.10.1995 (L 281, 31) για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων

[124] Βλ. Αλεξανδροπούλου–Αιγυπτιάδου, Ε. (2007). Προσωπικά δεδομένα.., ό.π. σελ. 123 και Αραβαντινός Β. (1997). Η προστασία των στοιχείων προσωπικού χαρακτήρα από την αθέμιτη επεξεργασία τους με ηλεκτρονικό υπολογιστή. (Συμβολή στη δικαιοκυβερνητική), Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, σελ. 14.

[125] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). Προσωπικά Δεδομένα, Νομική Βιβλιοθήκη, Αθήνα, σελ. 195.

[126] Περισσότερες πληροφορίες σχετικά με το νομοθετήματα τρίτης γενιάς, βλ. Αλεξανδροπούλου Ε., Προσωπικά δεδομένα: Η νομική ρύθμιση της ηλεκτρονικής επεξεργασίας, ό.π. σελ: 129-133.

προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, η Οδηγία 2002/58/Ε.Κ. της 12.7.2002 (L 201, 37) σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) οι διατάξεις της οποίας εξειδικεύουν και συμπληρώνουν την Οδηγία 95/46/ΕΚ, η καταργημένη Οδηγία 2006/24/ΕΚ της 15.3.2006 (L 105, 54) για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της Οδηγίας 2002/58/ΕΚ (L 105, 54) η οποία ακυρώθηκε το 2014 αναδρομικά ως ασύμβατη με το ευρωπαϊκό νομικό πλαίσιο και η Οδηγία 2009/136/ΕΚ της 25.11.2007 (L 337, 11) για τη τροποποίηση εκτός άλλων και της Οδηγίας 2002/58/ΕΚ.

Σήμερα, τη δεκαετία του 2010, θα μπορούσαμε να πούμε πως έχουμε τα νομοθετήματα της επόμενης γενιάς με σημαντικότερο τον Κανονισμό (ΕΕ) 2016/679. Ειδικότερα, στις 27 Απριλίου το 2016 ψηφίστηκε ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) ο οποίος επικαιροποιεί και εκσυγχρονίζει τις αρχές που θεσπίστηκαν με την Οδηγία 95/46/Ε.Κ. την οποία και καταργεί.

Τέλος, στο Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης[127], ο οποίος δεσμεύει όλα τα Όργανα σε όλες τις δράσεις και πολιτικές της Ένωσης, καθώς και στη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης[128], ορίζεται ότι κάθε πρόσωπο έχει δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν. Συγκεκριμένα, στο άρθρο 8 του Τίτλου ΙΙ του Χάρτη, όπου αναγνωρίζονται οι

[127] Περισσότερες πληροφορίες σχετικά με τον Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (2012/C 326/02) διαθέσιμες στο http://www.europarl.europa.eu/charter/default_el.htm. Επίσης, βλ. Τζέμος, Β.-Γ. (2015). Ο Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ. Ερμηνεία κατ' άρθρο, Νομική Βιβλιοθήκη και Ιγγλεζάκης Ι. (2005). Κοινωνικό Κράτος Δικαίου. Υπό το πρίσμα της συνταγματικής αναθεώρησης του 2001 (άρθρο 25§1 Σ) και του Ευρωπαϊκού Κοινοτικού Δικαίου, εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη, σελ: 195-245.

[128] Βλ. άρθρο 16 παράγραφος 1 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (2012/C 326/49) διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A12012E%2FTXT

ελευθερίες του ατόμου, αναφέρεται ρητά ότι[129] «*η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο, κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους»* και ότι *«ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής*».

Σε αυτό το κεφάλαιο παρουσιάζονται τα νομοθετήματα τα οποία σχετίζονται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στον ευρωπαϊκό χώρο. Συγκεκριμένα, γίνεται αναφορά στις Οδηγίες 95/46/ΕΚ, 2002/58/ΕΚ, 2006/24/ΕΚ και 2009/136/ΕΚ και στο Γενικό Κανονισμό για την Προστασία Δεδομένων (ΕΕ) 2016/679.

1.1. Η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24.10.1995

Η πρώτη σημαντική προσπάθεια σε ευρωπαϊκό επίπεδο για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, είναι η έκδοση της Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995. Σκοπός της εν λόγω Οδηγίας είναι η επίτευξη υψηλού επιπέδου προστασίας της ιδιωτικής ζωής των προσώπων και ταυτόχρονα η ελεύθερη κυκλοφορία των προσωπικών δεδομένων στα κράτη-μέλη της Ευρωπαϊκής Ένωσης[130].

[129] Βλ. άρθρο 8, στην επίσημη διακήρυξη του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (2012/C 326/02), διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=uriserv:OJ.C_.2012.326.01.0391.01.ELL&toc=OJ:C:2012:326:TOC. Επίσης βλ. Τζέμος, Β.-Γ. (2015). Ο Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ. Ερμηνεία κατ' άρθρο, ό.π. σελ. 97-109.

[130] Αναλυτικά βλ. 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», Επίσημη Εφημερίδα της ΕΕ αριθ. L 281 της 23/11/1995, σελ: 31–50, διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:31995L0046.

Το πεδίο εφαρμογής της Οδηγίας, όπως ορίζεται στο άρθρο 3 παρ.1, είναι τα δεδομένα προσωπικού χαρακτήρα τα οποία τίθενται σε επεξεργασία με αυτοματοποιημένες διαδικασίες (π.χ. τα δεδομένα που είναι αποθηκευμένα σε μία βάση δεδομένων) καθώς και αυτά που περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο και τίθενται σε μη αυτοματοποιημένη επεξεργασία (π.χ. στο χαρτί). Ενώ, στην παρ. 2 του άρθρου 3, ορίζεται ότι οι διατάξεις της Οδηγίας δεν εφαρμόζονται στην επεξεργασία δεδομένων που αφορούν τη δημόσια ασφάλεια, την άμυνα, την ασφάλεια του κράτους και το ποινικό δίκαιο καθώς και δεδομένων αποκλειστικά προσωπικών ή οικιακών δραστηριοτήτων.

Επίσης, ορίζονται οι αρχές που είναι απαραίτητο να τηρούνται για την εξασφάλιση της ποιότητας των δεδομένων καθώς και οι αρχές της νομιμότητας της επεξεργασίας (άρθρο 6 και 7 αντίστοιχα), καθορίζονται τα δικαιώματα του ατόμου του οποίου τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία με ορισμένες εξαιρέσεις και περιορισμούς (άρθρα 10-15) και προβλέπεται ότι ο υπεύθυνος της επεξεργασίας οφείλει να λαμβάνει κατάλληλα τεχνικά και οργανωτικά μέτρα ασφαλείας (άρθρο 17). Ακόμη, ορίζονται οι βασικές αρχές που πρέπει να τηρούνται για τη διαβίβαση προσωπικών δεδομένων προς τρίτες χώρες (άρθρο 25), προβλέπεται η δημιουργία από κάθε κράτος μέλος δημόσιας αρχής ελέγχου επιφορτισμένης με τον έλεγχο της εφαρμογής των εθνικών διατάξεων που έχουν θεσπισθεί (άρθρο 28) καθώς και η δημιουργία ανεξάρτητης ομάδας με συμβουλευτικό χαρακτήρα η οποία θα παρέχει στην Επιτροπή τη γνώμη της σχετικά με το επίπεδο προστασίας, θα συμβουλεύει την Επιτροπή για κάθε σχέδιο τροποποιήσεως της παρούσας Οδηγίας και θα γνωμοδοτεί επί των κωδίκων δεοντολογίας που εκπονούνται σε κοινοτικό επίπεδο (άρθρο 29).

Τέλος, δόθηκε τριετής προθεσμία σε όλα τα κράτη μέλη προκειμένου να συμμορφωθούν με τους κανόνες της Οδηγίας. Η Ελλάδα, ακολουθώντας τις υποδείξεις της Οδηγίας, θέσπισε το 1997 το νόμο 2472/1997[131] για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ο οποίος ισχύει μέχρι και σήμερα.

[131] Σχετικά με το ν. 2472/97 βλ. Μέρος δεύτερο, υποκεφάλαιο 0.

1.2. Οι Οδηγίες 2002/58/ΕΚ, 2006/24/ΕΚ και 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου

Η Οδηγία 2002/58/ΕΚ[132] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (L 201, 37) αντικατέστησε την Οδηγία 97/66/ΕΚ[133] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα (L 24, 1).

Σύμφωνα με το άρθρο 1 της εν λόγω Οδηγίας, οι διατάξεις της εξειδικεύουν και συμπληρώνουν την Οδηγία 95/46/ΕΚ, έχοντας ως στόχο "*..την εναρμόνιση των εθνικών διατάξεων που απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, και ιδίως του δικαιώματος στην ιδιωτική ζωή και την εμπιστευτικότητα, όσον αφορά την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και να διασφαλίζεται η ελεύθερη κυκλοφορία των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Κοινότητα".*

Η Οδηγία αυτή, η οποία τροποποιήθηκε με τις Οδηγίες 2006/24/ΕΚ[134,135] και 2009/136/ΕΚ[136] και είναι γνωστή και ως ePrivacy

[132] Οδηγία 2002/58/ΕΚ, διαθέσιμη στο https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32002L0058, όπως τροποποιήθηκε από την Οδηγία 2009/136/ΕΚ, διαθέσιμη στο https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32009L0136

[133] Οδηγία 97/66/ΕΚ διαθέσιμη στο https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A31997L0066

[134] Οδηγία 2006/24/ΕΚ διαθέσιμη στο https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=uriserv:OJ.L_.2006.105.01.0054.01.ELL. Σχετικά με την οδηγία βλ. Ιγγλεζάκης, Ι. (2008). Το Δίκαιο της πληροφορικής (β΄ εκδ.), εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη 2008, σελ. 264-272.

[135] Η Οδηγία 2006/24/ΕΚ ακυρώθηκε με απόφαση του Δ ΕΕ στις 8 Απριλίου το 2014, ως ασύμβατη με το ευρωπαϊκό νομικό πλαίσιο. Η απόφαση του ΔΕΕ της ακύρωσης της Οδηγίας 2006/24/ΕΚ είναι διαθέσιμη στο https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX:62012CJ0293.

[136] Οδηγία 2009/136/ΕΚ διαθέσιμη στο https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:El:PDF

Directive (ePD), ενσωματώθηκε στο ελληνικό δίκαιο με το ν. 3471/2006[137] και μετέπειτα ενσωματώθηκε και η τροποποίησή της με το ν. 4070/2012[138]. Σύμφωνα με το άρθρο 2 παράγραφος 3 της Οδηγίας 2009/136/ΕΚ (σελ. 29), με το άρθρο 169 του ν. 4070/2012 αντικαταστάθηκε η παράγραφος 1 του άρθρου 3 του ν. 3471/2006 η οποία αφορά το πεδίο εφαρμογής του νόμου και προστέθηκαν και τα δημόσια δίκτυα ηλεκτρονικών επικοινωνιών που υποστηρίζουν συσκευές συλλογής δεδομένων και ταυτοποίησης. Τέτοιες συσκευές θα μπορούσανε να είναι και ανεπαφικές συσκευές που χρησιμοποιούν ραδιοσυχνότητες, όπως οι συσκευές που φέρουν την τεχνολογία RFID, για να λαμβάνουν δεδομένα από ετικέτες RFID, τα οποία στη συνέχεια μπορούν να μεταφερθούν σε υφιστάμενα δίκτυα επικοινωνιών. Όταν λοιπόν οι συσκευές αυτές συνδέονται σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών ή χρησιμοποιούν υπηρεσίες ηλεκτρονικών επικοινωνιών εμπίπτουν στην ePD, περιλαμβανομένων των διατάξεων για την ασφάλεια, για τα δεδομένα κίνησης, τα δεδομένα θέσης και για το απόρρητο (L 337/11, αιτιολογική σκέψη 56).

Το γεγονός εάν η ePD έχει εφαρμογή για την προστασία των προσωπικών δεδομένων στις εφαρμογές της τεχνολογίας RFID, ιδίως μετά την τροποποίηση στο πεδίο εφαρμογής του νόμου έχει σχολιαστεί πολύ[139]. Η ePD συμπληρώνει τη γενική Οδηγία για την προστασία των προσωπικών δεδομένων και εφαρμόζει τις αρχές στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα σε συνδυασμό με την παροχή δημόσια διαθέσιμων

[137] Σχετικά με το ν. 3471/2006 βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2010). Νομική Διασφάλιση του Απορρήτου των Κινητών Επικοινωνιών (Η ελληνική νομική ρύθμιση ενόψει και του πρόσφατου ν. 3674/2008), σε Λαμπρινουδάκη, Κ.-Μήτρου, Λ.-Γκρίτζαλη, Σ.-Κάτσικα,Σ., Προστασία της ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, εκδ. Παπασωτηρίου, Αθήνα 2010, σελ: 667-678, Alexandropoulou-Egyptiadou, E. (2011). The Greek Regulatory Framework on confidentiality and its waiver in mobile communications (after the implementation of the Directives 1995/46, 2002/58 & 2006/24/E.C.), Hellenic Review of International Law 64 (2011), pp. 425-35, Ιγγλεζάκη Ι. (2006). Εισαγωγή στο Δίκαιο της Πληροφορικής, εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη, σελ. 195-207 και Κίτσος, Π. (2011). Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών, Διδακτορική Διατριβή, Πανεπιστήμιο Μακεδονίας, Θεσσαλονίκη.

[138] Βλ. Τάσσης Σπ. (2012). Συνοπτική παρουσίαση του νέου νόμου για τις ηλεκτρονικές επικοινωνίες (Ν. 4070/2012), ΔiΜΕΕ 2/2012, σελ: 54-60, διαθέσιμο στο http://www.tassis.com/images/publications/DiMEE_TASSHS%20%CE%BD%CE%B5%CE%BF%CF%82%20%CE%BD%CE%BF%CE%BC%CE%BF%CF%82%202012.pdf.

[139] Βλ. Kosta, E. (2012). The application of the ePrivacy Directive on RFID systems, Informatiebeveiliging, Vol. (1), pp. 4-7.

ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα επικοινωνιών. Εξαιτίας όμως αυτού του περιορισμού, πολλές εφαρμογές RFID δεν καλύπτονται και εμπίπτουν μόνο στο πεδίο της γενικής Οδηγίας προστασίας των προσωπικών δεδομένων, όπως έχει αναφέρει και η Επιτροπή σε ανακοίνωσή της[140].

1.3. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 2016/679

Είναι γεγονός ότι οι νομοθετικοί μηχανισμοί αδυνατούν να ακολουθήσουν τους ραγδαίους ρυθμούς ανάπτυξης των νέων τεχνολογιών. Οι διασυνοριακές ροές και οι ανταλλαγές δεδομένων αυξήθηκαν σημαντικά τα τελευταία χρόνια με τη χρήση των νέων τεχνολογιών και δημιούργησαν νέες προκλήσεις στην προστασία των δεδομένων προσωπικού χαρακτήρα, ενώ ταυτόχρονα αυξήθηκαν σημαντικά και οι ανησυχίες των πολιτών. Σε έρευνα του Ευρωβαρομέτρου που έγινε το 2011 σχετικά με την τάση των πολιτών όσον αφορά την προστασία των δεδομένων και της ηλεκτρονικής ταυτότητας[141], «το 70% δήλωσε ότι ανησυχεί για τους τρόπους με τους οποίους οι εταιρείες χρησιμοποιούν τα δεδομένα αυτά».

Η Ευρωπαϊκή Επιτροπή, προκειμένου να προστατέψει το θεμελιώδες δικαίωμα των ανθρώπων στην προστασία των δεδομένων προσωπικού χαρακτήρα, πρότεινε το 2012 τη σφαιρική μεταρρύθμιση των κανόνων της Οδηγίας 95/46/ΕΚ. Συγκεκριμένα, στις 25 Ιανουαρίου 2012, δημοσίευσε πρόταση Κανονισμού[142] στην οποία πρότεινε τη δημιουργία ενός πιο ισχυρού

[140] Βλ. Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των περιφερειών, «Η ραδιοσυχνική αναγνώριση (RFID) στην Ευρώπη: βήματα προς την κατεύθυνση χάραξης πλαισίου πολιτικής», {SEC(2007) 312}, COM (2007) 96 τελικό, σελ. 6, διαθέσιμη στο http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:EL:PDF.

[141] Βλ. δελτίο τύπου (IP/11/742), "Προστασία δεδομένων: σύμφωνα με νέα μελέτη, οι Ευρωπαίοι αποκαλύπτουν προσωπικά δεδομένα τους στο Διαδίκτυο, όμως εξακολουθούν να ανησυχούν για την προστασία της ιδιωτικής τους ζωής", Brussels, 16 June 2011, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-11-742_el.htm.

[142] Βλ. πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Γενικός Κανονισμός για την Προστασία Δεδομένων), COM/2012/011 final, 2012/0011 (COD), διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52012PC0011&from=EN. Επίσης βλ. Ιγγλεζάκης, Ι. (2012). Η

και ταυτόχρονα συνεκτικού πλαισίου προστασίας των προσωπικών δεδομένων με τον εκσυγχρονισμό των αρχών προστασίας, την ενίσχυση και αναλυτική περιγραφή των δικαιωμάτων των υποκειμένων και τον καθορισμό των υποχρεώσεων εκείνων που εκτελούν την επεξεργασία.

Σύμφωνα με την αντιπρόεδρο της Επιτροπής Reding V.[143] «*Η προτεινόμενη μεταρρύθμιση (…) θα κάνει τη ζωή ευκολότερη και λιγότερο δαπανηρή για τις επιχειρήσεις. Ένα στιβαρό, ευκρινές και ενιαίο νομικό πλαίσιο σε επίπεδο ΕΕ θα συντελέσει στην απελευθέρωση των δυνατοτήτων που προσφέρει η ψηφιακή ενιαία αγορά και θα ενισχύσει την οικονομική ανάπτυξη, την καινοτομία και τη δημιουργία θέσεων εργασίας*».

Ακολουθώντας την ιστορική διαδρομή για την ψήφιση του Κανονισμού[144], μετά από τέσσερα περίπου χρόνια διαβουλεύσεων και 3.999 τροπολογίες[145], στις 8 Απριλίου του 2016 το Συμβούλιο ενέκρινε τη θέση του σε πρώτη ανάγνωση σχετικά με τη μεταρρύθμιση της προστασίας των δεδομένων[146] και τελικά στις 27 Απριλίου του 2016 ψηφίστηκε ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ) 2016/679[147] ο οποίος τέθηκε σε εφαρμογή από τις 25 Μαΐου του 2018[148].

μεταρρύθμιση των κανόνων προστασίας προσωπικών δεδομένων στην ΕΕ. Η Πρόταση Κανονισμού για την αντικατάσταση της Οδηγίας 95/46/ΕΚ, ΣΥΝήΓΟΡΟΣ 92/2012, σελ: 72-75, Ιγγλεζάκης, Ι. (2012). Ζητήματα εναρμόνισης της νομοθεσίας για την προστασία προσωπικών δεδομένων στην ΕΕ, ΔiΜΕΕ 4/2012, σελ: 477-481.

[143] Βλ. δελτίο τύπου (IP/12/46), Η Επιτροπή προτείνει τη σφαιρική μεταρρύθμιση των κανόνων περί προστασίας δεδομένων με σκοπό την αύξηση του ελέγχου που οι χρήστες ασκούν επί των δεδομένων τους και τη μείωση των εξόδων για τις επιχειρήσεις, Brussels, 25 January 2012, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-12-46_el.htm

[144] Περισσότερες πληροφορίες σχετικά με το χρονολόγιο των διαδικασιών από την πρόταση Κανονισμού μέχρι και την εφαρμογή του διαθέσιμες στο http://www.consilium.europa.eu/el/policies/data-protection-reform/data-protection-regulation/.

[145] Βλ. Μήτρου, Λ. (2017). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, Νέο δίκαιο - νέες υποχρεώσεις - νέα δικαιώματα, Εκδόσεις Σάκκουλα Α.Ε., σημ. 93 και Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2018). Η προστασία των προσωπικών δεδομένων ανηλίκων στο Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679, ΔiΜΕΕ 1/2018, σελ: 6.

[146] Βλ. δελτίο τύπου 171/16, Μεταρρύθμιση της προστασίας των δεδομένων: το Συμβούλιο εγκρίνει τη θέση του σε πρώτη ανάγνωση, (08/04/2016) διαθέσιμο στο http://www.consilium.europa.eu/el/press/press-releases/2016/04/08/data-protection-reform-first-reading/pdf

[147] 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), διαθέσιμος στο http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL. Επίσης σχετικά βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2018). Ο Γενικός Κανονισμός Προστασίας Δεδομένων

Οι σημαντικότερες καινοτόμες ρυθμίσεις του Κανονισμού είναι[149]:

- η διεύρυνση του πεδίου εφαρμογής (άρθρο 3, παρ. 2)
- η εισαγωγή νέων δικαιωμάτων του υποκειμένου (π.χ. δικαίωμα διαγραφής/ δικαίωμα στη λήθη[150], δικαίωμα στη φορητότητα)
- η προσθήκη νέων αρχών επεξεργασίας (όπως της διαφάνειας, της λογοδοσίας, της ακεραιότητας και της εμπιστευτικότητας)
- το ενισχυμένο πλέγμα υποχρεώσεων του υπευθύνου επεξεργασίας (όπως η λογοδοσία, η γνωστοποίηση παραβιάσεων προσωπικών δεδομένων στην Εποπτική Αρχή και στο υποκείμενο, η προστασία των δεδομένων ήδη από το σχεδιασμό της επεξεργασίας και εξ ορισμού: privacy by design/ privacy by default[151] και η εκτίμηση αντικτύπου όταν η επεξεργασία ενέχει σοβαρούς κινδύνους για τα προσωπικά δεδομένα)
- η αύξηση των υποχρεώσεων του εκτελούντος την επεξεργασία

2016/679/ΕΕ - Προκλήσεις εφαρμογής, Πρακτικά 1ου διεπιστημονικού συνεδρίου «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ» Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής, Νομική Σχολή ΔΠΘ, Κομοτηνή 25-26 Μαΐου, σελ. 17-30, Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2018). Η προστασία των προσωπικών δεδομένων πριν και μετά τον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679/ΕΕ, Πρακτικά 9ου Συνεδρίου ΕΕΝ e-Θέμις: Προσωπικά δεδομένα και δικηγορία (Ιωάννινα 11-12/5/2018), εκδ. Νομική Βιβλιοθήκη, Αθήνα, Ιγγλεζάκης, Ι. (2018). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679) - Εισαγωγή στο νέο νομικό πλαίσιο προστασίας προσωπικών δεδομένων, εκδ. Interactive και Παναγοπούλου-Κουτνατζή Φ. (2017). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 679/2016/ΕΕ. Εισαγωγή και Προστασία Δικαιωμάτων, ISBN/ISSN: 978-960-568-740-3, Εκδόσεις Σάκκουλα Α.Ε..

[148] Επίσημη ιστοσελίδα https://www.eugdpr.org/.

[149] Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2018). Η προστασία των προσωπικών δεδομένων ανηλίκων στο Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679, ΔiΜΕΕ 1/2018, σελ: 6.

[150] Σχετικά με το δικαίωμα στη λήθη βλ. Ιγγλεζάκης Ι. (2012). Το δικαίωμα στην ψηφιακή λήθη σύμφωνα με την πρόταση Κανονισμού της ΕΕ για την προστασία δεδομένων, ΣΥΝήΓΟΡΟΣ 94/2012, σελ. 76-79, Ιγγλεζάκης Ι. (2012). Το δικαίωμα στην ψηφιακή λήθη και οι περιορισμοί του, εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη, Παναγοπούλου-Κουτνατζή Φ. (2016). Η εξέλιξη του δικαιώματος στη λήθη (περί λήθης της λήθης;), Εφημερίδα Διοικητικού Δικαίου, 6/2016, σελ. 714-728, Παναγοπούλου-Κουτνατζή Φ. (2012). Το δικαίωμα στη λήθη στην εποχή της αβάσταχτης μνήμης: Σκέψεις αναφορικά με την Πρόταση Κανονισμού Προστασίας Δεδομένων, Εφημερίδα Διοικητικού Δικαίου, 2/2012, σελ. 264-278, Iglezakis I. (2014). The Right to Be Forgotten in the Google Spain Case (Case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet?, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472323 και Bouchagiar G., Botti M. (2018). THE RIGHT TO BE FORGOTTEN: Memory holes as the default?, Amsterdam Privacy Conference, Amsterdam, The Netherlands, 2018, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3226404

[151] Σχετικά με την προστασία των δεδομένων ήδη από το σχεδιασμό της επεξεργασίας και εξ ορισμού βλ. Ιγγλεζάκης, Ι. (2013). Προστασία δεδομένων προσωπικού χαρακτήρα από τον σχεδιασμό και εξ ορισμού, ΣΥΝήΓΟΡΟΣ 96/2013, σελ: 79-95, Ιγγλεζάκης, Ι. (2018). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679).., ό.π. σελ. 78-79 και Μήτρου, Λ. (2013). Privacy by Design. Η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων, ΔiΜΕΕ 1/2013, σελ:14-25. Επίσης βλ. παρακάτω Μέρος δεύτερο, υποκεφάλαιο 1.3.1.

- ο θεσμός του υπευθύνου προστασίας δεδομένων
- οι ειδικές προστατευτικές ρυθμίσεις για τα προσωπικά δεδομένα των παιδιών
- η ρητή δυνατότητα ανάκλησης της συγκατάθεσης του υποκειμένου
- η απάλειψη της γενικής υποχρέωσης δήλωσης της επεξεργασίας στην Εποπτική Αρχή ή λήψης της σχετικής άδειας
- η σύσταση του Ευρωπαϊκού Συμβουλίου Προστασίας δεδομένων[152]
- ο μηχανισμός συνεκτικότητας
- η ενθάρρυνση για θέσπιση μηχανισμών πιστοποίησης και
- η αυστηροποίηση των κυρώσεων

Η Ελλάδα ακολουθώντας τις υποδείξεις του Κανονισμού θέσπισε το νόμο 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 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» (βλ. Μέρος Δεύτερο, υποκεφάλαιο 6.4).

1.3.1. Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (Ο.Ο.Σ.Α.) ήδη σε κείμενό του το 2008[153] είχε αναφέρει ότι η προστασία εκ σχεδιασμού (privacy by design) θα διευκολύνει σημαντικά την προστασία της ιδιωτικότητας

[152] Το Ευρωπαϊκό Συμβούλιο Προστασίας δεδομένων θα αντικαταστήσει την Ομάδα εργασίας του άρθρου 29. Βλ. καθήκοντα του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων στο άρθρο 70 του Κανονισμού. Επίσης, σύμφωνα με άρθρο 94 του Κανονισμού οι παραπομπές στην Ομάδα εργασίας του άρθρου 29 στην καταργούμενη Οδηγία 95/46/ΕΚ, θεωρούνται παραπομπές στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων που συστήνεται με τον παρόντα Κανονισμό.

[153] OECD (2008), OECD Policy Guidance on Radio Frequency Identification (RFID), Ministerial Meeting on the future of the meeting economy, Seoul, Korea, 17-18 June, διαθέσιμο σε http://www.oecd.org/sti/ieconomy/oecdpolicyguidanceonradiofrequencyidentificationrfid.htm. Επίσης σχετικά με τη συμβολή του Ο.Ο.Σ.Α. στην υιοθέτηση ενός πλαισίου για την προστασία της ιδιωτικής ζωής και των δεδομένων από τις εφαρμογές RFID βλ. Μέρος δεύτερο, Κεφάλαιο 3.

και θα ενισχύσει την εμπιστοσύνη των καταναλωτών. Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων το ίδιο έτος σε γνωμοδότησή[154] του είχε προτείνει την ανάπτυξη τεχνικών και προτύπων βασισμένων στην προστασία της ιδιωτικής ζωής εκ σχεδιασμού. Η Ομάδα εργασίας του άρθρου 29 είχε προτείνει το 2009[155] την εισαγωγή της αρχής προστασίας της ιδιωτικότητας εκ σχεδιασμού στο πλαίσιο προστασίας των δεδομένων προσωπικού χαρακτήρα για την αντιμετώπιση των κινδύνων που προκύπτουν από την τεχνολογική ανάπτυξη. Το 2011 στην αναθεωρημένη πρόταση πλαισίου[156] για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID, παρατηρείται ότι συνιστάται η εφαρμογή του εν λόγω πλαισίου έγκαιρα από το στάδιο σχεδιασμού και ανάπτυξης του συστήματος. Ενώ και η Ευρωπαία Επίτροπος Reding V. είχε αναφέρει σε μία ομιλία της το 2012[157] ότι είναι απαραίτητο να εισαχθεί η έννοια της προστασίας της ιδιωτικότητας εκ σχεδιασμού ως κανόνας, εξαιτίας της αβεβαιότητας των επιπτώσεων των νέων τεχνολογιών στις ζωές των ανθρώπων. Η σχετική ρύθμιση περιλήφθηκε στο άρθρο 23 της πρότασης Κανονισμού.

Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων, Hustinx P., σε γνώμη[158] του εξέφρασε την ικανοποίησή του στο γεγονός ότι στην πρόταση

[154] Βλ. Γνωμοδότηση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων όσον αφορά την ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, η ραδιοσυχνική αναγνώριση (RFID) στην Ευρώπη: βήματα προς την κατεύθυνση χάραξης πλαισίου πολιτικής COM(2007) 96, (2008/C 101/01), διαθέσιμη στο https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EL.pdf. Επίσης βλ. Μέρος δεύτερο, Κεφάλαιο 4.

[155] Βλ. Μήτρου Λ. (2007). Privacy by design. Η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων, ΔΙΜΕΕ, 2013 (1), σελ. 21 και συγκεκριμένα υποσημείωση 47, και Article 29 Data Protection Working Party (WP 168), The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, σελ: 12, διαθέσιμο στο http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

[156] Βλ. λεπτομέρειες σχετικά με το αναθεωρημένο πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID, στο Μέρος δεύτερο Κεφάλαιο 5.

[157] Βλ. Μήτρου Λ. (2007), Privacy by design. Η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων, ό.π. σελ: 20 και ιδίως υποσημείωση 40 και ομιλία της Reding V. (SPEECH/12/26), The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, 22 January 2012, διαθέσιμη στο http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm

[158] Βλ. EDPS, Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012, σελ: 29, παρ. 177-181, διαθέσιμη στο http://www.europarl.europa.eu/document/activities/cont/201205/20120524ATT45776/20120524ATT45776EN.pdf

Κανονισμού συμπεριλήφθηκε η προστασία των προσωπικών δεδομένων εκ σχεδιασμού. Όμως, τόνισε και ότι δεν είναι ξεκάθαρη η εφαρμογή της και δεν προσθέτει κάτι παραπάνω στις αρχές επεξεργασίας έτσι όπως περιγράφεται, παρά μόνο επιβεβαιώνει ότι πρέπει να ληφθούν υπόψη κατά τον σχεδιασμό της τεχνολογίας. Επίσης συμβουλεύει ότι, εφόσον σκοπός είναι η προστασία των υποκειμένων όταν υπάρχει έλλειψη κατανόησης της επεξεργασίας, οφείλει να προστεθεί ότι τα μέτρα που θα ληφθούν πρέπει να περιοριστούν στην απλή χρήση ενός προϊόντος και να δοθεί στο υποκείμενο η δυνατότητα επιλογής.

Επίσης, θα έπρεπε οι προαναφερόμενες υποχρεώσεις να αφορούν τόσο τους υπεύθυνους επεξεργασίας όσο και τους σχεδιαστές της τεχνολογίας[159]. Κάτι τέτοιο κρίνεται απαραίτητο διότι αυτοί οι οποίοι κατασκευάζουν μία τεχνολογία είναι σημαντικό να προσχεδιάσουν και να καθορίζουν τις απαραίτητες τεχνολογικές ρυθμίσεις.

Ο Κανονισμός αναφέρεται στην προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού στο άρθρο 25 (privacy by design and privacy by default)[160]. Συγκεκριμένα, καθορίζονται οι υποχρεώσεις του υπευθύνου επεξεργασίας εφαρμογής «*κατάλληλ[ων] τεχνικ[ών] και οργανωτι[κών] μέτρ[ων], όπως η ψευδωνυμοποίηση, σχεδιασμέν[ων] 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*». Ειδικότερα, στην παρ. 2 επιβάλλεται στον υπεύθυνο επεξεργασίας να «*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,*

[159] Μήτρου, Λ. (2013). Privacy by Design. Η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων, ΔiΜΕΕ 1/2013, σελ: 21.

[160] Η αρχή της προστασίας δεδομένων ήδη από το σχεδιασμό και εξ ορισμού «*συμπληρώνει τις ουσιαστικές ρυθμίσεις με τις οποίες προστατεύεται η ιδιωτική ζωή και τα προσωπικά δεδομένα του ατόμου*.», βλ. Ιγγλεζάκης, Ι. (2018). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679).., ό.π. σελ. 78.

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».

Ακόμη, στην αιτιολογική σκέψη 78, αναφέρεται ότι απαιτείται η λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων, τόσο κατά τον σχεδιασμό της επεξεργασίας όσο και κατά την ίδια την επεξεργασία, ώστε να διασφαλίζεται η σωστή εφαρμογή των αρχών της προστασίας των δεδομένων. Ο υπεύθυνος επεξεργασίας «*προκειμένου να μπορεί να αποδείξει συμμόρφωση προς τον παρόντα κανονισμό θα πρέπει να θεσπίζει εσωτερικές πολιτικές και να εφαρμόζει μέτρα τα οποία ανταποκρίνονται ειδικότερα στις αρχές της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού*».

Ολοκληρώνοντας αναφορικά με τον ΓΚΠΔ και τις καινοτόμες ρυθμίσεις του σχετικά με τη προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, αξίζει να αναφερθεί πως μετά τη ψήφισή του, στο άρθρο 35 δίνονται οδηγίες για τη διενέργεια εκτίμησης αντικτύπου[161] σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα από τους υπεύθυνους επεξεργασίας, δηλαδή εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα, πριν γίνει η επεξεργασία[162]. Είναι άξιο αναφοράς και το γεγονός ότι στην Ελλάδα, σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ, δημοσιεύτηκε κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων (ΦΕΚ Β΄

[161] Περισσότερες λεπτομέρειες σχετικά με την εκτίμηση αντικτύπου βλ. Ιγγλεζάκης, Ι. (2018). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679).., ό.π. σελ. 91.

[162] Σύμφωνα με τον Ζωγραφόπουλο Δ. Γ. (2017, σελ. 43, υποσημ. 2), η ελληνική ΑΠΔΠΧ θεωρεί ότι η υποχρέωση του υπεύθυνου επεξεργασίας για τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα δεν είναι καινοτομία, καθώς προκύπτει ερμηνευτικά και από τις διατάξεις της Οδηγίας 95/46/ΕΚ και εκείνες του ν. 2472/1997, ως παράδειγμα βλ. Γνωμοδότηση ΑΠΔΠΧ 1/2017 σχετικά με τη γνωστοποίηση επεξεργασίας προσωπικών δεδομένων στο πλαίσιο του ηλεκτρονικού εισιτηρίου του Ο.Α.Σ.Α., ιδίως Σκέψεις υπ' αρ. (3), διαθέσιμη στο https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwiWn6yC2LreAhUExYsKHWxHBJEQFjABegQIAxAC&url=http%3A%2F%2Fwww.dpa.gr%2FAPDPXPortlets%2Fhtdocs%2FdocumentDisplay.jsp%3Fdocid%3D234%2C52%2C89%2C47%2C103%2C69%2C62%2C94&usg=AOvVaw0mj9QxP9_qHZOC7WEhlHsd.

1622/10-5-2019)[163]. Ο κατάλογος αυτός βασίζεται στο άρθρο 35 του ΓΚΠΔ και ιδίως στις παρ. 1 και 3 καθώς και στις "Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του Κανονισμού 2016/679"[164] που εξέδωσε η Ομάδα εργασίας του άρθρου 29.

2. Η γνώμη της Ομάδας εργασίας του άρθρου 29 σχετικά με τις πρόσφατες εξελίξεις στο διαδίκτυο των πραγμάτων

Η τεχνολογία RFID, όπως έχει ήδη προαναφερθεί, είναι μία από τις υφιστάμενες εφαρμογές του ΔτΠ, όπου το διαδίκτυο δε συνδέει πλέον μονάχα υπολογιστές και τερματικά, όπως έκανε στο παρελθόν, αλλά συνδέει και οποιοδήποτε άλλο αντικείμενο με πρόσωπα και αντικείμενο με αντικείμενο. Επομένως, όπως αναφέρει και η Επιτροπή σε σχετική ανακοίνωσή της[165] για το σχέδιο δράσης για την Ευρώπη για το ΔτΠ, το ΔτΠ δεν μπορεί να χαρακτηριστεί ως μια απλή επέκταση του γνωστού ως σήμερα διαδικτύου αλλά ως μία σειρά από νέα ανεξάρτητα συστήματα τα οποία λειτουργούν με δικές τους υποδομές και εν μέρει στηρίζονται και στις υπάρχουσες υποδομές του διαδικτύου.

Απαραίτητη προϋπόθεση για την υιοθέτηση τέτοιων εφαρμογών, όπως την τεχνολογία RFID, και κατ' επέκταση του ΔτΠ είναι η λήψη των κατάλληλων μέτρων προστασίας των δεδομένων που υφίστανται επεξεργασία. Επομένως, προσδιορίζοντας καταρχήν τους κινδύνους από εφαρμογές της τεχνολογίας

[163] Βλ. ΦΕΚ Β΄ 1622/10-5-2019, διαθέσιμο στο https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/GDPR/FILES%20GDPR/%CE%A6%CE%95%CE%9A%20%CE%92%CE%84%20162210-5-2019.PDF

[164] Βλ. "Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του Κανονισμού 2016/679", WP 248, ό.π. σελ. 26

[165] Βλ. Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των περιφερειών, Το Ίντερνετ των πραγμάτων-Ένα σχέδιο δράσης για την Ευρώπη, COM(2009) 278 τελικό, διαθέσιμη στο http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2009)0278_/com_com(2009)0278_el.pdf

RFID που επηρεάζουν την αξιοπιστία της και λαμβάνοντας τα κατάλληλα μέτρα προστασίας των δεδομένων, κατανοούνται και οι κίνδυνοι κατά της ασφάλειας και της προστασίας της ιδιωτικότητας στο ΔτΠ και αυξάνεται η αξιοπιστία του και επομένως και η κοινωνική του αποδοχή[166].

Η Επιτροπή, ήδη από το 2007 σε ανακοίνωσή της[167], είχε εκφράσει τον προβληματισμό της σχετικά με τον ανοιχτό χαρακτήρα και την ουδετερότητα των βάσεων δεδομένων όπου θα καταγράφονται οι μοναδικοί αναγνωριστικοί κωδικοί που βρίσκονται στη βάση του συστήματος RFID και την αποθήκευση και το χειρισμό των συλλεγόμενων δεδομένων, συμπεριλαμβανομένης της χρήσης τους από τρίτους, καθώς ενδέχεται να δημιουργηθεί μία παγκόσμια δικτυωμένη επικοινωνιακή δομή, όπως αυτή του ΔτΠ.

Επειδή η ανάπτυξη του ΔτΠ παρουσιάζει νέους κινδύνους και προκλήσεις για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής λόγω του αυξανόμενου συνεχώς όγκου των διακινούμενων δεδομένων, το Σεπτέμβριο του 2014 η Ομάδα εργασίας του άρθρου 29 εξέδωσε γνώμη για τις πρόσφατες εξελίξεις στο ΔτΠ. Στην εν λόγω γνώμη, προσδιορίζονται οι κυριότεροι κίνδυνοι που απειλούν την προστασία των δεδομένων στο ΔτΠ και παρέχεται καθοδήγηση για τον τρόπο εφαρμογής του νομικού πλαισίου της ΕΕ. Συγκεκριμένα, ορισμένες από τις συστάσεις που έκανε οι οποίες σχετίζονται με την εφαρμογή της τεχνολογίας RFID, είναι οι εξής[168]:

- πριν από την υλοποίηση οποιασδήποτε νέας εφαρμογής στο ΔτΠ, πρέπει να πραγματοποιούνται ενέργειες για την εκτίμηση των επιπτώσεων για την προστασία της ιδιωτικής ζωής, όπως αυτές που προτάθηκαν και εγκρίθηκαν από την Ομάδα εργασίας του άρθρου 29

[166] Βλ. Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των περιφερειών, Το Ίντερνετ των πραγμάτων-Ένα σχέδιο δράσης για την Ευρώπη, ό.π. σελ 6-8.

[167] Βλ. Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των περιφερειών , «Η ραδιοσυχνική αναγνώριση (RFID) στην Ευρώπη: βήματα προς την κατεύθυνση χάραξης πλαισίου πολιτικής», ό.π., σελ. 8, διαθέσιμη στο http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:EL:PDF

[168] Βλ. Γνώμη 8/2014 σχετικά με τις πρόσφατες εξελίξεις στο διαδίκτυο των πραγμάτων, 1471/14/EL, WP 223, 6 Σεπτεμβρίου, σελ. 26-30, διαθέσιμη στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_el.pdf

στο πλαίσιο[169] εκτίμησης των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων για τις εφαρμογές RFID

- τα ενδιαφερόμενα μέρη πρέπει να διαγράφουν τα ακατέργαστα δεδομένα αμέσως μετά την εξαγωγή των δεδομένων που είναι απαραίτητα για την επεξεργασία δεδομένων που εκτελούν
- κάθε ενδιαφερόμενο μέρος πρέπει να εφαρμόζει τις αρχές της προστασίας της ιδιωτικής ζωής ήδη από τον σχεδιασμό και της προστασίας της ιδιωτικής ζωής βάσει προεπιλεγμένων ρυθμίσεων
- οι μέθοδοι της παροχής πληροφοριών και της παροχής του δικαιώματος άρνησης ή αίτησης συγκατάθεσης θα πρέπει να είναι όσο το δυνατόν πιο προσιτές για το χρήστη και οι πολιτικές ενημέρωσης και συγκατάθεσης πρέπει να επικεντρώνονται σε πληροφορίες που είναι κατανοητές
- οι κατασκευαστές συσκευών πρέπει να ενημερώνουν τους χρήστες για το είδος των δεδομένων που συλλέγονται και υποβάλλονται σε περαιτέρω επεξεργασία καθώς επίσης και για τον τρόπο με τον οποίο τα δεδομένα αυτά θα υποβληθούν σε επεξεργασία και θα συνδυαστούν
- οι κατασκευαστές συσκευών πρέπει να έχουν τη δυνατότητα να ενημερώνουν όλα τα άλλα ενδιαφερόμενα μέρη μόλις ένα πρόσωπο στο οποίο αναφέρονται τα δεδομένα ανακαλέσει τη συγκατάθεσή του ή εκφράσει την αντίρρησή του για την επεξεργασία των δεδομένων
- προκειμένου να επιβάλλεται η διαφάνεια και ο έλεγχος από τους χρήστες, οι κατασκευαστές συσκευών πρέπει να παρέχουν εργαλεία που θα επιτρέπουν την τοπική ανάγνωση, επεξεργασία και τροποποίηση των δεδομένων πριν αυτά διαβιβαστούν σε οποιονδήποτε υπεύθυνο επεξεργασίας δεδομένων
- οι χρήστες έχουν δικαίωμα πρόσβασης στα προσωπικά τους δεδομένα, επομένως πρέπει να τους παρέχονται εργαλεία που θα τους

[169] Βλ. Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 Ιανουαρίου 2011, διαθέσιμο στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf.

επιτρέπουν να εξαγάγουν εύκολα τα δεδομένα σε δομημένη και κοινά χρησιμοποιούμενη μορφή

- οι κατασκευαστές συσκευών πρέπει να περιορίζουν στο μέτρο του δυνατού τον όγκο των δεδομένων που αντλούνται από συσκευές, μέσω της μετατροπής των ακατέργαστων δεδομένων σε συγκεντρωτικά δεδομένα απευθείας στη συσκευή
- οι κατασκευαστές συσκευών πρέπει να συνεργαστούν με οργανισμούς τυποποίησης και πλατφόρμες δεδομένων για να υποστηρίξουν ένα κοινό πρωτόκολλο βάσει του οποίου θα εκφράζονται προτιμήσεις ως προς τη συλλογή και την επεξεργασία δεδομένων από υπεύθυνους της επεξεργασίας, ιδίως όταν τα δεδομένα αυτά συλλέγονται από συσκευές που δεν γίνονται αντιληπτές
- πρέπει να σχεδιαστούν ανακοινώσεις ή προειδοποιήσεις προκειμένου να υπενθυμίζεται συχνά στους χρήστες ότι πραγματοποιείται συλλογή δεδομένων από αισθητήρες
- οι εφαρμογές πρέπει να διευκολύνουν τα πρόσωπα στα οποία αναφέρονται τα δεδομένα ώστε να ασκούν τα δικαιώματα πρόσβασης, τροποποίησης και διαγραφής των προσωπικών πληροφοριών που συλλέγονται από συσκευές του ΔτΠ
- οι σχεδιαστές εφαρμογών πρέπει να εφαρμόζουν την αρχή της ελαχιστοποίησης των δεδομένων. Εάν ο επιδιωκόμενος σκοπός μπορεί να επιτευχθεί με τη χρήση συγκεντρωτικών δεδομένων, οι σχεδιαστές δεν πρέπει να έχουν πρόσβαση στα ακατέργαστα δεδομένα. Γενικότερα, οι σχεδιαστές πρέπει να ακολουθούν την προσέγγιση της προστασίας της ιδιωτικής ζωής ήδη από το στάδιο του σχεδιασμού και να ελαχιστοποιούν τον όγκο των συλλεγόμενων δεδομένων στο επίπεδο που είναι απαραίτητο για την παροχή της υπηρεσίας

Οι παραπάνω συστάσεις κρίνεται σημαντικό να ληφθούν υπόψη για τη δημιουργία ειδικής ρύθμισης της χρήσης της τεχνολογίας RFID στην ελληνική έννομη τάξη.

3. Η συμβολή του Ο.Ο.Σ.Α. στην υιοθέτηση ενός πλαισίου για την προστασία της ιδιωτικής ζωής και των δεδομένων από εφαρμογές των συστημάτων RFID

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (Ο.Ο.Σ.Α.), δημιουργήθηκε το 1948 ως Οργανισμός Ευρωπαϊκής Οικονομικής Συνεργασίας και έπειτα το 1961 με νέα Σύμβαση[170] ανασυστήθηκε και μετασχηματίστηκε στον Ο.Ο.Σ.Α. που λειτουργεί μέχρι και σήμερα. Η αποστολή του οργανισμού είναι να βελτιώσει την οικονομική και κοινωνική ευημερία των ανθρώπων σε όλο τον κόσμο και προκειμένου να πετύχει το στόχο του, παρέχει ένα φόρουμ συζητήσεων για τις κυβερνήσεις για να συνεργάζονται, να μοιράζονται τις εμπειρίες τους και να αναζητούν λύσεις σε κοινά προβλήματα που αντιμετωπίζουν[171].

Ο Ο.Ο.Σ.Α. έχει παίξει καθοριστικό ρόλο στη διασφάλιση της ιδιωτικότητας ως θεμελιώδους αξίας αλλά και προαπαιτούμενου για την ελεύθερη διασυνοριακή ροή των προσωπικών δεδομένων. Για πρώτη φορά το 1980 πρότεινε οκτώ κατευθυντήριες αρχές για την προστασία της ιδιωτικής ζωής και τη διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα, οι οποίες έχουν αποτελέσει τη βάση των περισσότερων νόμων για την προστασία των δεδομένων προσωπικού χαρακτήρα. Έπειτα το 2013, έγινε αναθεώρηση[172] των κατευθυντήριων γραμμών για την προστασία των προσωπικών δεδομένων και τη διασυνοριακή ροή τους, η οποία αναφέρεται και στην

[170] Η Σύμβαση για την ανασύσταση και το μετασχηματισμού του Ο.Ο.Σ.Α. είναι διαθέσιμη στο http://www.oecd.org/general/conventionontheorganisationforeconomicco-operationanddevelopment.htm

[171] Περισσότερες πληροφορίες διαθέσιμες στην επίσημη ιστοσελίδα του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (Ο.Ο.Σ.Α.) http://www.oecd.org/about/.

[172] OECD (2013), The OECD Privacy Framework (2013), διαθέσιμο στο http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

τεχνολογία RFID ως μία από τις τεχνολογικές εξελίξεις που μπορεί να τα αποκαλύψει σε τρίτους προσωπικά δεδομένα τα οποία φέρουν οι ετικέτες[173].

Ο Ο.Ο.Σ.Α., στις ετήσιες εκδόσεις του βιβλίου "Προοπτικές της Τεχνολογίας της Πληροφορίας" (Information Technology Outlook) τα έτη 2004[174] και 2006[175], αναφέρεται στην τεχνολογία RFID ως ένα νέο σύστημα παρακολούθησης το οποίο παρέχει πολλές δυνατότητες σε χαμηλό κόστος το οποίο όμως ταυτόχρονα εγείρει και έντονες ανησυχίες για την ιδιωτικότητα. Και στην ετήσια έκδοση του 2008[176] τονίζει ότι μία από τις σημαντικότερες αδυναμίες είναι η έλλειψη συνέπειας όσον αφορά τις πολιτικές αξιολόγησης και εκτίμησης.

Πίνακας 8 Πινακοποίηση των βημάτων του Ο.Ο.Σ.Α. προς την υιοθέτηση ενός πλαισίου για την προστασία της ιδιωτικής ζωής και των δεδομένων από τις εφαρμογές RFID

ΕΤΟΣ	ΤΙΤΛΟΣ
2004	Emerging Technology Applications, in OECD, Information Technology Outlook 2004, OECD Publishing, Paris
2006	Emerging Technology Applications, in OECD, OECD Information Technology Outlook 2006, OECD Publishing, Paris.
2006	Radio-Frequency Identification: Drivers, Challenges and Public Policy Considerations
2007	Radio Frequency Identification Implementation in Germany: Challenges and Benefits
2008	ICT Policy Developments, in OECD, OECD Information Technology Outlook 2008, OECD Publishing, Paris
2008	OECD Policy Guidance on Radio Frequency Identification (RFID)
2013	The OECD privacy framework

Από το 2005, ο Ο.Ο.Σ.Α. ξεκίνησε συζητήσεις και πραγματοποίησε μελέτες σχετικά με την ανάπτυξη και την ένταξη της τεχνολογίας RFID στη ζωή και μάλιστα στην καθημερινότητα των ανθρώπων, χωρίς να τίθεται σε

[173] Βλ. OECD (2013), The OECD Privacy Framework (2013), ό.π. σελ: 84.
[174] OECD (2004), "Emerging Technology Applications", in OECD, Information Technology Outlook 2004, OECD Publishing, Paris, pp. 272-275, doi: http://dx.doi.org/10.1787/it_outlook-2004-9-en.
[175] OECD (2006), "Emerging Technology Applications", in OECD, OECD Information Technology Outlook 2006, OECD Publishing, Paris, pp. 248-252, doi: http://dx.doi.org/10.1787/it_outlook-2006-9-en και περίληψη στα ελληνικά διαθέσιμη στο: http://www.oecd.org/sti/ieconomy/37765618.pdf.
[176] OECD (2008), "ICT Policy Developments", in OECD, OECD Information Technology Outlook 2008, OECD Publishing, Paris, pp. 307, doi: http://dx.doi.org/10.1787/it_outlook-2008-9-en

κίνδυνο η ιδιωτική τους ζωή. Συγκεκριμένα, το 2006 σε κείμενό[177] του παρουσίασε τις προκλήσεις που υπάρχουν και εμποδίζουν την υιοθέτηση της τεχνολογίας RFID και το 2007[178] μελέτησε τα οφέλη αλλά και τα προβλήματα που μπορεί να προκύψουν από τη χρήση της τεχνολογίας RFID σε διάφορους τομείς στη Γερμανία, όπως στην αυτοκινητοβιομηχανία, στον τομέα του λιανικού εμπορίου και των καταναλωτικών αγαθών, στον τομέα των αεροπορικών μεταφορών, στον τομέα της δασοκομίας και στο νοσοκομειακό τομέα.

Έπειτα, το 2008 πρότεινε την ανάπτυξη αντίληψης σχετικά με την ασφάλεια των συστημάτων που χρησιμοποιούν την τεχνολογία RFID και τη δημιουργία κουλτούρας όσον αφορά την προστασία της ιδιωτικότητας. Γι' αυτό το λόγο, δημοσίευσε ένα σχετικό έγγραφο με οδηγίες για τη σωστή εφαρμογή της τεχνολογίας RFID το οποίο χώρισε σε τρία επιμέρους κείμενα. Στο πρώτο κείμενο προτείνει κατευθυντήριες αρχές άσκησης πολιτικής σχετικά με την ανάπτυξη και την εφαρμογή της τεχνολογίας RFID, στο δεύτερο κείμενο δίνει έμφαση στην ασφάλεια των πληροφοριών και στην προστασία της ιδιωτικότητας από τη χρήση της τεχνολογίας RFID και στο τρίτο κείμενο παρουσιάζει τις εφαρμογές της τεχνολογίας RFID που είχαν αναπτυχθεί μέχρι τότε.

Αναλυτικότερα, στο πρώτο κείμενο[179] πρότεινε δεκατέσσερις κατευθυντήριες αρχές άσκησης πολιτικής σχετικά με την ανάπτυξη και την εφαρμογή της τεχνολογίας RFID αναδεικνύοντας τα πλεονεκτήματά της και ταυτόχρονα λαμβάνοντας υπόψη και τα πιθανά προβλήματα που μπορεί να προκύψουν. Οι πρώτες έξι πρακτικές αφορούν κυβερνητικές και επιχειρησιακές πολιτικές και πρακτικές για τη χρήση της τεχνολογίας αξιοποιώντας τα πλεονεκτήματά της και οι υπόλοιπες παρέχουν καθοδήγηση

[177] OECD (2006), Radio-Frequency Identification: Drivers, Challenges and Public Policy Considerations, [DSTI/ICCP(2005)19/FINAL], διαθέσιμο σε http://www.oecd.org/internet/consumer/36323191.pdf

[178] OECD (2007), Radio Frequency Identification Implementation in Germany: Challenges and Benefits, [DSTI/ICCP/IE(2007)6/FINAL], διαθέσιμο σε https://www.oecd.org/germany/39693586.pdf

[179] OECD (2008), OECD Policy Guidance on Radio Frequency Identification (RFID), Ministerial Meeting on the future of the meeting economy, Seoul, Korea, 17-18 June, p.p. 3-10, διαθέσιμο σε http://www.oecd.org/sti/ieconomy/oecdpolicyguidanceonradiofrequencyidentificationrfid.htm

για την εφαρμογή των αρχών προστασίας της ιδιωτικότητας και αφορούν όλους τους ενδιαφερομένους. Πιο αναλυτικά,

1. Η πρώτη πρακτική αφορά την υποστήριξη από την κυβέρνηση και την παροχή κινήτρων για έρευνα και ανάπτυξη εφαρμογών συσχετιζόμενων με την τεχνολογία RFID και ταυτόχρονα ανάπτυξη και αποδοτικών μέτρων προστασίας της ιδιωτικότητας.
2. Η δεύτερη πρακτική αναφέρεται στην εφαρμογή της αρχής της ουδετερότητας, δηλαδή τη στάση ουδετερότητας που οφείλει να διατηρεί η κυβέρνηση απέναντι στην ανάπτυξη οποιασδήποτε τεχνολογίας ώστε να μην επισκιάσει την ανάπτυξη άλλων τεχνολογιών.
3. Η τρίτη πρακτική επισημαίνει ότι η κυβέρνηση λειτουργεί ως υπόδειγμα, δηλαδή παράδειγμα προς μίμηση, και γι’ αυτό είναι σημαντικό να μοιράζεται τις εμπειρίες της.
4. Η τέταρτη πρακτική τονίζει την ανάγκη για αύξηση της ευαισθητοποίησης και της ενημέρωσης σχετικά με τα πλεονεκτήματα αλλά και τις προκλήσεις της τεχνολογίας RFID.
5. Στην πέμπτη πρακτική προτείνεται η ανάπτυξη διεθνών προτύπων, τα οποία θα διευκολύνουν στη διατήρηση της ασφάλειας των πληροφοριών και της ιδιωτικότητας από τα πρώτα στάδια του σχεδιασμού των εφαρμογών.
6. Η έκτη πρακτική συμβουλεύει την κυβέρνηση να υποστηρίξει την αδειοδότηση ραδιοφάσματος σε εφαρμογές RFID.
7. Η έβδομη πρακτική αφορά τη διαχείριση της ασφάλειας των πληροφοριών και του ιδιωτικού απορρήτου. Όλες οι εφαρμογές οι οποίες χρησιμοποιούν την τεχνολογία RFID είναι απαραίτητο να έχουν καθορισμένες στρατηγικές ασφαλείας, ενώ οι εφαρμογές που συλλέγουν ή επεξεργάζονται προσωπικά δεδομένα οφείλουν να έχουν περαιτέρω και στρατηγικές προστασίας της ιδιωτικότητας.
8. Η όγδοη πρακτική τονίζει την αναγκαιότητα χρήσης εργαλείων για την εκτίμηση των επιπτώσεων στην ασφάλεια των πληροφοριών και στην προστασία της ιδιωτικότητας.

9. Η ένατη πρακτική προτείνει την ανάπτυξη και την υιοθέτηση κατάλληλων τεχνικών μέτρων για την προστασία της ασφάλειας των πληροφοριών και της ιδιωτικότητας.
10. Η δέκατη πρακτική επισημαίνει την αναγκαιότητα ενημέρωσης των υποκειμένων αλλά και τη λήψη συγκατάθεσης όταν συλλέγονται και υφίστανται επεξεργασία τα προσωπικά τους δεδομένα. Συγκεκριμένα, αναφέρεται ότι η ενημέρωση των υποκειμένων καθίσταται απαραίτητη σε όλο τον κύκλο ζωής των δεδομένων τους στο σύστημα.
11. Στην ενδέκατη πρακτική, λόγω του αδιαφανούς τρόπου με τον οποίο η τεχνολογία RFID συλλέγει τα δεδομένα, προτείνεται οι επισημάνσεις περί απορρήτου (privacy notices)[180] να περιλαμβάνουν περισσότερες πληροφορίες απ' ό,τι συνηθίζεται. Συγκεκριμένα, πληροφορίες που αφορούν την ύπαρξη των ετικετών, το περιεχόμενό τους, τους αναγνώστες τους, τη δυνατότητα απενεργοποίησής τους και τα σημεία για περαιτέρω πληροφόρηση.
12. Η δωδέκατη πρακτική συνιστά να επικρατεί διαφάνεια. Δηλαδή να ενημερώνονται τα υποκείμενα σχετικά με την ύπαρξη των ετικετών, των κινδύνων τους και των σχετικών μέτρων αντιμετώπισης που πιθανόν να υπάρχουν.
13. Η δέκατη τρίτη πρακτική δίνει έμφαση στο συνεχή διάλογο και στη συνεργασία για τη δημιουργία καλύτερων πολιτικών οι οποίες θα βοηθήσουν και στην προώθηση των πλεονεκτημάτων της τεχνολογίας.
14. Τέλος, η δέκατη τέταρτη πρακτική συνιστά τη συνεχή παρακολούθηση των εξελίξεων από τη χρήση της τεχνολογίας RFID σε συνδυασμό με άλλες τεχνολογίες και συστήματα, ώστε να αξιοποιούνται νέες δυνατότητες αλλά και να αντιμετωπίζονται νέες προκλήσεις κάθε φορά σε πρώιμο στάδιο.

Στη συνέχεια, στο δεύτερο κείμενο[181] ο Ο.Ο.Σ.Α., έδωσε έμφαση στην ασφάλεια των πληροφοριών και στην προστασία της ιδιωτικότητας από τη

[180] Αναφορικά με τις επισημάνσεις απορρήτου σύμφωνα με τον ΓΚΠΔ βλ. Γιαννακάκης Ι. Ε., Η επισήμανση απορρήτου (Privacy Notice) ως βέλτιστη πρακτική για την ενημέρωση των υποκειμένων προσωπικών δεδομένων (GDPR), ΣΥΝήΓΟΡΟΣ, 124/2017, 54-56.
[181] OECD (2008), OECD Policy Guidance on Radio Frequency Identification (RFID), ό.π. p.p. 11-81, διαθέσιμο σε http://www.oecd.org/sti/ieconomy/oecdpolicyguidanceonradiofrequencyidentificationrfid.htm

χρήση της τεχνολογίας RFID. Συγκεκριμένα, στην πρώτη ενότητα του κειμένου αυτού παρουσιάζει αναλυτικά τα χαρακτηριστικά της τεχνολογίας RFID, ενώ στη δεύτερη ενότητα επικεντρώνεται στα θέματα ασφάλειας των πληροφοριών και προστασίας της ιδιωτικότητας από τη χρήση της. Αρχικά παρουσιάζει περιληπτικά τους κινδύνους που μπορεί να προκύψουν από τη χρήση της τεχνολογίας RFID και τις πιθανές λύσεις με ορισμένα παραδείγματα και έπειτα επικεντρώνεται στην προστασία της ιδιωτικότητας, η οποία από έρευνες που έχουν γίνει έχει χαρακτηριστεί ως η μεγαλύτερη ανησυχία των καταναλωτών[182].

Τονίζει ότι η ασφάλεια των πληροφοριών και η διαφύλαξη της ιδιωτικότητας είναι δύο ζητήματα τα οποία πρέπει να ληφθούν σοβαρά υπόψη από τα αρχικά στάδια ανάπτυξης της τεχνολογίας, πριν ακόμη αυτή εξαπλωθεί ευρέως, ειδάλλως υπάρχει κίνδυνος να ζημιωθούν και οι επιχειρήσεις που την υιοθέτησαν και να προκύψουν αρνητικές συνέπειες στους πελάτες τους. Σήμερα, εξαιτίας τέτοιων περιπτώσεων με αρνητική εξέλιξη από την υιοθέτηση της τεχνολογίας, έχουν δημιουργηθεί ομάδες ανθρώπων οι οποίες εμποδίζουν την περαιτέρω ανάπτυξη και εξάπλωση της τεχνολογίας και επομένως και των πλεονεκτημάτων που προσφέρει.

Επίσης, προτείνει τη χρήση μεθοδολογιών, όπως τη δημιουργία ενός πλαισίου για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων, το οποίο θα βοηθήσει στον εντοπισμό των προβλημάτων που μπορεί να προκληθούν από την υιοθέτηση της τεχνολογίας αλλά και στην εύρεση στρατηγικών αντιμετώπισης για την ελαχιστοποίηση και εξάλειψη αυτών με τη λιγότερο δυνατό κόστος[183]. Παράλληλα, καθώς τα ενδιαφερόμενα μέλη και οι εμπλεκόμενοι φορείς είναι πολλοί, επισημαίνει ότι είναι σημαντικό να υπάρχει συνεχής ανοικτός διάλογος, επικοινωνία και συνεργασία μεταξύ αυτών, ώστε συνεχώς να

[182] Βλ. OECD (2008), OECD Policy Guidance on Radio Frequency Identification (RFID), ό.π. σελ:52 και συγκεκριμένα υποσημείωση 64. Επίσης βλ. Cap Gemini (2005), RFID and Consumers: What European Consumers Think About Radio Frequency Identification and the Implications for Business, Cap Gemini, Paris.

[183] Βλ. OECD (2008), OECD Policy Guidance on Radio Frequency Identification (RFID),ό.π. σελ: 16

επιτυγχάνεται όλο και περισσότερο εξασφάλιση της ασφάλειας των πληροφοριών και της ιδιωτικότητας.

Ακόμη, αναφέρει ότι πρέπει να ενθαρρυνθούν οι προσπάθειες που γίνονται για την ανάπτυξη της τεχνολογίας RFID ως τεχνολογίας ενίσχυσης της ιδιωτικότητας, ενώ επισημαίνει και ότι η προστασία εκ σχεδιασμού ή η ενσωμάτωση της έννοιας της ιδιωτικότητας κατά το σχεδιασμό της τεχνολογίας θα διευκολύνει σημαντικά την προστασία της ιδιωτικότητας και θα ενισχύσει την εμπιστοσύνη των καταναλωτών.

Ολοκληρώνοντας, στο τρίτο κείμενό[184] του ο Ο.Ο.Σ.Α παρουσιάζει τις εφαρμογές της τεχνολογίας RFID που είχαν αναπτυχθεί μέχρι τότε. Ειδικότερα, παρουσιάζει σε πινακοειδή μορφή παραδείγματα εφαρμογών που είχαν αναπτυχθεί μέχρι τότε στο δημόσιο (βλ. Πίνακας 9) και στον ιδιωτικό τομέα. Επίσης, κάνει μία ανασκόπηση των οικονομικών επιπτώσεων της τεχνολογίας και τέλος παρουσιάζει ανά χώρα ποιες εφαρμογές αναπτύχθηκαν στο δημόσιο τομέα, τι είδους ενημερωτικές και εκπαιδευτικές δραστηριότητες έγιναν σε κάθε περίπτωση και ποια προγράμματα χρηματοδοτήθηκαν.

[184] OECD (2008), RFID Applications, Impacts and Country Initiatives, OECD Digital Economy Papers, No. 144, OECD Publishing. DOI: http://dx.doi.org/10.1787/230464075484.

Πίνακας 9 Υλοποίηση εφαρμογών RFID στο δημόσιο τομέα ανά χώρα του Ο.Ο.Σ.Α

Πηγή: OECD (2008c, σελ. 18)

Χώρα	Εφαρμογές	Περιγραφή
Αυστρία	Υγεία	Δοκιμές από τη δημοτική διοίκηση της Βιέννης για την εφαρμογή του RFID στο σύστημα υγείας
	Δημόσιες Υπηρεσίες	Διαχείριση των πάρκινγκ
Δανία	Εκπαίδευση	Συστήματα δανεισμού σε βιβλιοθήκες
	Ηλεκτρονικά Διαβατήρια	Ηλεκτρονικά διαβατήρια (μέσα 2006) και βιομετρικά διαβατήρια (μέσα 2009)
Γερμανία	Ηλεκτρονικά Διαβατήρια	Ηλεκτρονικά διαβατήρια (τέλη 2005) και ηλεκτρονικές ταυτότητες (τέλη 2009)
	Δημόσιες Υπηρεσίες	Διαχείριση των απορριμάτων
	Εκπαίδευση	Συστήματα δανεισμού σε βιβλιοθήκες
Ιαπωνία	Logistics/Μεταφορές	Free Mobility Assistance σύστημα για την παροχή πληροφοριών (διαδρομές και τρόποι μεταφοράς)
Κορέα	Δημόσιες Υπηρεσίες	Πιλοτικά προγράμματα σε διάφορους τομείς όπως διαχείριση αποσκευών, παρακολούθηση επικίνδυνων αποβλήτων, χειρισμός πυρομαχικών
	Υγεία	
	Άμυνα	
	Logistics/Μεταφορές	
Μεξικό	Υγεία	Κάρτα υγείας
Ολλανδία	Ηλεκτρονικά Διαβατήρια	Ηλεκτρονικά Διαβατήρια
	Υγεία	Στα νοσοκομεία
	Εκπαίδευση	Στις βιβλιοθήκες
	Logistics/Μεταφορές	Εισιτήρια μεταφορών
Πορτογαλία	Ηλεκτρονικά Διαβατήρια	Ηλεκτρονικά Διαβατήρια και συστήματα ελέγχου των ηλεκτρονικών διαβατηρίων
Ισπανία	Διαχείριση εγγράφων Ταχυδρομικές υπηρεσίες	Στο ταχυδρομείο
Ηνωμένο Βασίλειο	Ηλεκτρονικά Διαβατήρια	Βιομετρικά διαβατήρια
ΗΠΑ	Άμυνα	Έλεγχος των εισερχόμενων και εξερχόμενων φορτίων στην εφοδιαστική αλυσίδα
Σιγκαπούρη	Logistics/Μεταφορές	Έλεγχος της κίνησης και της πληρωμής τελών κυκλοφορίας
	Δημόσιες Υπηρεσίες	Αντικατάσταση των χάρτινων εισιτηρίων στάθμευσης
	Εκπαίδευση	Συστήματα δανεισμού σε βιβλιοθήκες

4. Τα βήματα προς τη δημιουργία ενός πλαισίου για την προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές συστημάτων RFID στον ευρωπαϊκό χώρο

Τα βήματα προς την κατεύθυνση χάραξης πολιτικής ενός αποδεκτού πλαισίου για την ορθή χρήση της τεχνολογίας RFID[185] ξεκίνησαν από το 2005, όταν η Ομάδα εργασίας του άρθρου 29 ενέταξε για πρώτη φορά στις δραστηριότητές της[186] την ενασχόληση με την τεχνολογία RFID στον κλάδο λιανικής. Από τότε πολλές εξελίξεις και μια σειρά δράσεων πραγματοποιήθηκαν στον ευρωπαϊκό χώρο για την αντιμετώπιση των προβλημάτων ιδιωτικότητας που προκύπτουν από τη χρήση της τεχνολογίας RFID, οι οποίες θα παρουσιαστούν σε αυτό το κεφάλαιο (βλ. Πινακοποίηση των βημάτων, Πίνακας 10).

Τον Ιανουάριο του 2005, η Ομάδα εργασίας του άρθρου 29 υιοθέτησε το πρώτο κείμενο εργασίας[187] το οποίο αφορά ζητήματα προστασίας προσωπικών δεδομένων που συνδέονται με τη χρήση της τεχνολογίας RFID. Ο σκοπός του κειμένου αυτού είναι διπλός, καταρχήν να παρέχει καθοδήγηση και κατευθυντήριες οδηγίες σε αυτούς που πρόκειται να εφαρμόσουν την τεχνολογία για την εξασφάλιση της εφαρμογής των αρχών προστασίας προσωπικών δεδομένων, όπως αυτές ορίζονται στις Οδηγίες 95/46/ΕΚ και 2002/58/ΕΚ, καθώς και να κατευθύνει τους κατασκευαστές της τεχνολογίας να σχεδιάζουν την τεχνολογία με τέτοιο τρόπο ώστε να διευκολύνουν την εφαρμογή των αρχών. Επίσης, τονίζεται και το γεγονός ότι το κείμενο αυτό είναι μία πρώτη εκτίμηση της υπάρχουσας κατάστασης αφού δεν υπήρχε

[185] Βλ. Nikita, M. (2015). The recommended RFID privacy and data protection impact assessment framework in the EU, in Bottis, M., Alexandropoulou, E., Iglezakis, I., (edit.). Lifting the barriers to empower the future of Information Law and Ethics, Proceedings of the 6th International Conference of Information Law and Ethics, University of Macedonia, 30-31 May 2014, ed. The University of Macedonia Press, Thessaloniki 2015, p. 197-210

[186] Πρόκειται για το Πρόγραμμα εργασίας 2005 της Ομάδας εργασίας του άρθρου 29 (00863/05/EL - WP 109) το οποίο εγκρίθηκε στις 14 Απριλίου 2005 και είναι διαθέσιμο στο http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp109_el.pdf.

[187] Πρόκειται για το κείμενο εργασίας Working document on data protection issues related to RFID technology, (10107/05/EN, WP 105), January 19, 2005. Το περιεχόμενο του οποίου βλ. σε http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf

μέχρι τότε εμπειρία στη χρήση της τεχνολογίας και ότι θα συνεχίσει να παρέχει περαιτέρω καθοδήγηση.

Το παραπάνω κείμενο εργασίας έπειτα τέθηκε σε δημόσια διαβούλευση[188] στην οποία πήραν μέρος ιδιώτες, ενώσεις καταναλωτών και πανεπιστήμια[189], οι οποίοι κατέληξαν ότι συμφωνούν με το κείμενο εργασίας και ζητούν επιπρόσθετη μελέτη και καθοδήγηση από την Ομάδα εργασίας του άρθρου 29 αλλά και συμπλήρωση της Οδηγίας 95/46/ΕΚ με πιο συγκεκριμένους κανόνες για την τεχνολογία RFID. Στον αντίποδα, πήραν μέρος επιχειρήσεις οι οποίες υποστήριξαν ότι η Οδηγία 95/46/ΕΚ καλύπτει τα θέματα προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων που προκύπτουν από τη χρήση της εν λόγω τεχνολογίας και επομένως δε χρειάζονται περαιτέρω μεταρρυθμίσεις, παρά μόνο αυτορρυθμίσεις. Ταυτόχρονα, πολλές άλλες εισηγήσεις[190] από διάφορους φορείς σχετικά με το προαναφερθέν κείμενο εργασίας έπαιξαν καταλυτικό ρόλο στα επόμενα βήματα εξέλιξης του πλαισίου για την προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID.

Το 2006, η Επιτροπή ξεκίνησε δημόσια διαβούλευση[191] σχετικά με την τεχνολογία RFID και οργάνωσε πέντε θεματικές ενότητες προκειμένου να εκτιμηθούν οι δυνατότητες της τεχνολογίας RFID για τις επιχειρήσεις και την κοινωνία, αλλά και να μελετηθούν και να καταγραφούν τα προβλήματα που προκύπτουν σε θέματα ιδιωτικότητας και προστασίας των προσωπικών δεδομένων. Σε αυτό το σημείο αξίζει να αναφερθεί ότι αυτή η δημόσια

[188] Τα αποτελέσματα της δημόσιας διαβούλευσης είναι συγκεντρωμένα στο έγγραφο Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology (1670/05/EN, WP 111). Το περιεχόμενο του οποίου βλ. σε http://ec.europa.eu/justice/data-protection/article-29/press-material/public-consultation/rfid/2005_rfid/0_summary_wp111_en.pdf

[189] Το μεγαλύτερο ποσοστό άνηκε σε κράτη μέλη της Ευρωπαϊκής Ένωσης, ενώ το 10% από τις ΗΠΑ και τον Καναδά. Βλ. "Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology", ό.π. κεφ. ΙΙ, σελ. 2.

[190] Όλες οι εισηγήσεις είναι συγκεντρωμένες και διαθέσιμες στο http://ec.europa.eu/justice/data-protection/article-29/press-material/public-consultation/rfid/2005_rfid.htm.

[191] Σχετικά με τη δημόσια διαβούλευση βλ. δελτίο τύπου (IP/06/289), Commission launches public consultation on radio frequency ID tags, Brussels, 9 March 2006 και δελτίο τύπου (IP/06/909), Commission opens online public consultation on radio frequency identification (RFID), Brussels, 3 July 2006, διαθέσιμα στο http://europa.eu/rapid/press-release_IP-06-289_en.htm και στο http://europa.eu/rapid/press-release_IP-06-909_en.htm?locale=en αντίστοιχα.

διαβούλευση, σε δελτίο τύπου[192] στις 30 Ιουλίου το 2014, έχει χαρακτηριστεί ως «*η μεγαλύτερη μέχρι σήμερα δημόσια διαβούλευση που έχει πραγματοποιηθεί σχετικά με προβλήματα που αφορούν την ψηφιακή εποχή (the largest ever policy-related consultation on digital issues)*».

Την ίδια χρονιά η Επιτροπή με απόφασή της όρισε[193] την εναρμόνιση των όρων για τη διάθεση και την αποτελεσματική χρήση ραδιοφάσματος για συσκευές RFID που λειτουργούν στη ζώνη υπερυψηλών συχνοτήτων (UHF). Η Ευρωπαία Επίτροπος, Reding V., δήλωσε[194] ότι η εναρμόνιση της ραδιοσυχνότητας θα βοηθήσει στην εξάπλωση της τεχνολογίας σε όλη την Ευρώπη και ο τομέας του λιανικού εμπορίου θα είναι ο πρώτος στον οποίο θα παρατηρηθούν μεγάλες αλλαγές.

Το 2007, η Επιτροπή, βασιζόμενη στα αποτελέσματα της παραπάνω διαβούλευσης, με ανακοίνωσή της[195] πρότεινε ένα πρόγραμμα αρχικών βημάτων προς την κατεύθυνση χάραξης σαφούς νομικού πλαισίου προκειμένου να ξεπεραστούν οι παράγοντες που καθυστερούν την υιοθέτηση της τεχνολογίας RFID, όπως η παραβίαση της ιδιωτικότητας. Απώτερος σκοπός του προτεινόμενου προγράμματος είναι να διασφαλιστεί η τήρηση των θεμελιωδών δικαιωμάτων των πολιτών και να ανακτηθεί η εμπιστοσύνη των καταναλωτών δίνοντας ταυτόχρονα ώθηση στα οικονομικά και κοινωνικά οφέλη της τεχνολογίας. Έτσι, ανήγγειλε ότι κρίνει απαραίτητο να παρασχεθούν κατευθυντήριες οδηγίες για την επίτευξη των παραπάνω μέσω μελλοντικών συστάσεων.

---

[192] Βλ. στο ιστορικό του δελτίου τύπου (IP/14/889), Digital privacy: EU-wide logo and "data protection impact assessments" aim to boost the use of RFID systems, Brussels, 30 July 2014, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-14-889_en.htm.

[193] Βλ. άρθρο 1, Απόφαση της Επιτροπής της 23ης Νοεμβρίου 2006 σχετικά με την εναρμόνιση του ραδιοφάσματος για συσκευές ταυτοποίησης ραδιοσυχνοτήτων (RFID) που λειτουργούν στη ζώνη υπερυψηλών συχνοτήτων (UHF) [κοινοποιηθείσα υπό τον αριθμό Ε (2006) 5599] (2006/804/ΕΚ), Επίσημη Εφημερίδα της ΕΕ αριθ. L 329/64 της 25.11.2006, διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32006D0804&from=EN. Οι ζώνες συχνοτήτων για συσκευές RFID είναι διαθέσιμες στο Παράρτημα της Απόφασης.

[194] Βλ. δελτίο τύπου (IP/06/1808), From alarms to medical implants: Commission frees frequencies for short range wireless devices across the EU, Brussels, 14 December 2006, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-06-1808_en.htm.

[195] Βλ. Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των περιφερειών, «Η ραδιοσυχνική αναγνώριση (RFID) στην Ευρώπη: βήματα προς την κατεύθυνση χάραξης πλαισίου πολιτικής», ό.π.

Το ίδιο έτος η Επιτροπή με απόφασή της[196], σύστησε μία ομάδα εμπειρογνωμόνων για τη ραδιοσυχνική αναγνώριση (RFID Expert Group). Τα καθήκοντα της ομάδας αυτής, όπως παρουσιάζονται στο άρθρο 2 της απόφασης, είναι να παρέχει συμβουλές στην Επιτροπή όσον αφορά τη χρήση της τεχνολογίας RFID και να θέτει κατευθυντήριες γραμμές για τον τρόπο λειτουργίας των εφαρμογών RFID λαμβάνοντας υπόψη τις απόψεις των άμεσα ενδιαφερόμενων και θέματα που αφορούν τους μακροχρόνιους χρήστες καθώς και τις οικονομικές και κοινωνικές πτυχές των τεχνολογιών RFID. Επίσης, να στηρίζει τις προσπάθειες της Επιτροπής για ευαισθητοποίηση των κρατών μελών και των πολιτών καθώς και να παρέχει αντικειμενικές πληροφορίες και να διευκολύνει την ανταλλαγή εμπειριών και ορθών πρακτικών σχετικά με τις δυνατότητες και τις προκλήσεις της τεχνολογίας RFID.

Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων, του οποίου ο ρόλος είναι η διασφάλιση του δικαιώματος των πολιτών για προστασία της ιδιωτικής ζωής κατά την επεξεργασία προσωπικών δεδομένων από τα όργανα και τους οργανισμούς της ΕΕ, ανταποκρίθηκε στην παραπάνω ανακοίνωση της Επιτροπής και γνωμοδότησε[197] τον Απρίλιο του 2008. Πιο συγκεκριμένα, δήλωσε ότι εγκρίνει την προαναφερθείσα ανακοίνωση γιατί καλύπτει τα κύρια θέματα εξέλιξης της τεχνολογίας χωρίς να παραλείπει τα θέματα προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων που προκύπτουν[198].

[196] Βλ. Απόφαση της Επιτροπής της 28ης Ιουνίου 2007 για τη σύσταση της ομάδας εμπειρογνωμόνων για τη ραδιοσυχνική αναγνώριση (2007/467/ΕΚ), Επίσημη Εφημερίδα της ΕΕ αριθ. L 176/25 της 6.7.2007, διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32007D0467&from=EN.

[197] Βλ. Γνωμοδότηση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων όσον αφορά την ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, η ραδιοσυχνική αναγνώριση (RFID) στην Ευρώπη: βήματα προς την κατεύθυνση χάραξης πλαισίου πολιτικής COM(2007) 96, (2008/C 101/01), Επίσημη Εφημερίδα της ΕΕ αριθ. C 101/1 της 23.4.2008, διαθέσιμη στο https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EL.pdf. Επίσης βλ. δελτίο τύπου (EDPS/07/13), EDPS Opinion on RFID: major opportunities for Information Society but privacy issues need to be addressed with more ambition, Thursday, 20 December 2007, διαθέσιμο στο http://europa.eu/rapid/press-release_EDPS-07-13_en.htm

[198] Βλ. Γνωμοδότηση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων όσον αφορά την ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, η ραδιοσυχνική αναγνώριση (RFID) στην Ευρώπη: βήματα προς την κατεύθυνση χάραξης πλαισίου πολιτικής COM(2007) 96197, ό.π. κεφ. VIII Συμπέρασμα, παρ. 81, σελ. 11.

Επίσης, μεταξύ άλλων, προτείνει στην Επιτροπή, σε συνεργασία με την ομάδα εμπειρογνωμόνων RFID, την παροχή σαφών κατευθυντήριων γραμμών για την εφαρμογή του ισχύοντος νομικού πλαισίου στο περιβάλλον της τεχνολογίας[199] και την ανάπτυξη τεχνικών και προτύπων βασισμένων στην προστασία της ιδιωτικής ζωής εκ σχεδιασμού (privacy by design)[200].

Σε αυτό το σημείο αξίζει να αναφερθεί και η δήλωση της Ευρωπαίας Επιτρόπου για την κοινωνία της πληροφορίας και τα μέσα επικοινωνίας, Reding V., σε βιντεοσκοπημένο μήνυμα[201] που αναρτήθηκε στην ιστοσελίδα της τον Απρίλιο του 2009. Η Ευρωπαία Επίτροπος τόνισε ότι "*Οι Ευρωπαίοι πρέπει να έχουν το δικαίωμα να ελέγχουν πώς χρησιμοποιούνται τα προσωπικά τους δεδομένα*", και μάλιστα συγκεκριμένα για την τεχνολογία RFID δήλωσε ότι "*πρέπει να χρησιμοποιείται <u>από</u> τον καταναλωτή και όχι <u>στον</u> καταναλωτή. Κανένας Ευρωπαίος δεν πρέπει να φέρει τσιπ σε κάποιο από τα υπάρχοντά του χωρίς πρώτα να έχει ενημερωθεί ακριβώς προς τι χρησιμοποιούνται και χωρίς να έχει την επιλογή να τα αφαιρέσει ή να τα θέσει εκτός λειτουργίας οποιαδήποτε στιγμή*".

Ένα χρόνο μετά, το Μάιο του 2009, η Επιτροπή εξέδωσε σύσταση (ΕΕ L 122/47)[202] για την εφαρμογή των αρχών προστασίας της ιδιωτικής ζωής και

---

[199] Βλ. Γνωμοδότηση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων όσον αφορά την ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, η ραδιοσυχνική αναγνώριση (RFID) στην Ευρώπη: βήματα προς την κατεύθυνση χάραξης πλαισίου πολιτικής COM(2007) 96197, ό.π., κεφ. VIII Συμπέρασμα, παρ. 87, σελ. 11.

[200] Βλ. Γνωμοδότηση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων όσον αφορά την ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, η ραδιοσυχνική αναγνώριση (RFID) στην Ευρώπη: βήματα προς την κατεύθυνση χάραξης πλαισίου πολιτικής COM(2007) 96197, ό.π., κεφ. VIII Συμπέρασμα, παρ. 88, σελ. 11.

[201] Βλ. το βιντεοσκοπημένο μήνυμα Protecting privacy in the digital age, διαθέσιμο στο http://ec.europa.eu/archives/commission_2004-2009/reding/video/20090414/index_en.htm. Επίσης, βλ. δελτίο τύπου (IP/09/571), Η προστασία της ιδιωτικής ζωής των πολιτών πρέπει να καταστεί προτεραιότητα στην ψηφιακή εποχή τονίζει η Ευρωπαία Επίτροπος κα Reding, Βρυξέλλες, 14 Απριλίου 2009, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-09-571_el.htm.

[202] Βλ. Σύσταση της Επιτροπής της 12ης Μαΐου 2009 για την εφαρμογή αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων στις εφαρμογές που υποστηρίζονται από ραδιοσυχνική αναγνώριση [κοινοποιηθείσα υπό τον αριθμό Ε(2009) 3200] (2009/387/ΕΚ), Επίσημη Εφημερίδα της ΕΕ αριθ. L 122/47 της 16.5.2009, διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009H0387&from=EN. Επίσης βλ. δελτίο τύπου (IP/09/740), Μικροκυκλώματα με μεγάλες δυνατότητες: Νέες συστάσεις της Ευρωπαϊκής Ένωσης εξασφαλίζουν ότι οι ραβδωτοί κωδικοί του 21ου αιώνα σέβονται την προσωπική ζωή, Βρυξέλλες, 12.05.2009, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-09-740_el.htm.

των δεδομένων σε εφαρμογές όπου χρησιμοποιείται η τεχνολογία RFID. Η σύσταση αυτή είναι ένα από τα σημαντικότερα βήματα που έγιναν για την χάραξη πλαισίου εκτίμησης των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων σχετικά με τη χρήση της τεχνολογίας RFID στις διάφορες εφαρμογές. Συγκεκριμένα, η Επιτροπή με τη σύσταση αυτή «*παρέχει καθοδήγηση στα κράτη μέλη σχετικά με το σχεδιασμό και τη λειτουργία των εφαρμογών RFID με νόμιμο, ηθικό και κοινωνικά και πολιτικά αποδεκτό τρόπο, σεβόμενη το δικαίωμα προστασίας της ιδιωτικής ζωής*[203] (…) *διασφαλίζοντας την προστασία των δεδομένων προσωπικού χαρακτήρα και σχετικά με τα μέτρα που πρέπει να ληφθούν για την εγκατάσταση εφαρμογών RFID»*[204]. Καλεί δηλαδή τα κράτη μέλη να αναπτύξουν ένα πλαίσιο εκπόνησης εκτιμήσεων των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων[205] και να το υποβάλουν προς έγκριση στην Ομάδα εργασίας του άρθρου 29.

Ταυτόχρονα, με τη σύσταση αυτή η Επιτροπή εξέδωσε και οδηγίες για τις εφαρμογές RFID που χρησιμοποιούνται συγκεκριμένα στον τομέα του λιανικού εμπορίου[206]. Ειδικότερα, μεταξύ άλλων, πρότεινε την ενημέρωση των καταναλωτών από τους φορείς εκμετάλλευσης βάσει μίας κοινής ευρωπαϊκής σήμανσης όταν τα προϊόντα φέρουν ετικέτες και την απενεργοποίηση ή την επιβεβαίωση από τους καταναλωτές ότι η απενεργοποίηση ή η αφαίρεση συνέβη πραγματικά. Εκτός και εάν οι καταναλωτές, αφού έχουν προηγουμένως ενημερωθεί με ακριβή και εύκολα κατανοητό τρόπο σχετικά με τη χρήση τους, έχουν επιλέξει να τις διατηρήσουν ενεργές. Μάλιστα, ακόμη

[203] Βλ. Σύσταση της Επιτροπής της 12ης Μαΐου 2009 για την εφαρμογή αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων στις εφαρμογές που υποστηρίζονται από ραδιοσυχνική αναγνώριση, ό.π. Πεδίο εφαρμογής παρ. 1, σελ. 3.

[204] Βλ. Σύσταση της Επιτροπής της 12ης Μαΐου 2009 για την εφαρμογή αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων στις εφαρμογές που υποστηρίζονται από ραδιοσυχνική αναγνώριση, ό.π. Πεδίο εφαρμογής παρ. 2, σελ. 3.

[205] Βλ. Σύσταση της Επιτροπής της 12ης Μαΐου 2009 για την εφαρμογή αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων στις εφαρμογές που υποστηρίζονται από ραδιοσυχνική αναγνώριση, ό.π. Εκτιμήσεις των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων παρ. 4, σελ. 4.

[206] Βλ. Σύσταση της Επιτροπής της 12ης Μαΐου 2009 για την εφαρμογή αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων στις εφαρμογές που υποστηρίζονται από ραδιοσυχνική αναγνώριση, ό.π. Εφαρμογές RFID που χρησιμοποιούνται στον τομέα του λιανικού εμπορίου, παρ. 9 έως 14, σελ. 4-5. Επίσης, περιπτωσιολογία σχετικά με τις εφαρμογές RFID στον τομέα του λιανικού εμπορίου βλ. Μέρος τρίτο, Κεφάλαιο 3.

και εάν οι ετικέτες δεν αποτελούν πιθανή απειλή για την προστασία της ιδιωτικής ζωής ή των δεδομένων, η Επιτροπή συνιστά ότι πάλι πρέπει να δίνεται η δυνατότητα άμεσης ή μεταγενέστερης απενεργοποίησης ή αφαίρεσης των ετικετών χωρίς χρέωση.

Το ίδιο έτος εκδόθηκε και η Οδηγία 2009/136/ΕΚ[207] για την τροποποίηση, μεταξύ άλλων, της Οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (βλ. Μέρος δεύτερο, υποκεφάλαιο 1.2). Η προσθήκη στο άρθρο 3 σχετικά με την εφαρμογή της Οδηγίας η οποία περιλαμβάνει πλέον και δημόσια δίκτυα επικοινωνιών που υποστηρίζουν συσκευές συγκέντρωσης δεδομένων και ταυτοποίησης, δηλώνει ξεκάθαρα ότι όσες εφαρμογές της τεχνολογίας RFID συνδέονται ή χρησιμοποιούν δημόσια δίκτυα ή υπηρεσίες επικοινωνιών υπάγονται στην εν λόγω Οδηγία[208]. Επομένως, οι υπεύθυνοι επεξεργασίας οφείλουν να συμμορφώνονται και με τις σχετικές διατάξεις[209]. Δεν είναι όμως απολύτως ξεκάθαρο τελικά εάν με την τροποποίηση αυτή η πρόθεση του νομοθέτη ήταν να καλύψει και περιπτώσεις εφαρμογών όπως η τεχνολογία RFID, επομένως δε προσφέρει βελτίωση νομικής σαφήνειας[210].

Από τον Ιούλιο του 2009, μία άτυπη «ομάδα εργασίας RFID» με εκπροσώπους του κλάδου της βιομηχανίας άρχισε να πραγματοποιεί συχνές συναντήσεις με ενδιαφερομένους, όπως ομάδες καταναλωτών, φορείς

[207] Οδηγία 2009/136/ΕΚ της 25ης Νοεμβρίου 2009, για τροποποίηση της Οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της Οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του Κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ), Επίσημη Εφημερίδα της ΕΕ αριθ. L 337/11, διαθέσιμη στο http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:El:PDF

[208] Βλ. Γνωμοδότηση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων όσον αφορά την πρόταση Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την τροποποίηση, μεταξύ άλλων, της Οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Οδηγίας σχετικά με την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες), Επίσημη Εφημερίδα της ΕΕ αριθ. C 181, 18.7.2008, σελ: 1–13, διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=uriserv:OJ.C_.2008.181.01.0001.01.ELL&toc=OJ:C:2008:181:FULL

[209] Παραπάνω λεπτομέρειες βλ. Iglezakis, I. (2011). Regulation models addressing data protection issues in the EU concerning RFID technology, 4th Conference on Information Law and Ethics, Thessaloniki, May 20-21.

[210] Kosta, E. (2012). The application of the ePrivacy Directive on RFID systems, ό.π. σελ.6.

τυποποίησης και πανεπιστημιακούς ερευνητές και να συζητάνε για θέματα σχετικά με τις εφαρμογές της τεχνολογίας RFID στους διάφορους τομείς. Έτσι, στις 31 Μαρτίου το 2010, η ομάδα αυτή κατέληξε σε μία πρόταση[211] για ένα πλαίσιο εκτίμησης των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID, βασισμένο στις παρατηρήσεις της σύστασης της Επιτροπής της 12ης Μαΐου 2009 (ΕΕ L 122/47). Έπειτα, η πρόταση αυτή κατατέθηκε για έγκριση στην Ομάδα εργασίας του άρθρου 29, όπως είχε προταθεί από την Επιτροπή.

Η παραπάνω πρόταση της ομάδας εργασίας RFID ήταν ομολογουμένως μία πολύ καλή προσπάθεια δημιουργίας ενός πλαισίου εκτίμησης των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων. Όμως, κυρίως λόγω της «*απουσίας σαφούς και συνολικής προσέγγισης αξιολόγησης των κινδύνων στην προστασία της ιδιωτικής ζωής και των δεδομένων στο προτεινόμενο πλαίσιο*»[212], η Ομάδα εργασίας του άρθρου 29 δεν ενέκρινε το προτεινόμενο πλαίσιο και ζήτησε τη βελτίωσή του.

Η Ευρωπαϊκή Επιτροπή ζήτησε και από τον ENISA[213], τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών, ο οποίος έχει εμπειρία στον εντοπισμό και στην αξιολόγηση κινδύνων, να υποβάλει τις παρατηρήσεις του σχετικά με το παραπάνω προτεινόμενο πλαίσιο της ομάδας εργασίας RFID. Ο ENISA υποστήριξε σε ανεξάρτητη γνώμη[214] ότι το προτεινόμενο πλαίσιο είναι ένα καλό αρχικό βήμα, αλλά επιδέχεται βελτίωση. Συγκεκριμένα, οι συστάσεις του επικεντρώθηκαν κυρίως στις μεθόδους

[211] Βλ. την πρόταση Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications. Appendix 1: The proposed Framework (March 31, 2010), διαθέσιμη στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp175_annex_en.pdf.

[212] Η Ομάδα εργασίας του άρθρου 29 έκανε κάποιες παρατηρήσεις και προτάσεις σχετικά με τη βελτίωση του προτεινόμενου πλαισίου, τις οποίες η ομάδα εργασίας RFID οφείλει να λάβει υπόψη της. Βλ. Γνώμη 5/2010 σχετικά με την πρόταση του κλάδου για ένα πλαίσιο εκπόνησης εκτιμήσεων των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID, (00066/10/EL, WP 175), σελ. 13. Εκδόθηκε την 13η Ιουλίου 2010, διαθέσιμη στο http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_el.pdf.

[213] Ο ENISA αποτελεί ένα «κέντρο εμπειρογνωμοσύνης σε θέματα Ασφάλειας των Δικτύων και Πληροφοριών και προωθεί τη συνεργασία ανάμεσα στο δημόσιο και ιδιωτικό τομέα». Περισσότερες πληροφορίες για τον οργανισμό διαθέσιμες στο http://www.enisa.europa.eu/media/enisa-in-greek/.

[214] Βλ. ENISA Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications [of March 31, 2010]", Ιούλιος 2010, διαθέσιμη στο https://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia/view.

αναγνώρισης, ανάλυσης και εκτίμησης των κινδύνων, την αξιολόγηση των επιπτώσεων και τις στρατηγικές ελαχιστοποίησης και εξάλειψης των κινδύνων.

Η ομάδα εργασίας RFID, αφού έλαβε υπόψη τις παρατηρήσεις της Ομάδας εργασίας του άρθρου 29 και του ENISA, πρότεινε έπειτα ένα νέο, αναθεωρημένο πλαίσιο εκτίμησης των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID[215] και το υπέβαλε προς έγκριση στην Ομάδα εργασίας του άρθρου 29, όπως είχε προταθεί από την Επιτροπή[216]. Η Αντιπρόεδρος της Ευρωπαϊκής Επιτροπής, Neelie Kroes, σε ομιλία της[217] χαρακτηρίζει το προτεινόμενο αυτό πλαίσιο ως το πρώτο στο είδος του στην Ευρώπη και επιβραβεύει τις προσπάθειες που έγιναν από την ομάδα εργασίας RFID. Στο επόμενο κεφάλαιο παρουσιάζεται αναλυτικά το αναθεωρημένο αυτό πλαίσιο, το οποίο πήρε τελικά και την έγκριση της Ομάδας εργασίας του άρθρου 29 και χρησιμοποιείται μέχρι σήμερα.

[215] Βλ. αναθεωρημένη πρόταση, Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 Ιανουαρίου 2011, διαθέσιμη στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf.

[216] Βλ. Σύσταση της Επιτροπής της 12ης Μαΐου 2009 για την εφαρμογή αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων στις εφαρμογές που υποστηρίζονται από ραδιοσυχνική αναγνώριση, ό.π..

[217] Βλ. ομιλία της Neelie Kr. “Smart tags - working together to protect privacy”, SPEECH/11/236, διαθέσιμη στο http://europa.eu/rapid/press-release_SPEECH-11-236_en.htm?locale=en

Πίνακας 10 Πινακοποίηση των βημάτων προς τη δημιουργία ενός πλαισίου για την προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID στον ευρωπαϊκό χώρο.

ΕΤΟΣ	ΕΓΓΡΑΦΟ	ΤΙΤΛΟΣ	ΣΥΝΤΑΚΤΗΣ
Ιαν. 2005	WP 105	Working document on data protection issues related to RFID technology	Ομάδα εργασίας άρθρου 29
Σεπτ. 2005	WP 111	Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology	Ομάδα εργασίας άρθρου 29
2005		Consultation on data protection issues related to RFID technology - contributions received	
Μάρτ. 2006	IP/06/289	Commission launches public consultation on radio frequency ID tags	Δελτίο Τύπου
Ιούλ. 2006	IP/06/909	Commission opens online public consultation on radio frequency identification (RFID)	Δελτίο Τύπου
Νοέμβρ. 2006	2006/804/ΕΚ	Απόφαση της Επιτροπής της 23ης Νοεμβρίου 2006 σχετικά με την εναρμόνιση του ραδιοφάσματος για συσκευές ταυτοποίησης ραδιοσυχνοτήτων (RFID) που λειτουργούν στη ζώνη υπερυψηλών συχνοτήτων (UHF)	Απόφαση της Επιτροπής
Δεκ. 2006	IP/06/1808	From alarms to medical implants: Commission frees frequencies for short range wireless devices across the EU	Δελτίο Τύπου
Μάρτ. 2007	COM (2007) 96 τελικό	Η ραδιοσυχνική αναγνώριση (RFID) στην Ευρώπη: βήματα προς την κατεύθυνση χάραξης πλαισίου πολιτικής	Ανακοίνωση της Επιτροπής
Ιούν. 2007	2007/467/ΕΚ	Σύσταση της ομάδας εμπειρογνωμόνων για τη ραδιοσυχνική αναγνώριση	Απόφαση της Επιτροπής
Δεκ. 2007	EDPS/07/13	EDPS Opinion on RFID: major opportunities for Information Society but privacy issues need to be addressed with more ambition	Δελτίο Τύπου
Απρ. 2008	2008/C 101/01	Όσον αφορά την ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, η ραδιοσυχνική αναγνώριση (RFID) στην Ευρώπη: βήματα προς την κατεύθυνση χάραξης πλαισίου πολιτικής COM(2007) 96	Γνωμοδότηση Ευρωπαίου Επόπτη Προστασίας Δεδομένων
Απρ. 2009	IP/09/571	Η προστασία της ιδιωτικής ζωής των πολιτών πρέπει να καταστεί προτεραιότητα στην ψηφιακή εποχή τονίζει η Ευρωπαία Επίτροπος κα Reding	Δελτίο Τύπου

Μάιος 2009	2009/387/ΕΚ	Εφαρμογή αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων στις εφαρμογές που υποστηρίζονται από ραδιοσυχνική αναγνώριση [κοινοποιηθείσα υπό τον αριθμό Ε(2009) 3200]	Σύσταση της Επιτροπής
Μάιος 2009	IP/09/740	Μικροκυκλώματα με μεγάλες δυνατότητες: Νέες συστάσεις της Ευρωπαϊκής Ένωσης εξασφαλίζουν ότι οι ραβδωτοί κωδικοί του 21ου αιώνα σέβονται την προσωπική ζωή	Δελτίο Τύπου
Δεκ. 2009	L 337/11	Οδηγία 2009/136/ΕΚ για τροποποίηση (..) της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (..)	Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης
Μάρτ. 2010	WP 175_ANNEX	Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications. Appendix 1: The proposed Framework	Ομάδα εργασίας RFID
Ιούλ. 2010	Γνώμη 5/2010	Γνώμη 5/2010 σχετικά με την πρόταση του κλάδου για ένα πλαίσιο εκπόνησης εκτιμήσεων των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID	Ομάδα εργασίας άρθρου 29
Ιούλ. 2010		ENISA position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications [of March 31, 2010]	ENISA
Φεβρ. 2011	WP 180_ANNEX	Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID	Ομάδα εργασίας RFID
Φεβρ. 2011	Γνώμη 9/2011	σχετικά με την αναθεωρημένη πρόταση του κλάδου για ένα πλαίσιο εκπόνησης εκτιμήσεων των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID	Ομάδα εργασίας άρθρου 29
Απρ. 2011	SPEECH/11/236	Smart tags - working together to protect privacy	Neelie Kroes
Ιούλ. 2014	IP/14/889	Digital privacy: EU-wide logo and “data protection impact assessments” aim to boost the use of RFID systems	Δελτίο Τύπου

5. Παρουσίαση του αναθεωρημένου πλαισίου για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID

Έπειτα από μία σειρά συνεχόμενων προσπαθειών και εξελίξεων, και ιδίως μετά τη Σύσταση της Επιτροπής της 12ης Μαΐου 2009, ξεκίνησαν οι προσπάθειες για τη δημιουργία ενός πλαισίου εκπόνησης εκτιμήσεων των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων από τη χρήση της τεχνολογίας RFID. Το 2011, μία ομάδα εργασίας RFID με εκπροσώπους του κλάδου, μετά από αρκετές συναντήσεις με ενδιαφερόμενα μέρη και αφού έλαβε υπόψη της τις παρατηρήσεις της Ομάδας εργασίας του άρθρου 29 και του ENISA, πρότεινε ένα αναθεωρημένο πλαίσιο[218] εκτίμησης των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων για τις εφαρμογές RFID, το οποίο στο εξής θα λέγεται πλαίσιο PIA (Privacy and data protection Impact Assessment framework).

Το πλαίσιο PIA είναι αποτελεσματικό διότι η δημιουργία αυτού αποτέλεσε μία διεθνή προσπάθεια[219]. Αφορά κυρίως τον ευρωπαϊκό χώρο, αλλά έχει επηρεαστεί πολύ και από τους υπεύθυνους χάραξης πολιτικής (policy makers) στις ΗΠΑ. Επομένως μπορεί να χρησιμοποιηθεί από τις επιχειρήσεις στις ΗΠΑ. Ενώ ταυτόχρονα μπορεί εύκολα να χρησιμοποιηθεί και από άλλες παρόμοιες τεχνολογίες και γιατί όχι να αποτελέσει και μία καλή αρχή (προοίμιο) για τη δημιουργία και χρήση πλαισίων PIA γενικότερα.

Σε αυτό το κεφάλαιο θα μελετηθεί και θα παρουσιαστεί αναλυτικά το προτεινόμενο πλαίσιο PIA, όσον αφορά εφαρμογές συστημάτων RFID.

[218] Βλ. Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID (2011). Σημειώνεται ότι η ελληνική εκδοχή δεν είναι πλέον διαθέσιμη, ενώ ήταν μέχρι 16/10/2014. Βλ. την αγγλική εκδοχή σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf.

[219] Spiekerman S. (2012). The RFID PIA – Developed by Industry, Endorsed by Regulators, Series: Law, Governance and Technology Series, Privacy Impact Assessment, Part IV, Vol. 6, σελ: 345.

5.1. Τι είναι το πλαίσιο PIA

Έχουν δοθεί διάφοροι ορισμοί για το πλαίσιο PIA και η έννοιά του έχει μεταβληθεί με την πάροδο του χρόνου[220]. Στην περίπτωσή μας, το πλαίσιο PIA είναι ένα εργαλείο εκτίμησης των πιθανών επιπτώσεων στην προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων. Ειδικότερα, είναι ένα εργαλείο λήψης αποφάσεων και διαχείρισης κινδύνων το οποίο χρησιμοποιείται για τον εντοπισμό των κινδύνων, την εκτίμηση της πιθανότητας εμφάνισης αυτών, την αξιολόγηση των επιπτώσεών τους αλλά και για την εύρεση μέτρων εξάλειψης ή τουλάχιστον ελαχιστοποίησης αυτών.

Στην Ευρώπη δεν είναι η πρώτη φορά[221] που προτείνεται η εφαρμογή της μεθόδου PIA (Privacy Impact Assessment process). Το 2007, το Γραφείο του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου (Information Commissioner's Office, ICO) δημοσίευσε εγχειρίδιο για τη διαδικασία υλοποίησης της μεθόδου PIA[222]. Το εγχειρίδιο αυτό δίνει κατευθυντήριες γραμμές σε οργανισμούς που αναλαμβάνουν την υλοποίηση εφαρμογών και έργων με πιθανές επιπτώσεις στην ιδιωτικότητα, προκειμένου να υλοποιούν την κατάλληλη για την περίπτωσή τους κάθε φορά διαδικασία PIA.

Τέλος, επειδή το πλαίσιο PIA έχει χρησιμοποιηθεί σε διάφορες χώρες, υπάρχουν διαφορές στον τρόπο εφαρμογής του[223] από χώρα σε χώρα και από περίπτωση σε περίπτωση. Γενικότερα όμως, ο σκοπός του σε όλες τις περιπτώσεις είναι η εκτίμηση των επιπτώσεων στην ιδιωτικότητα που πιθανόν να έχει η υλοποίηση της υπό μελέτη κάθε φορά εφαρμογής και ο προσδιορισμός ελέγχων για τον περιορισμό τους.

---

[220] Βλ. Clarke R. (2009), Privacy Impact Assessment: Its Origins and Development,ό.π.. βλ. του ορισμούς για το πλαίσιο PIA στο Appendix 1: Definitions, σελ. 130.

[221] Wright D. & Hert P. De (2012). Introduction to Privacy Impact Assessment, Series: Law, Governance and Technology Series, Privacy Impact Assessment, Part I, Vol. 6, pp. 3-32.

[222] Information Commissioner's Office (ICO), Privacy Impact Assessment Handbook. Version 2.0, Wilmslow, Cheshire, Δεκέμβριος 2007, Version 2.0, Ιούνιος 2009, διαθέσιμο στο http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

[223] Wright D. (2011). Should Privacy Impact Assessments Be Mandatory?, Communications of the ACM, Vol. 54 (8), pp. 121-131, σελ. 3.

5.2. Σκοπός και οφέλη του πλαισίου PIA

Το πλαίσιο PIA δημιουργήθηκε έχοντας ως απώτερο σκοπό να δώσει κατευθυντήριες γραμμές στους φορείς εκμετάλλευσης των εφαρμογών RFID, ώστε να διαχειρίζονται αποτελεσματικά τους κινδύνους για την ιδιωτικότητα. Πιο συγκεκριμένα, βοηθάει στον εντοπισμό των κινδύνων από τη χρήση της εφαρμογής RFID και στην εύρεση μεθόδων αντιμετώπισής τους ή τουλάχιστον ελαχιστοποίησής τους ώστε να μην αποτελούν πλέον κίνδυνο για την ιδιωτικότητα και ταυτοχρόνως να συμμορφώνονται στις αρχές προστασίας της ιδιωτικότητας.

Πέρα από την παροχή κατευθύνσεων, το πλαίσιο PIA καθορίζει το περιεχόμενο και την κοινή οργανωτική δομή των εκθέσεων PIA. Στις εκθέσεις PIA πρέπει οι φορείς εκμετάλλευσης να τεκμηριώνουν τα αποτελέσματά τους και να τα κοινοποιούν στην αρμόδια αρχή ελέγχου. Επομένως, το πλαίσιο PIA αποτελεί ένα μοντέλο το οποίο βοηθάει στην αποτελεσματικότερη διεξαγωγή της διαδικασίας από τους φορείς εκμετάλλευσης και στην κατάρτιση των σχετικών εκθέσεων.

Με την εφαρμογή του πλαισίου PIA το σημαντικότερο πλεονέκτημα είναι ότι εξασφαλίζεται η συμμόρφωση των φορέων εκμετάλλευσης με τους νομικούς κανόνες για την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων[224]. Επιπλέον, οι φορείς εκμετάλλευσης οι οποίοι εφαρμόζουν το πλαίσιο PIA στις εφαρμογές τους και υπάρχει διαφάνεια στον τρόπο εφαρμογής, έχουν περισσότερες πιθανότητες να κερδίσουν την εμπιστοσύνη των καταναλωτών και να δημιουργήσουν ένα πολύ καλό και ελκυστικό εταιρικό προφίλ. Έτσι, αποκτούν ανταγωνιστικό πλεονέκτημα και διαφοροποιούνται από τους ανταγωνιστές τους[225].

---

[224] Βλ. Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID (2011), σελ. 3. Σημειώνεται ότι η ελληνική εκδοχή δεν είναι πλέον διαθέσιμη, ενώ ήταν μέχρι 16/10/2014. Βλ. την αγγλική εκδοχή σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf, σελ. 3.

[225] Βλ. Wright D. & Hert P. De (2012). Introduction to Privacy Impact Assessment, ό.π. σελ.16. Επίσης, βλ. Stewart Bl. (2002). Privacy Impact Assessment Handbook, Office of the Privacy Commissioner, Auckland, March 2002, revised June 2007, σελ. 29, διαθέσιμο στο http://www.privacy.org.nz/assets/Uploads/Privacy-Impact-Assessment-Handbook-June2007.pdf. Επίσης, βλ. Wright D. (2011). Should Privacy Impact Assessments Be Mandatory?, ό.π. σελ. 7.

Επίσης, αξίζει να αναφερθεί ότι οι φορείς εκμετάλλευσης εφαρμογών RFID οφείλουν να εφαρμόζουν το πλαίσιο PIA πριν την εγκατάσταση της τεχνολογίας, στα πρώιμα ακόμη στάδια σχεδιασμού και ανάπτυξης της εφαρμογής της, γνωστή ως ιδιωτικότητα εκ σχεδιασμού (privacy by design), προκειμένου να απολαμβάνουν όλα τα οφέλη του στο έπακρον και να μειώνεται και το κόστος εφαρμογής[226]. Ενώ, σε αντίθετη περίπτωση, η εκ των υστέρων υλοποίηση, είναι μια ιδιαίτερα δαπανηρή διαδικασία καθώς είναι πιθανόν να χρειαστεί να γίνουν προσαρμογές και σημαντικές αλλαγές στις λειτουργίες της ώστε να επιτευχθεί η συμμόρφωση με τους νομικούς κανόνες για την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων. Μάλιστα, είναι πολύ πιθανόν το πλαίσιο PIA να μην έχει την ίδια αποτελεσματικότητα απ' ότι στην περίπτωση εφαρμογής της εκ σχεδιασμού.

Βέβαια, στην περίπτωση που γίνουν μελλοντικά αλλαγές στην εφαρμογή RFID, το πλαίσιο PIA πρέπει να υλοποιηθεί ξανά. Τέτοιες περιπτώσεις είναι είτε αλλαγές στον σκοπό χρήσης της εφαρμογής, είτε αλλαγές στον τύπο των δεδομένων που συλλέγονται. Για παράδειγμα, στην περίπτωση της διοίκησης της εφοδιαστικής αλυσίδας, αρχικά η χρήση RFID ετικετών μπορεί να αφορά μόνο τη διαχείριση των προϊόντων στην αποθήκη και μετέπειτα να συνδεθούν με άτομα για καταναλωτικούς σκοπούς και επομένως να είναι εύκολο να γίνει ταυτοποίηση των ατόμων. Σε αυτή την περίπτωση είναι απαραίτητο να υλοποιηθεί ξανά το πλαίσιο PIA.

Όπως είναι όμως αναμενόμενο, υπάρχουν και μειονεκτήματα στην υλοποίηση ενός πλαισίου PIA. Καταρχήν προσθέτει περισσότερη γραφειοκρατία, κάτι που έρχεται σε αντίθεση με τον εκσυγχρονισμό των μεθόδων και επομένως καθυστερεί την ολοκλήρωση της εφαρμογής[227]. Επίσης, η υλοποίησή του προσθέτει επιπλέον κόστος στον φορέα εκμετάλλευσης καθώς απαιτούνται κάποιες εσωτερικές διαδικασίες[228], οι οποίες θα αναλυθούν παρακάτω, τις οποίες οφείλουν να εκτελούν οι φορείς εκμετάλλευσης για την υποστήριξη της εκτέλεσης του πλαισίου PIA.

[226] Βλ. Wright D. & Hert P. De (2012). Introduction to Privacy Impact Assessment, ό.π. σελ.17.
[227] Βλ. Wright D. (2011). Should Privacy Impact Assessments Be Mandatory?, ό.π. σελ. 8.
[228] Βλ. Privacy and Data Protection Impact Assessment Framework for RFID Applications (2011), ό.π. σελ. 5.

5.3. Υποστήριξη εκτέλεσης του πλαισίου PIA

Το πλαίσιο PIA από μόνο του αποτελεί μονάχα ένα εργαλείο για την προστασία της ιδιωτικότητας και προκειμένου να είναι αποτελεσματικό παίζουν σημαντικό ρόλο και οι διαδικασίες που γίνονται για την υποστήριξή του. Συγκεκριμένα, για τη σωστή και επιτυχημένη εκτέλεση του πλαισίου PIA απαιτείται υψηλού βαθμού υποστήριξη και τεχνογνωσία σε θέματα ιδιωτικότητας αλλά και δημιουργία κουλτούρας ιδιωτικότητας[229].

Η ομάδα εργασίας RFID, η οποία πρότεινε το πλαίσιο PIA, στο έγγραφό της συμπεριέλαβε και ορισμένες εσωτερικές διαδικασίες[230] τις οποίες οφείλουν να διαθέτουν οι φορείς εκμετάλλευσης των εφαρμογών RFID. Οι διαδικασίες αυτές βοηθούν στη σωστή εκτέλεση και ολοκλήρωση του PIA, επομένως και στη συνολική προσπάθεια για την προστασία της ιδιωτικότητας από την υλοποίηση εφαρμογών RFID.

Καταρχήν, ο χρονοπρογραμματισμός της διαδικασίας υλοποίησης του πλαισίου PIA είναι πολύ σημαντικός προκειμένου να γίνουν έγκαιρα οι απαραίτητες εσωτερικές αλλαγές και οι προσαρμογές που μπορεί να προκύψουν. Συγκεκριμένα, το προτεινόμενο χρονικό διάστημα για να κατατεθεί στην αρμόδια αρχή μία έκθεση σχετικά με το πλαίσιο PIA, είναι τουλάχιστον 6 εβδομάδες πριν από την εγκατάσταση της εφαρμογής RFID, ώστε να υπάρχει αρκετός χρόνος για να γίνουν όλες οι τυχόν απαραίτητες αλλαγές. Ειδάλλως, το κόστος υλοποίησης που θα προκύψει ενδεχομένως να είναι αρκετά μεγαλύτερο.

---

[229] Hert De P., Kloza D. & Wright D (2012). Recommendations for a privacy impact assessment framework for the European Union, Παραδοτέο D3 του έργου PIAF (A Privacy Impact Assessment Framework for data protection and privacy rights), σελ. 23, διαθέσιμο στο https://piafproject.files.wordpress.com/2018/03/piaf_d3_final.pdf

[230] Βλ. Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID (2011), σελ. 5-6. Σημειώνεται ότι η ελληνική εκδοχή δεν είναι πλέον διαθέσιμη, ενώ ήταν μέχρι 16/10/2014. Βλ. την αγγλική εκδοχή σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf, σελ. 4-5. Οι διαδικασίες αυτές είχαν προταθεί και στο πρώτο προτεινόμενο πλαίσιο PIA (βλ. Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications (2010), ό.π. σελ: 6-7) το οποίο δεν εγκρίθηκε, και συμπεριλήφθηκαν και στο αναθεωρημένο πλαίσιο PIA με ορισμένες προσθήκες.

Η διαδικασία υλοποίησης του πλαισίου PIA πρέπει να ελέγχεται εσωτερικά σε όλα τα στάδιά της από τους φορείς εκμετάλλευσης της εφαρμογής και να υπάρχει συνεχώς ανάδραση, ακόμη και μετά την υλοποίηση της εφαρμογής, ώστε να αντιμετωπίζονται ενδεχόμενες επιπτώσεις που δεν προβλέφθηκαν. Επίσης, οι εκθέσεις PIA που κατατίθενται στην αρμόδια αρχή πρέπει να ελέγχονται ως προς τη συνέπεια και να τεκμηριώνονται με συγκεκριμένες αναφορές και παραδείγματα από την εφαρμογή RFID, όπως την υλοποίηση της ετικέτας και τα συστατικά στοιχεία του προϊόντος.

Η συλλογή των δικαιολογητικών και όλου του υλικού που αποδεικνύει ότι ο φορέας εκμετάλλευσης για τη συγκεκριμένη εφαρμογή RFID έχει εκπληρώσει όλες τις υποχρεώσεις του και εφάρμοσε τα προτεινόμενα βήματα για την προστασία της ιδιωτικότητας από την υλοποίηση της εφαρμογής του, είναι μία εξίσου σημαντική διαδικασία. Για παράδειγμα, ο φορέας εκμετάλλευσης οφείλει να συλλέγει τα αντίγραφα ανακοινώσεων και τα αποτελέσματα από επιθεωρήσεις ασφάλειας, ώστε ανά πάσα στιγμή να μπορεί να υποστηρίξει ότι εκπλήρωσε τις υποχρεώσεις του με διαφανείς διαδικασίες.

Ακόμη, ο καθορισμός καθηκόντων σε συγκεκριμένα άτομα και ο καθορισμός των λειτουργιών εντός του οργανισμού, είναι εσωτερικές ενέργειες που δεν πρέπει να παραλειφθούν για να επιτευχθεί η ομαλή υλοποίηση και ολοκλήρωση του πλαισίου PIA. Επιπροσθέτως, είναι απαραίτητος και ο καθορισμός κριτηρίων, ακόμη και η δημιουργία μοντέλου αξιολόγησης του βαθμού ωριμότητας της εφαρμογής προς εγκατάσταση.

Ταυτόχρονα, πρέπει να οριστούν και να εκτιμηθούν οι παράγοντες που μπορεί να επιβάλλουν την αναθεώρηση ή ακόμη και τη δημιουργία νέας έκθεσης PIA. Τέτοιοι παράγοντες είναι σημαντικές αλλαγές στην εφαρμογή, όπως τύποι πληροφοριών που υπόκεινται σε επεξεργασία και ανταπόκριση σε σημαντική αντίδραση ενδιαφερόμενου μέρους και σημαντικές τεχνολογικές αλλαγές με συνέπειες για την προστασία της ιδιωτικότητας. Ωστόσο, υπάρχουν και περιπτώσεις που δεν απαιτούν την επανεξέταση της έκθεσης PIA, όπως η αλλαγή υλικών η οποία δεν επεκτείνει αλλά περιορίζει το

αντικείμενο της χρήσης, καθώς και περιπτώσεις όπου η δημιουργία νέας έκθεσης PIA είναι δικαιολογημένη, όπως στην περίπτωση που αλλάζει το επίπεδο της εφαρμογής, στο πρώτο στάδιο της αρχικής ανάλυσης.

Τελευταία και εξίσου σημαντική διαδικασία είναι η εξασφάλιση διαβουλεύσεων με τους ενδιαφερόμενους. Μέσα στους οργανισμούς, άτομα τα οποία είναι αρμόδια για τη διασφάλιση της ιδιωτικότητας και άτομα με τεχνικές γνώσεις είναι σημαντικά στη διαδικασία υλοποίησης του πλαισίου PIA και η γνώμη τους και τα σχόλιά τους πρέπει να λαμβάνονται υπόψη. Επίσης, η χρήση μηχανισμών διαβούλευσης όπου θα μπορούν να καταθέσουν τα σχόλιά τους οι εξωτερικοί ενδιαφερόμενοι και οι άμεσα επηρεαζόμενοι από την εφαρμογή RFID, όπως οι πελάτες του φορέα εκμετάλλευσης της συγκεκριμένης εφαρμογής RFID, είναι μία ακόμη πρόταση της ομάδας RFID. Τα σχόλια και οι απόψεις που παρατίθενται πρέπει να λαμβάνονται υπόψη και να υπάρχει ανάδραση για την αντιμετώπιση πιθανών προβλημάτων.

Η διαβούλευση με ενδιαφερομένους είναι μία από τις σημαντικότερες διαδικασίες η οποία κρίνεται απαραίτητο να γίνεται[231]. Ειδικότερα, τονίζεται ότι είναι σημαντική η επιλογή των ενδιαφερομένων, η σωστή και πλήρης ενημέρωση αυτών, οι τρόποι παροχής συμβουλών (όπως συνεντεύξεις, έρευνες, θεματικά εργαστήρια, δημόσιες διαβουλεύσεις) και τέλος η εκτίμηση αυτών και η αιτιολόγηση σε περίπτωση απόρριψης.

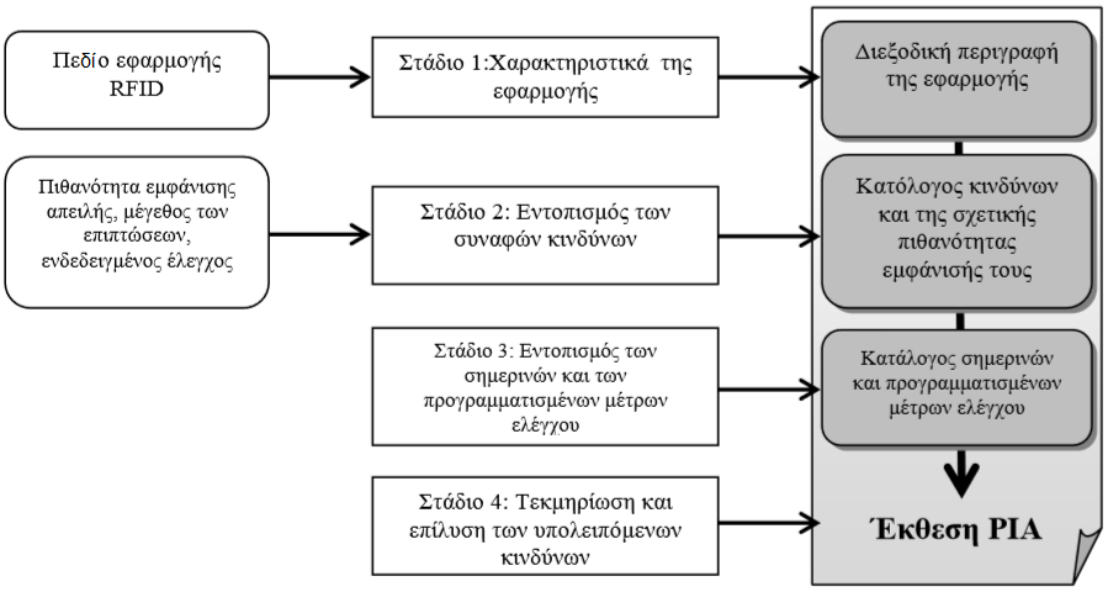
5.4. Η διαδικασία του πλαισίου PIA

Η διαδικασία του αναθεωρημένου πλαισίου PIA χωρίζεται σε δύο φάσεις, τη φάση αρχικής ανάλυσης και τη φάση αξιολόγησης των κινδύνων. Και οι δύο φάσεις είναι εξίσου σημαντικές, αλληλοσυνδεόμενες και αλληλοεξαρτώμενες. Οι φορείς εκμετάλλευσης των εφαρμογών RFID είναι υποχρεωμένοι πρώτα να υλοποιήσουν τη φάση της αρχικής ανάλυσης για να καθορίσουν εάν απαιτείται η υλοποίηση του πλαισίου PIA για την εφαρμογή τους και μετά να εκτελέσουν την επόμενη φάση της εκτίμησης κινδύνων για να

[231] Επίσης βλ. Hert De P., Kloza D. & Wright D (2012). Recommendations for a privacy impact assessment framework for the European Union, ό.π. σελ: 28-29.

προσδιορίζουν τους κινδύνους για την ιδιωτικότητα εξαιτίας της υλοποίησης της εφαρμογής τους.

Η φάση της αρχικής ανάλυσης αποτελείται από ένα στάδιο, το χαρακτηρισμό της εφαρμογής, τη διεξοδική δηλαδή περιγραφή της υπό μελέτη εφαρμογής. Ενώ η φάση εκτίμησης των κινδύνων αποτελείται από τρία στάδια, τον εντοπισμό των κινδύνων που μπορεί να προκύψουν στην ιδιωτικότητα εξαιτίας της υλοποίησης της εφαρμογής, τον προσδιορισμό ελέγχων για τον περιορισμό όλων των εντοπισμένων κινδύνων και τέλος τη τεκμηρίωση των αποτελεσμάτων της παραπάνω ανάλυσης.



Εικόνα 12 Τα στάδια της διαδικασίας PIA

Πηγή: Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID (2011), σελ. 9. Σημειώνεται ότι η ελληνική εκδοχή δεν είναι πλέον διαθέσιμη, ενώ ήταν μέχρι 16/10/2014. Βλ. την αγγλική εκδοχή σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf, σελ. 8.

Η διαδικασία της PIA στοχεύει στην εξέταση όλων των πιθανών κινδύνων και στη συνέχεια εκτιμά το μέγεθος, την πιθανότητα και τον ενδεχόμενο περιορισμό τους. Ως αποτέλεσμα τούτων προκύπτει ο εντοπισμός εκείνων των κινδύνων για την ιδιωτικότητα που είναι πραγματικά σημαντικοί για την εγκατάσταση RFID του οργανισμού και που πρέπει να περιοριστούν μέσω αποτελεσματικών ελέγχων.

Στο προτεινόμενο πλαίσιο τονίζεται ότι[232] προκειμένου να εξοικονομηθεί χρόνος και να περιοριστούν οι δαπάνες, η διεξαγωγή των εν λόγω φάσεων πρέπει να γίνεται αρκετά πριν από τη λήψη των τελικών αποφάσεων, κυρίως όσον αφορά αποφάσεις σχετικά με την αρχιτεκτονική της εφαρμογής RFID. Συγκεκριμένα, οι τεχνικές περιορισμού των κινδύνων, εφόσον έχουν αποδειχθεί αποτελεσματικές και πρέπει να υλοποιηθούν, πρέπει να ενταχθούν έγκαιρα στο στάδιο σχεδιασμού και ανάπτυξης του συστήματος. Ειδάλλως, η μεταγενέστερη υλοποίησή τους μπορεί να καθυστερήσει την εφαρμογή, να αυξήσει το κόστος υλοποίησης και τελικά να μην έχουν τη ίδια αποτελεσματικότητα.

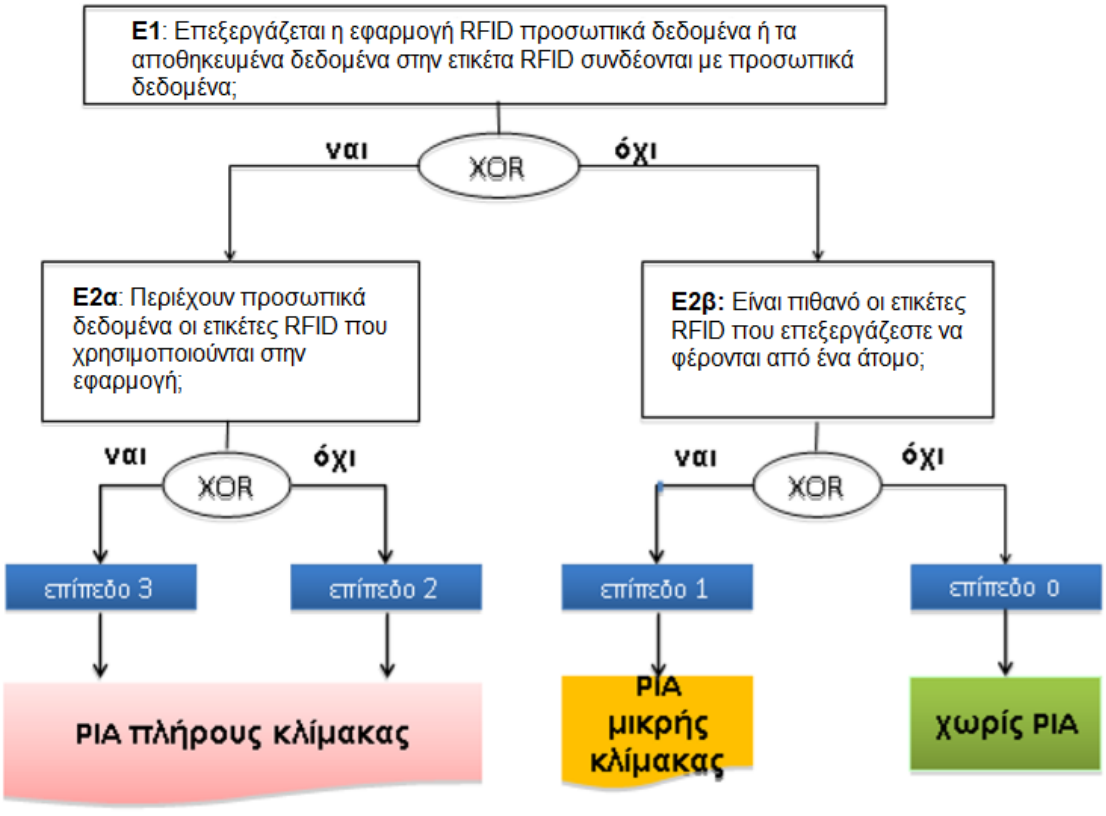
5.4.1. Φάση αρχικής ανάλυσης

Η φάση αρχικής ανάλυσης είναι το πρώτο στάδιο του πλαισίου PIA το οποίο πρέπει να εκτελέσει ο φορέας εκμετάλλευσης. Σε αυτή τη φάση καθορίζεται εάν απαιτείται ή όχι η υλοποίηση του πλαισίου PIA για τη συγκεκριμένη εφαρμογή και αν ναι, σε ποιο βαθμό. Πιο συγκεκριμένα, υπάρχουν απλές περιπτώσεις εφαρμογών RFID που δεν προκαλούν προβλήματα ιδιωτικότητας και επομένως δε χρειάζεται ο φορέας εκμετάλλευσης της εφαρμογής να επιβαρυνθεί παραπάνω σε χρόνο και σε κόστος και να προχωρήσει στη δεύτερη φάση ανάλυσης των κινδύνων. Ενώ, υπάρχουν και περιπτώσεις οι οποίες προκαλούν προβλήματα ιδιωτικότητας και μάλιστα σε διαφορετικό βαθμό η καθεμία. Ο βαθμός που προκαλούν προβλήματα ιδιωτικότητας καθορίζεται από το εάν συνδέονται με προσωπικά δεδομένα ή εάν απευθείας επεξεργάζονται προσωπικά δεδομένα. Σε αυτές τις περιπτώσεις ο φορέας οφείλει να προχωρήσει στην επόμενη φάση ανάλυσης κινδύνων και να ολοκληρώσει το πλαίσιο PIA.

[232] Βλ. Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID (2011), σελ. 8. Σημειώνεται ότι η ελληνική εκδοχή δεν είναι πλέον διαθέσιμη, ενώ ήταν μέχρι 16/10/2014. Βλ. την αγγλική εκδοχή σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf, σελ. 8.

Η ομάδα εργασίας RFID, για να βοηθήσει τους φορείς εκμετάλλευσης στη λήψη αποφάσεων σε αυτό το πρώτο στάδιο, πρότεινε το παρακάτω δενδροδιάγραμμα αποφάσεων (βλ. Εικόνα 13). Στο δενδροδιάγραμμα αυτό παρουσιάζονται οι παρακάτω ερωτήσεις τις οποίες πρέπει να απαντήσει ο φορέας εκμετάλλευσης RFID και οι απαντήσεις σε κάθε περίπτωση είναι της μορφής ναι ή όχι.

- (Ε1): Επεξεργάζεται η εφαρμογή RFID προσωπικά δεδομένα; Ή θα συνδέει η εφαρμογή RFID, τα δεδομένα RFID με προσωπικά δεδομένα?
- (Ε2α): Περιέχουν προσωπικά δεδομένα οι ετικέτες RFID που χρησιμοποιούνται στην εφαρμογή RFID;
- (Ε2β): Είναι πιθανό οι ετικέτες RFID που επεξεργάζεστε να φέρονται από ένα άτομο;



Εικόνα 13 Δενδροδιάγραμμα αποφάσεων σχετικά με τη διεξαγωγή PIA

Πηγή: Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID (2011), σελ. 8. Σημειώνεται ότι η ελληνική εκδοχή δεν είναι πλέον διαθέσιμη, ενώ ήταν μέχρι 16/10/2014. Βλ. την αγγλική εκδοχή σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf, σελ. 7.

Οι ερωτήσεις αυτές βοηθάνε τον φορέα εκμετάλλευσης RFID προκειμένου να αποφασίσει εάν η εφαρμογή του απαιτεί την υλοποίηση της δεύτερης φάσης του πλαισίου PIA και σε ποιο βαθμό, ανάλογα με το επίπεδο στο οποίο ανήκει η εφαρμογή τους. Ο χαρακτηρισμός των εφαρμογών σε επίπεδα δηλώνει το επίπεδο λεπτομερειών που απαιτείται στην επόμενη φάση εκτίμησης και ανάλυσης των κινδύνων. Η πρώτη βασική ερώτηση κλειδί που πρέπει να απαντηθεί είναι εάν η εφαρμογή RFID επεξεργάζεται προσωπικά δεδομένα ή αν τα αποθηκευμένα δεδομένα στην ετικέτα RFID συνδέονται με προσωπικά δεδομένα. Η απάντηση σε αυτή την ερώτηση θα καθορίσει εάν χρειάζεται ή όχι η υλοποίηση του πλαισίου PIA.

Εάν η απάντηση στην αρχική ερώτηση (Ε1) είναι ότι όχι, δεν επεξεργάζεται προσωπικά δεδομένα, τότε αρκεί να απαντήσει στη δεύτερη ερώτηση (Ε2β, στα δεξιά του δενδροδιαγράμματος αποφάσεων) εάν είναι πιθανό αυτές τις ετικέτες RFID να τις φέρουν άτομα. Εδώ, ο φορέας εκμετάλλευσης RFID καλείται να ελέγξει εάν η εφαρμογή μπορεί να προκαλέσει πρόβλημα και πέρα της δικής τους υλοποίησης. Εάν και πάλι η απάντηση είναι όχι, σημαίνει ότι η εφαρμογή RFID δε φέρει κανένα κίνδυνο ιδιωτικότητας, άρα είναι επιπέδου 0 και επομένως δε χρειάζεται ο φορέας εκμετάλλευσης να προχωρήσει στην υλοποίηση του πλαισίου PIA. Εάν η απάντηση είναι ότι όχι δεν επεξεργάζεται προσωπικά δεδομένα, αλλά είναι πιθανό τις ετικέτες RFID να τις φέρουν άτομα, τότε η εφαρμογή είναι επιπέδου 1 και χρειάζεται ο φορέας εκμετάλλευσης να υλοποιήσει το πλαίσιο PIA μικρής κλίμακας, δηλαδή πιο περιορισμένο στο επίπεδο των λεπτομερειών διότι είναι χαμηλού κινδύνου. Σε αυτή την περίπτωση (Ε2β) είναι πολύ σημαντικό οι φορείς εκμετάλλευσης να σκεφτούν διεξοδικά όλες τις πιθανές περιπτώσεις που μπορεί κάποιος να φέρει μαζί του την ετικέτα RFID και εκτός του χώρου του οργανισμού και την επικινδυνότητά του.

Στην αντίθετη περίπτωση που η απάντηση στην αρχική ερώτηση (Ε1) είναι θετική, δηλαδή ότι η εφαρμογή επεξεργάζεται προσωπικά δεδομένα, τότε πρέπει να απαντήσει στην ερώτηση (Ε2α, αριστερά του δενδροδιαγράμματος) εάν οι ετικέτες RFID της εφαρμογής περιέχουν προσωπικά δεδομένα. Εάν η

απάντηση είναι ότι όχι δεν περιέχουν προσωπικά δεδομένα αλλά συνδέονται με προσωπικά δεδομένα και τα επεξεργάζονται, τότε η εφαρμογή είναι επιπέδου 2. Ενώ στην αντίθετη περίπτωση, όπου οι ετικέτες περιέχουν προσωπικά δεδομένα, η οποία αποτελεί και την πιο επικίνδυνη περίπτωση για την προσβολή της ιδιωτικότητας, τότε η εφαρμογή είναι επιπέδου 3. Και στις δύο αυτές περιπτώσεις το προς υλοποίηση πλαίσιο PIA είναι πλήρους κλίμακας γιατί απαιτείται λεπτομερής εκτίμηση των κινδύνων, χαρακτηρίζονται όμως ως εφαρμογές διαφορετικού επιπέδου (2 και 3).

Στην περίπτωση υλοποίησης του πλαισίου PIA μικρής κλίμακας[233], οι εφαρμογές χαρακτηρίζονται ως επιπέδου 1 καθώς έχουν χαμηλά χαρακτηριστικά κινδύνων και επομένως το πλαίσιο PIA θα είναι πιο περιορισμένο στο αντικείμενο και στο επίπεδο των λεπτομερειών. Ενώ στην περίπτωση υλοποίησης του πλαισίου PIA της πλήρους κλίμακας[234], οι εφαρμογές χαρακτηρίζονται ως επιπέδου 2 εάν επεξεργάζονται προσωπικά δεδομένα ή ως επιπέδου 3 εάν οι ετικέτες έχουν αποθηκευμένα προσωπικά δεδομένα και σε αυτές τις περιπτώσεις στο πλαίσιο PIA απαιτείται λεπτομερής εκτίμηση των κινδύνων ώστε να εντοπιστούν όλοι οι πιθανοί κίνδυνοι και να βρεθούν οι κατάλληλοι έλεγχοι. Η διαφορά στα τελευταία δύο επίπεδα στην εκτέλεση του πλαισίου PIA της πλήρους κλίμακας είναι στο περιβάλλον κινδύνου και στις στρατηγικές περιορισμού.

Σε αυτή τη φάση της αρχικής ανάλυσης, σε κάθε περίπτωση, σε οποιοδήποτε επίπεδο και αν ανήκει η εφαρμογή, είτε χρειάζεται να υλοποιηθεί το πλαίσιο PIA, είτε όχι, ο φορέας εκμετάλλευσης οφείλει να δημιουργήσει ένα έγγραφο το οποίο θα καταθέσει στην αρμόδια αρχή προστασίας προσωπικών δεδομένων, εφόσον του ζητηθεί. Στο έγγραφο αυτό θα παρουσιάζονται

[233] Βλ. Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID (2011), σελ. 8. Σημειώνεται ότι η ελληνική εκδοχή δεν είναι πλέον διαθέσιμη, ενώ ήταν μέχρι 16/10/2014. Βλ. την αγγλική εκδοχή σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf, σελ. 7. Σύμφωνα με τον Wright D. (2011) το πλαίσιο PIA μικρής κλίμακας είναι η ίδια διαδικασία με το πλαίσιο PIA πλήρους κλίμακας, αλλά λιγότερο τυποποιημένη και δεν απαιτεί ούτε πολύ χρόνο, ούτε πολλούς πόρους για την υλοποίησή του.

[234] Βλ. Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID (2011), σελ. 7. Σημειώνεται ότι η ελληνική εκδοχή δεν είναι πλέον διαθέσιμη, ενώ ήταν μέχρι 16/10/2014. Βλ. την αγγλική εκδοχή σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf, σελ. 7.

αναλυτικά και με πλήρη τεκμηρίωση όλες οι πληροφορίες που συγκεντρώθηκαν στην αρχική φάση της ανάλυσης, ώστε να απαντηθούν οι ερωτήσεις του δενδροδιαγράμματος και να παρθεί η απόφαση εάν η εφαρμογή απαιτεί την υλοποίηση της δεύτερης φάσης του πλαισίου PIA και σε ποιο βαθμό.

Το έγγραφο αυτό προς κατάθεση στην ουσία είναι μία διεξοδική περιγραφή της λειτουργίας της εφαρμογής. Πρέπει να περιέχει πληροφορίες σχετικά με τους σκοπούς της εφαρμογής, τους τύπους των επεξεργασμένων και των αποθηκευμένων στοιχείων, τη διάρκεια αποθήκευσης, τα κριτήρια πρόσβασης (ποιοι και γιατί) και πώς ελέγχονται, τους σκοπούς μεταβίβασης είτε εσωτερικά, είτε εξωτερικά του οργανισμού και τους πιθανούς αποδέκτες, καθώς και πληροφορίες σχετικά με τη χρησιμοποιούμενη τεχνολογία. Η άτυπη ομάδα εργασίας RFID, προς διευκόλυνση των φορέων εκμετάλλευσης δημιούργησε έναν πίνακα ώστε να δώσει τις κατευθυντήριες γραμμές σχετικά με τις απαιτούμενες πληροφορίες που πρέπει να συγκεντρωθούν για την επαρκή και πλήρη τεκμηρίωση (βλ. παρακάτω Πίνακας 11).

Πίνακας 11 Απαιτούμενες πληροφορίες για την περιγραφή της τεχνολογίας RFID στη φάση της αρχικής ανάλυσης

Πηγή: Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID (2011), σελ. 13. Σημειώνεται ότι η ελληνική εκδοχή δεν είναι πλέον διαθέσιμη, ενώ ήταν μέχρι 16/10/2014. Βλ. την αγγλική εκδοχή σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf, σελ. 12.

Φορέας εκμετάλλευσης εφαρμογής RFID	• επωνυμία και έδρα νομικής οντότητας • πρόσωπο ή γραφείο αρμόδιο για την έγκαιρη εκτέλεση της PIA • αρμόδιοι επαφής και μέθοδος απεύθυνσης στον φορέα εκμετάλλευσης
Επισκόπηση εφαρμογής RFID	• όνομα εφαρμογής RFID • σκοπός(οί) εφαρμογής(ών) RFID • βασικά σενάρια χρήσης της εφαρμογής RFID • συστατικά στοιχεία και χρησιμοποιούμενη τεχνολογία εφαρμογής RFID (π.χ. συχνότητες κ.λπ.) • γεωγραφικό πεδίο της εφαρμογής RFID • τύποι χρηστών / ατόμων που επηρεάζονται από την εφαρμογή RFID • πρόσβαση ατόμων και έλεγχος
Αριθμός έκθεσης PIA	• αριθμός έκδοσης της έκθεσης PIA (διάκριση αν πρόκειται για νέα PIA ή απλώς για τροποποιήσεις ήσσονος σημασίας) • ημερομηνία τελευταίας τροποποίησης στην έκθεση PIA
Επεξεργασία δεδομένων RFID	• κατάλογος τύπων των επεξεργασμένων στοιχείων δεδομένων • ύπαρξη ευαίσθητων πληροφοριών στα δεδομένα πριν από την επεξεργασία, π.χ. υγεία
Αποθήκευση δεδομένων	• κατάλογος τύπων των αποθηκευμένων στοιχείων δεδομένων • διάρκεια αποθήκευσης
Εσωτερική μεταβίβαση δεδομένων	• περιγραφή διαγραμμάτων ή ροής δεδομένων στις εσωτερικές πράξεις όπου περιλαμβάνονται δεδομένα RFID • σκοπός(οί) μεταβίβασης των δεδομένων προσωπικού χαρακτήρα
Εξωτερική μεταβίβαση δεδομένων RFID (αν υπάρχει)	• τύπος αποδέκτη(ών) δεδομένων • εν γένει σκοπός(οί) μεταβίβασης ή πρόσβασης • προσδιορισμένο ή / και προσδιορίσιμο επίπεδο δεδομένων προσωπικού χαρακτήρα στη μεταβίβαση • μεταβιβάσεις εκτός Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ)

Αξίζει να σημειωθεί ότι μια εναλλακτική περίπτωση είναι η χρήση των ερωτήσεων στον οδηγό που εξέδωσε ο Επίτροπος Προστασίας Προσωπικών Δεδομένων της Βικτώριας (Αυστραλία) το 2009[235] σχετικά με την υλοποίηση

[235] Office of the Victorian Privacy Commissioner, Privacy Impact Assessments - A guide for the Victorian Public Sector, Edition 2, Melburne, April 2009, σελ. 5 και 22, διαθέσιμο στο

της διαδικασίας PIA στο δημόσιο τομέα. Συγκεκριμένα, πρότεινε για την πρώτη φάση της ανάλυσης την απάντηση 17 ερωτήσεων από έναν αρμόδιο υπάλληλο ο οποίος δεν είναι απαραίτητο να έχει γνώσεις στην προστασία της ιδιωτικότητας. Εάν έστω και σε μία από αυτές τις ερωτήσεις η απάντηση είναι ναι, τότε πρέπει να τις παραδώσει στον υπεύθυνο προστασίας των προσωπικών δεδομένων και να μελετηθεί το ενδεχόμενο εκτέλεσης του πλαισίου PIA.

5.4.2. Φάση εκτίμησης κινδύνων

Η εκτίμηση των κινδύνων είναι η διαδικασία αναγνώρισης, ανάλυσης και αξιολόγησης των κινδύνων[236]. Πιο συγκεκριμένα η διαδικασία της αναγνώρισης των κινδύνων περιλαμβάνει την εύρεση και την περιγραφή αυτών και ειδικότερα την εύρεση των πηγών τους, τις αιτίες και τις πιθανές συνέπειες χρησιμοποιώντας ιστορικά στοιχεία αλλά και διαβουλεύσεις εμπειρογνώμων. Η διαδικασία της ανάλυσης των κινδύνων περιλαμβάνει την κατανόηση της φύσης των κινδύνων, την εκτίμησή τους και τον καθορισμό του επιπέδου τους σύμφωνα με το μέγεθος και την πιθανότητα εμφάνισης. Και τέλος, η διαδικασία αξιολόγησης των κινδύνων είναι η σύγκριση των αποτελεσμάτων της ανάλυσης και ορίζεται κατά πόσο ο κάθε κίνδυνος είναι αποδεκτός ή χρήζει αντιμετώπισης.

Στην περίπτωσή μας, εφόσον ο φορέας εκμετάλλευσης έχει εκτελέσει την πρώτη φάση αρχικής ανάλυσης και η εφαρμογή έχει αποδειχθεί ότι είναι επιπέδου 1, 2 ή 3, τότε οφείλει να προχωρήσει στη δεύτερη φάση εκτίμησης των κινδύνων. Η ορθή εκτέλεση της πρώτης φάσης, η διεξοδική δηλαδή περιγραφή της εφαρμογής, συνεισφέρει σημαντικά στην εκτέλεση της δεύτερης φάσης.

---

https://www.privacy.vic.gov.au/privacy/web2.nsf/files/privacy-impact-assessments-guide/$file/guideline_05_09_no1.pdf

[236] Βλ. Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization, ISO) (2009), ISO Guide 73:2009. Risk Management – Vocabulary, διαθέσιμο στο https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en:term:3.8.1

Στόχος λοιπόν της δεύτερης φάσης είναι ο εντοπισμός των κινδύνων της ιδιωτικότητας, η αξιολόγησή τους και η εύρεση τρόπων περιορισμού αυτών με ελέγχους. Ειδικότερα, εντοπίζονται και εκτιμώνται όλοι οι πιθανοί κίνδυνοι προσβολής της ιδιωτικότητας εξαιτίας της υλοποίησης της υπό μελέτη εφαρμογής RFID. Έπειτα, προτείνονται στρατηγικές ελαχιστοποίησης αυτών και τέλος τεκμηριώνονται όλα τα παραπάνω αποτελέσματα στην έκθεση PIA[237]. Η άτυπη ομάδα εργασίας RFID διευκρινίζει ότι με την υλοποίηση της φάσης αυτής επιτυγχάνεται συμμόρφωση και ικανοποίηση των νομικών απαιτήσεων της προστασίας της ιδιωτικότητας, όπως ορίζονται στην Οδηγία 95/46[238].

Αξίζει να σημειωθεί ότι στη βιβλιογραφία υπάρχουν διάφορες προτεινόμενες μέθοδοι διαχείρισης κινδύνων οι οποίες είναι εξίσου αποτελεσματικές. Σύμφωνα όμως με τον Διεθνή Οργανισμό Τυποποίησης[239], ο σχεδιασμός της κατάλληλης μεθόδου διαχείρισης των κινδύνων εξαρτάται κάθε φορά από τον οργανισμό στον οποίο εφαρμόζεται, όπως από τις ανάγκες, τους στόχους και τη δομή του.

Παρακάτω παρουσιάζονται τα στάδια ολοκλήρωσης της φάσης εκτίμησης των κινδύνων, όπως προτάθηκαν από την άτυπη ομάδα εργασίας RFID στο προτεινόμενο πλαίσιο PIA.

5.4.2.1. Εντοπισμός των κινδύνων

Αρχικά, εντοπίζονται όλοι οι πιθανοί κίνδυνοι προσβολής της ιδιωτικότητας εξαιτίας της υλοποίησης της υπό μελέτη εφαρμογής RFID. Η διαδικασία αυτή εντοπισμού των κινδύνων είναι από τις πιο κρίσιμες και τις πιο δύσκολες καθώς οι κίνδυνοι μπορεί να εντοπιστούν είτε από το

[237] Σχετικά με την έκθεση PIA βλ. Μέρος δεύτερο, υποκεφάλαιο 5.4.3.

[238] Βλ. Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID (2011), σελ. 8. Σημειώνεται ότι η ελληνική εκδοχή δεν είναι πλέον διαθέσιμη, ενώ ήταν μέχρι 16/10/2014. Βλ. την αγγλική εκδοχή σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf, σελ. 7.

[239] Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization, ISO) (2009), ISO 31000:2009, Risk management - Principles and guidelines, ενότητα: 1. Scope, διαθέσιμο στο https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en.

εσωτερικό, είτε από το εξωτερικό περιβάλλον[240]. Συνήθως όμως, οι κίνδυνοι προκύπτουν από τις χρήσεις αλλά και τις καταχρήσεις των πληροφοριών που επεξεργάζεται η εφαρμογή και κυρίως εάν οι ετικέτες περάσουν στην κατοχή των πελατών και ταυτόχρονα παραμείνουν οι πληροφορίες ενεργές στην επιχείρηση.

Έπειτα, γίνεται σχετική ποσοτικοποίηση των κινδύνων που εντοπίστηκαν και εκτίμηση αυτών από την σκοπιά της ιδιωτικότητας προκειμένου να καθοριστούν βάσει επικινδυνότητας. Δηλαδή υπολογίζεται το επίπεδο των κινδύνων (κίνδυνοι υψηλού, μέσου ή χαμηλού επιπέδου), η πιθανότητα εμφάνισής τους και το μέγεθος των επιπτώσεων βάσει των αρχών προστασίας των προσωπικών δεδομένων. Οι κίνδυνοι σε αυτό το στάδιο χαρακτηρίζονται μεγάλοι εάν το επίπεδο κινδύνου είναι υψηλό, μεσαίοι εάν το επίπεδο κινδύνου είναι μέσο και μικροί εάν το επίπεδο κινδύνου είναι χαμηλό.

Η άτυπη ομάδα εργασίας RFID, πρότεινε στους φορείς εκμετάλλευσης εφαρμογών RFID να λάβουν υπόψη τους τους στόχους προστασίας της ιδιωτικότητας που περιλαμβάνονται στην Οδηγία 95/46/ΕΚ (βλ. Πίνακας 12) προκειμένου να προσδιορίσουν τις συνθήκες εμφάνισης των κινδύνων που απειλούν τους στόχους αυτούς. Επίσης, δημιούργησε και έναν κατάλογο δυνητικών κινδύνων για την προστασία της ιδιωτικότητας από τη χρήση εφαρμογών RFID (βλ. Πίνακας 13) για μεγαλύτερη διευκόλυνση. Οι κίνδυνοι αυτοί όμως τονίζεται ότι είναι παραδείγματα και αποτελούν μονάχα έναν οδηγό για τον προσδιορισμό ενδεχόμενων κινδύνων, επομένως πιθανόν να μην καλύπτουν όλες τις περιπτώσεις εφαρμογών. Λεπτομερής ενημέρωση σχετικά με τον εντοπισμό των κινδύνων θα γίνει εφόσον αναπτυχθούν εξειδικευμένα μοντέλα βάσει του εν λόγω προτεινόμενου πλαισίου και χρησιμοποιηθούν σε διάφορους κλάδους δραστηριοτήτων.

[240] Η καλή περιγραφή της εφαρμογής RFID και η διαβούλευση με ενδιαφερόμενους συμβάλουν σημαντικά στον εντοπισμό των κινδύνων. Βλ. Hert De P., Kloza D. & Wright D (2012). Recommendations for a privacy impact assessment framework for the European Union, Παραδοτέο D3 του έργου PIAF (A Privacy Impact Assessment Framework for data protection and privacy rights), σελ. 30, υποκεφάλαιο 3.3.4.1. Risks Assessment, διαθέσιμο στο https://piafproject.files.wordpress.com/2018/03/piaf_d3_final.pdf

Πίνακας 12 Στόχοι προστασίας της ιδιωτικότητας σύμφωνα με την Οδηγία 95/46/ΕΚ

Πηγή: Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID (2011), σελ. 14-15. Σημειώνεται ότι η ελληνική εκδοχή δεν είναι πλέον διαθέσιμη, ενώ ήταν μέχρι 16/10/2014. Βλ. την αγγλική εκδοχή σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf, σελ. 13

Στόχος	Περιγραφή του στόχου
Διασφάλιση της ποιότητας των δεδομένων προσωπικού χαρακτήρα	Οι κύριοι στόχοι που πρέπει να εξασφαλιστούν είναι η αποφυγή και ελαχιστοποίηση των δεδομένων, ο προσδιορισμός και ο καθορισμός του σκοπού, η ποιότητα των δεδομένων και η διαφάνεια.
Σύννομος χαρακτήρας της επεξεργασίας προσωπικών δεδομένων	Πρέπει να εξασφαλίζεται ο σύννομος χαρακτήρας της επεξεργασίας προσωπικών δεδομένων υπό όρους συναίνεσης, συμβατικής συμφωνίας, νομικής υποχρέωσης κ.λπ.
Σύννομος χαρακτήρας της επεξεργασίας ευαίσθητων προσωπικών δεδομένων	Πρέπει να εξασφαλίζεται ο σύννομος χαρακτήρας της επεξεργασίας ευαίσθητων προσωπικών δεδομένων υπό όρους ρητής συναίνεσης, ειδικής νομικής βάσης κ.λπ.
Συμμόρφωση με το δικαίωμα του υποκειμένου των δεδομένων να τηρείται ενήμερο	Πρέπει να εξασφαλίζεται ότι το υποκείμενο των δεδομένων ενημερώνεται εγκαίρως σχετικά με τη συλλογή των δεδομένων του.
Συμμόρφωση με το δικαίωμα του υποκειμένου των δεδομένων για πρόσβαση σε δεδομένα, διόρθωση και διαγραφή τους	Πρέπει να εξασφαλίζεται η έγκαιρη εκπλήρωση της επιθυμίας του υποκειμένου των δεδομένων για πρόσβαση, διόρθωση, διαγραφή και φραγή των δεδομένων του.
Συμμόρφωση με το δικαίωμα εναντίωσης του υποκειμένου των δεδομένων	Πρέπει να εξασφαλίζεται ότι τα δεδομένα του υποκειμένου δεν υφίστανται πλέον επεξεργασία εφόσον αυτό αντιτάσσεται. Ιδιαίτερα πρέπει να εξασφαλίζεται η διαφάνεια αυτοματοποιημένων αποφάσεων όσον αφορά άτομα.
Διασφάλιση του απορρήτου & της ασφάλειας της επεξεργασίας	Βασικοί στόχοι που πρέπει να εξασφαλιστούν είναι η αποτροπή μη εξουσιοδοτημένης πρόσβασης, η καταγραφή της επεξεργασίας δεδομένων, η ασφάλεια δικτύων και μεταφορών, καθώς και η αποτροπή τυχαίας απώλειας δεδομένων.
Συμμόρφωση με τις απαιτήσεις κοινοποίησης	Βασικοί στόχοι που πρέπει να εξασφαλιστούν είναι η κοινοποίηση σχετικά με την επεξεργασία δεδομένων, ο έλεγχος και η τεκμηρίωση της προηγούμενης συμμόρφωσης.
Συμμόρφωση με τις απαιτήσεις διαφύλαξης των δεδομένων	Η διαφύλαξη των δεδομένων πρέπει να ισχύει για την ελάχιστη χρονική περίοδο, ανάλογα με το σκοπό της ή με άλλες νομικές απαιτήσεις.

Πίνακας 13 Ενδεχόμενοι κίνδυνοι που σχετίζονται με τη χρήση της τεχνολογίας RFID προτεινόμενοι από την άτυπη ομάδα εργασίας RFID

Πηγή: Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID (2011), σελ. 16-18. Σημειώνεται ότι η ελληνική εκδοχή δεν είναι πλέον διαθέσιμη, ενώ ήταν μέχρι 16/10/2014. Βλ. την αγγλική εκδοχή σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf, σελ. 14-16.

Κίνδυνος για την ιδιωτικότητα	Περιγραφή και περιεχόμενο
Μη καθορισμένος και μη περιορισμένος σκοπός	Ο σκοπός της συλλογής δεδομένων δεν έχει καθοριστεί και δεν έχει τεκμηριωθεί ή χρησιμοποιούνται περισσότερα δεδομένα από τα απαιτούμενα για το συγκεκριμένο σκοπό. Παράδειγμα: Δεν υπάρχει τεκμηρίωση των σκοπών για για τους οποίους χρησιμοποιούνται δεδομένα RFID ή/και χρήση δεδομένων RFID για κάθε είδος εφικτής ανάλυσης.
Η συλλογή υπερβαίνει το σκοπό	Τα δεδομένα συλλέγονται σε αναγνωρίσιμη μορφή που υπερβαίνει την προσδιορισμένη στο σκοπό έκταση. Παράδειγμα: Οι πληροφορίες της κάρτας πληρωμών RFID χρησιμοποιούνται μόνο για το σκοπό της επεξεργασίας των συναλλαγών αλλά και για τη δημιουργία ατομικών προφίλ.
Ελλιπείς πληροφορίες ή έλλειψη διαφάνειας	Οι πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων σχετικά με το σκοπό και τη χρήση των δεδομένων δεν είναι πλήρεις, η επεξεργασία των δεδομένων δεν καθίσταται διαφανής, ή δεν παρέχονται εγκαίρως οι πληροφορίες. Παράδειγμα: Στους καταναλωτές διατίθενται πληροφορίες RFID χωρίς σαφή πληροφόρηση σχετικά με τον τρόπο επεξεργασίας και χρήσης των δεδομένων RFID, την ταυτότητα του φορέα εκμετάλλευσης ή τα δικαιώματα των χρηστών.
Ο συνδυασμός υπερβαίνει το σκοπό	Τα προσωπικά δεδομένα συνδυάζονται σε βαθμό που δεν επιβάλλει ο καθορισμένος σκοπός. Παράδειγμα: Οι πληροφορίες της κάρτας πληρωμών RFID συνδυάζονται με δεδομένα προσωπικού χαρακτήρα που έχουν αποκτηθεί από τρίτους.
Δεν υφίστανται πολιτικές ή μηχανισμοί διαγραφής δεδομένων	Τα δεδομένα τηρούνται για χρονικό διάστημα μεγαλύτερο από το απαραίτητο για την κάλυψη του καθορισμένου σκοπού. Παράδειγμα: Προσωπικά δεδομένα συλλέγονται ως μέρος της εφαρμογής και αποθηκεύονται για χρονικό διάστημα μεγαλύτερο από το νόμιμο.
Ακύρωση ρητής συναίνεσης (Διακύβευση της ελευθερίας της συγκατάθεσης)	Η συναίνεση έχει προκύψει υπό την απειλή μειονεκτήματος/ζημίας. Παράδειγμα: Αδυναμία επιστροφής / ανταλλαγής / χρήσης νομικών εγγυήσεων για προϊόντα όταν η ετικέτα RFID έχει απενεργοποιηθεί ή αφαιρεθεί (βλ. και υπ' αριθ. 42 αιτιολογική σκέψη Κανονισμού 2016/679).
Κρυφή συλλογή δεδομένων από τον φορέα εκμετάλλευσης RFID	Ορισμένα δεδομένα καταγράφονται κρυφά και εν αγνοία του υποκειμένου των δεδομένων, π.χ. τα προφίλ κινήσεων. Παράδειγμα: Πληροφορίες σχετικά με τους καταναλωτές συλλέγονται ενώ περπατούν μπροστά από καταστήματα ή σε εμπορικά κέντρα χωρίς να προειδοποιούνται, με λογότυπο ή έμβλημα, σχετικά με την ανάγνωση RFID.

Αδυναμία χορήγησης πρόσβασης	Το υποκείμενο των δεδομένων δεν μπορεί να αρσκήσει το δικαιώμα διόρθωσης ή διαγραφής. Παράδειγμα: Ο εργοδότης δεν μπορεί να παράσχει στους απασχολούμενους πλήρη εικόνα των αποθηκευμένων στοιχείων που τους αφορούν και έχουν συλλεγεί από πρόσβαση σε RFID και δεδομένα παραγωγής.
Παρεμπόδιση άσκησης δικαιωμάτων	Δεν υφίστανται τεχνικά ή επιχειρησιακά μέσα ανταπόκρισης στην άσκηση δικαιωμάτων του υποκειμένου των δεδομένων. Παράδειγμα: Επισκέπτης νοσοκομείου δεν μπορεί να αυτοεξαιρεθεί εμποδίζοντας την ανάγνωση ευαίσθητων προσωπικών πληροφοριών σε ετικέτες (δηλ. σε συνταγογραφημένα φάρμακα).
Έλλειψη διαφάνειας σχετικά με αυτοματοποιημένη ατομική λήψη αποφάσεων	Χρησιμοποιείται αυτοματοποιημένη ατομική λήψη αποφάσεων που βασίζεται σε προσωπικές πτυχές, αλλά το υποκείμενο των δεδομένων δεν ενημερώνεται σχετικά με τη λογική της διαδικασίας λήψης της απόφασης (πρβλ. στο άρθρο 22 του Κανονισμού 2016/679). Παράδειγμα: Χωρίς ενημέρωση των καταναλωτών, ένας φορέας εκμετάλλευσης RFID διαβάζει όλες τις ετικέτες που φέρει ένα άτομο, περιλαμβανομένων και αυτών άλλης οντότητας, και βάσει αυτών καθορίζει τον τύπο του διαφημιστικού
Ανεπαρκής διαχείριση δικαιωμάτων πρόσβασης	Δεν γίνεται ανάκληση των δικαιωμάτων πρόσβασης όταν αυτά δεν είναι πλέον απαραίτητα. Παράδειγμα: Μέσω μιας κάρτας RFID, ένας πρώην ασκούμενος αποκτά πρόσβαση σε τμήματα μιας επιχείρησης, ως μη όφειλε.
Ανεπαρκής μηχανισμός επαλήθευσης ταυτότητας	Δεν αποτρέπεται εντυπωσιακός αριθμός αποπειρών ταυτοποίησης και επαλήθευσης ταυτότητας. Παράδειγμα: Τα προσωπικά δεδομένα που περιέχονται σε ταυτότητες δεν προστατεύονται εκ κατασκευής μέσω συνθηματικού κωδικού ή αλλού μηχανισμού επαλήθευσης ταυτότητας.
Αθέμιτη επεξεργασία δεδομένων	Η επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν βασίζεται σε συναίνεση, σύμβαση, νομική υποχρέωση κ.λπ. Παράδειγμα: Ένας φορέας εκμετάλλευσης RFID ανταλλάσσει με τρίτους πληροφορίες που έχει συλλέξει χωρίς ειδοποίηση ή συναίνεση, όπως συνήθως επιτάσσει ο νόμος.
Ανεπαρκής μηχανισμός καταγραφής / πρωτοκόλλησης	Ο εφαρμοζόμενος μηχανισμός καταγραφής / πρωτοκόλλησης είναι ανεπαρκής. Δεν καταγράφονται/πρωτοκολλούνται διοικητικές διαδικασίες. Παράδειγμα: Δεν καταγράφονται όσοι είχαν πρόσβαση στα δεδομένα της κάρτας RFID ενός απασχολούμενου.
Ανεξέλεγκτη συλλογή δεδομένων από ετικέτες RFID	Κίνδυνος δυνατότητας χρησιμοποίησης των ετικετών RFID για συστηματική διαμόρφωση προφίλ. Παράδειγμα: Οι λιανοπωλητές διαβάζουν όλες τις ετικέτες στις οποίες μπορούν να έχουν πρόσβαση.

5.4.2.2. Προσδιορισμός και διενέργεια ελέγχων

Αφού λοιπόν έχουν εντοπιστεί οι ενδεχόμενοι κίνδυνοι της ιδιωτικότητας, το επόμενο στάδιο είναι να προσδιοριστούν και οι έλεγχοι που θα γίνονται για την ελαχιστοποίηση, τον περιορισμό και στην ιδανικότερη περίπτωση την εξάλειψη αυτών. Για κάθε πιθανό κίνδυνο πρέπει να προταθεί συγκεκριμένος έλεγχος και να αιτιολογηθεί πώς και γιατί ο έλεγχος αυτός θα μετριάσει τον κίνδυνο σε τέτοιο βαθμό ώστε να πάψει να είναι πρόβλημα και να προσβάλει την ιδιωτικότητα.

Οι έλεγχοι αυτοί, σύμφωνα με την άτυπη ομάδα εργασίας RFID, είναι τεχνικοί, μη τεχνικοί και φυσικοί. Οι έλεγχοι τεχνικής φύσεως αφορούν την αρχιτεκτονική και τις τεχνικές πολιτικές που εφαρμόζονται στην εφαρμογή RFID, για παράδειγμα μηχανισμοί ελέγχου πρόσβασης και μέθοδοι κρυπτογράφησης. Οι έλεγχοι μη τεχνικής φύσεως είναι διαχειριστικοί και επιχειρησιακοί και αφορούν προληπτικούς ελέγχους για την αποτροπή παραβιάσεων και ανιχνευτικούς ελέγχους για την προειδοποίηση σχετικά με πιθανές παραβιάσεις. Τέλος, μπορούν να γίνουν και φυσικοί έλεγχοι, όπως η φυσική ύπαρξη ή μη αναγνωστών για την παρακολούθηση των ετικετών. Απαραίτητο είναι να γίνει και ανάλυση κόστους των προτεινόμενων ελέγχων προκειμένου να αποφασιστεί ποιοι είναι οι καταλληλότεροι προς υλοποίηση[241].

Στο παράρτημα IV του προτεινόμενου πλαισίου, η άτυπη ομάδα εργασίας RFID συμπεριέλαβε έναν κατάλογο παραδειγμάτων με πιθανά μέτρα ελέγχου (βλ. Πίνακας 14). Οι προτεινόμενοι έλεγχοι αποτελούν παραδείγματα προκειμένου να βοηθηθούν οι φορείς εκμετάλλευσης εφαρμογών RFID στην εξεύρεση ενδεδειγμένων στρατηγικών περιορισμού και τονίζεται ότι είναι επικουρικοί στο υφιστάμενο κανονιστικό πλαίσιο της ΕΕ για την προστασία των δεδομένων και δεν επιδιώκει τροποποίηση ή αλλαγή αυτού.

[241] Βλ. Hert De P., Kloza D. & Wright D (2012). Recommendations for a privacy impact assessment framework for the European Union, ό.π. σελ. 30.

Πίνακας 14 Προτεινόμενα πιθανά μέτρα ελέγχου από την άτυπη ομάδα εργασίας RFID

Πηγή: Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID (2011), σελ. 19-22. Σημειώνεται ότι η ελληνική εκδοχή δεν είναι πλέον διαθέσιμη, ενώ ήταν μέχρι 16/10/2014. Βλ. την αγγλική εκδοχή σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf, σελ. 17-20.

Πρακτικές διοίκησης και διαχείρισης εφαρμογών RFID	1. Πρακτικές διαχείρισης από τον φορέα εκμετάλλευσης εφαρμογής RFID. 2. Πολιτικές καταστροφής και διαγραφής για δεδομένα RFID. 3. Πολιτικές που αναφέρονται στη σύννομη επεξεργασία πληροφοριών προσωπικού χαρακτήρα. 4. Κανονισμοί για ελαχιστοποίηση δεδομένων κατά την επεξεργασία δεδομένων RFID, εφόσον αυτό είναι εφικτό. 5. Επεξεργασία ή αποθήκευση πληροφοριών από ετικέτες που δεν ανήκουν στον φορέα εκμετάλλευσης RFID. 6. Πρακτικές διοίκησης και διαχείρισης ασφάλειας.
Μεμονωμένη πρόσβαση και έλεγχος	1. Παροχή πληροφοριών σχετικά με τους σκοπούς της επεξεργασίας και τις κατηγορίες των σχετικών δεδομένων προσωπικού χαρακτήρα. 2. Περιγραφή του τρόπου προβολής αντιρρήσεων στην επεξεργασία δεδομένων προσωπικού χαρακτήρα ή άρσης της συναίνεσης. 3. Προσδιορισμός της διαδικασίας απαίτησης επανόρθωσης ή διαγραφής ελλιπών ή ανακριβών δεδομένων προσωπικού χαρακτήρα.
Προστασία του συστήματος	1. Εάν υφίστανται έλεγχοι πρόσβασης που αναφέρονται στον τύπο των προσωπικών δεδομένων και τη λειτουργικότητα των συστημάτων. 2. Εάν υφίστανται έλεγχοι και πολιτικές ώστε να εξασφαλίζεται ότι ο φορέας εκμετάλλευσης δεν συνδέει δεδομένα προσωπικού χαρακτήρα στην εφαρμογή RFID κατά τρόπο ασυμβίβαστο με την έκθεση PIA. 3. Εάν υφίστανται κατάλληλα μέτρα για την προστασία του απορρήτου, της ακεραιότητας και της διάθεσης δεδομένων προσωπικού χαρακτήρα στα συστήματα και στην επικοινωνιακή υποδομή. 4. Πολιτικές για την αποθήκευση και καταστροφή των δεδομένων προσωπικού χαρακτήρα. 5. Ύπαρξη και υλοποίηση ελέγχων ασφάλειας όπως: -Μέτρα που αφορούν την ασφάλεια δικτύων και μεταφορών των δεδομένων RFID. -Μέτρα που διευκολύνουν τη διαθεσιμότητα των δεδομένων RFID μέσω αντιγράφων ασφαλείας και ανάκτησης.
Προστασία ετικετών RFID	1. Έλεγχοι πρόσβασης για λειτουργικότητα και πληροφορίες, συμπεριλαμβανομένης της επαλήθευσης ταυτότητας αναγνωστών, συντακτών, και των υποκείμενων διεργασιών, καθώς και εξουσιοδότηση επενέργειας στην ετικέτα RFID. 2. Μέθοδοι για την εξασφάλιση / τήρηση του απορρήτου των πληροφοριών (π.χ. μέσω κρυπτογράφησης της πλήρους ετικέτας RFID ή επιλεγμένων πεδίων της). 3. Μέθοδοι για τη διασφάλιση / τήρηση της ακεραιότητας των πληροφοριών. 4. Αποθήκευση των πληροφοριών μετά την αρχική συλλογή (π.χ. διάρκεια της αποθήκευσης, διαδικασίες για την καταστροφή των δεδομένων στο τέλος της περιόδου αποθήκευσης ή για τη διαγραφή των πληροφοριών στην ετικέτα RFID, διαδικασίες αποθήκευσης ή διαγραφής επιλεγμένων πεδίων). 5. Ανθεκτικότητα έναντι παραβιάσεων της ετικέτας RFID αυτής καθαυτής. 6. Απενεργοποίηση ή αφαίρεση, εφόσον απαιτηθεί ή εφόσον άλλως προβλέπεται.

Μέτρα λογοδοσίας	1. Εξασφαλίζεται η εύκαιρη διάθεση περιεκτικής πολιτικής πληροφοριών που περιλαμβάνει: - Την ταυτότητα και διεύθυνση του φορέα εκμετάλλευσης εφαρμογής RFID. - Τον σκοπό της εφαρμογής RFID. - Τους τύπους δεδομένων που επεξεργάζεται η εφαρμογή RFID, ιδίως εάν γίνεται επεξεργασία δεδομένων προσωπικού χαρακτήρα. - Εάν παρακολουθούνται οι θέσεις των ετικετών RFID όταν γίνεται επεξεργασία τους από άτομα. - Τις πιθανές επιπτώσεις στην προστασία της ιδιωτικότητας και των δεδομένων, εφόσον υπάρχουν, σχετικά με τη χρήση ετικετών RFID στην εφαρμογή RFID και με τα διαθέσιμα μέτρα για τον περιορισμό τους. 2. Εξασφάλιση συνοπτικών, ακριβών και εύληπτων ανακοινώσεων περί παρουσίας συσκευών ανάγνωσης RFID, όπου περιλαμβάνονται: -Υπόλογη(ες) νομικές οντότητες του φορέα εκμετάλλευσης RFID (ενδεχομένως μια ανά δικαιοδοσία, ή ανά περιοχή λειτουργίας). - Στοιχεία επαφής του ατόμου ή της υπηρεσίας στα οποία έχει ανατεθεί η ευθύνη αναθεώρησης των εκτιμήσεων και της συνεχούς καταλληλότητας των τεχνικών και οργανωτικών μέτρων που αφορούν την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας. - Ερευνητικές μέθοδοι (π.χ. μέθοδοι προσέγγισης του φορέα εκμετάλλευσης εφαρμογής RFID για τη διατύπωση ερωτήματος, αιτήματος, καταγγελίας ή για την άσκηση δικαιώματος). - Μέθοδοι προβολής αντιρρήσεων στην επεξεργασία, άσκησης των δικαιωμάτων πρόσβασης σε δεδομένα προσωπικού χαρακτήρα (συμπεριλαμβανομένης της απάλειψης και της διόρθωσης προσωπικών δεδομένων), ανάκλησης συναίνεσης ή για την αλλαγή ελέγχων ή άλλων επιλογών όσον αφορά την επεξεργασία προσωπικών δεδομένων. - Άλλες μέθοδοι έννομης προστασίας

5.4.2.3. Τεκμηρίωση αποτελεσμάτων ανάλυσης και εναπομείναντες κίνδυνοι

Σε αυτό το στάδιο πλέον έχουν εντοπιστεί οι πιθανοί κίνδυνοι και έχουν βρεθεί και οι έλεγχοι για τον περιορισμό τους. Το επόμενα βήμα για τους φορείς εκμετάλλευσης είναι να τεκμηριώσουν τα αποτελέσματα των παραπάνω διαδικασιών στην έκθεση του πλαισίου PIA, την οποία έχουν υποχρέωση να καταθέσουν στην αρμόδια αρχή. Εφόσον οι φορείς ολοκληρώσουν τα παραπάνω στάδια, οφείλουν στην τεκμηρίωση των αποτελεσμάτων να εξασφαλίσουν ότι οι εναπομείναντες κίνδυνοι, ύστερα από τον καλύτερο δυνατό περιορισμό τους, είναι πλέον χαμηλού κινδύνου και δεν αποτελούν κίνδυνο για την ιδιωτικότητα και επομένως η εφαρμογή τους καλύπτει όλες τις απαιτήσεις προς συμμόρφωση με τους νομικούς κανόνες για την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων.

Στην περίπτωση που σε μια εφαρμογή βρεθεί ότι οι εναπομείναντες κίνδυνοι ακόμη αποτελούν κίνδυνο για την ιδιωτικότητα, η υλοποίησή της δεν εγκρίνεται και πρέπει να εκτελέσει ξανά τη δεύτερη φάση εκτίμησης των κινδύνων και των επιπτώσεών τους στην ιδιωτικότητα.

5.4.3. Η έκθεση PIA

Ολοκληρώνοντας, η έκθεση PIA συμπεριλαμβάνει την αναλυτική περιγραφή της εφαρμογής RFID και την επαρκή και πλήρη τεκμηρίωση όλων των σταδίων της διαδικασίας του πλαισίου PIA. Η ολοκληρωμένη πλέον έκθεση PIA, παραδίδεται στον υπεύθυνο προστασίας της ιδιωτικότητας του οργανισμού και κοινοποιείται στην αρμόδια αρχή ελέγχου έξι εβδομάδες πριν την εγκατάσταση της εφαρμογής. Έτσι, εξασφαλίζεται ότι εάν προκύψουν αλλαγές θα εντοπιστούν και θα πραγματοποιηθούν πριν την εγκατάσταση του συστήματος ώστε να είναι εύκολο να ενσωματωθούν με το μικρότερο δυνατό κόστος.

Η Ευρωπαϊκή Επιτροπή με τη Σύσταση του 2009[242] για την εφαρμογή των αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων στις εφαρμογές που υποστηρίζονται από ραδιοσυχνική αναγνώριση, στην ενότητα εκτιμήσεις των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων στην παρ. 5(α), συνιστά ότι "*τα κράτη μέλη πρέπει να διασφαλίζουν ότι οι φορείς εκμετάλλευσης, εκπονούν εκθέσεις για την εκτίμηση των επιπτώσεων που έχει η εγκατάσταση της εφαρμογής στην προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής, συμπεριλαμβανομένης της πιθανής χρήσης της εφαρμογής για την παρακολούθηση ενός φυσικού προσώπου*". Επίσης, τονίζει ότι "*το επίπεδο λεπτομέρειας της εκτίμησης πρέπει να είναι το ενδεδειγμένο για τους κινδύνους αναφορικά με την προστασία της ιδιωτικής ζωής που ενδεχομένως*

[242] Βλ. Σύσταση της Επιτροπής της 12ης Μαΐου 2009 για την εφαρμογή αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων στις εφαρμογές που υποστηρίζονται από ραδιοσυχνική αναγνώριση [κοινοποιηθείσα υπό τον αριθμό Ε(2009) 3200] (2009/387/ΕΚ), Επίσημη Εφημερίδα της ΕΕ αριθ. L 122/47 της 16.5.2009, διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009H0387&from=EN

να συνδέονται με την εφαρμογή". Παράλληλα, στην παρ. 5(δ) συνιστά ότι πρέπει να "*θέτουν στη διάθεση της αρμόδιας αρχής την έκθεση αξιολόγησης τουλάχιστον έξι εβδομάδες πριν την εγκατάσταση της εφαρμογής*".

Κατά συνέπεια, όταν η ομάδα εργασίας RFID πρότεινε το πλαίσιο PIA, στη δεύτερη φάση της εκτίμησης των κινδύνων, συμπεριέλαβε αναλυτικά τις οδηγίες για τη σύνταξη μίας έκθεσης PIA.

5.5. Ολοκληρώνοντας το πλαίσιο PIA

Οι φορείς εκμετάλλευσης εφαρμογών RFID, εάν έχουν πάνω από μία εφαρμογή που χρησιμοποιεί την τεχνολογία RFID, οφείλουν να υλοποιούν το πλαίσιο PIA για κάθε εφαρμογή ξεχωριστά και να δημιουργούν διαφορετικές εκθέσεις PIA. Στην περίπτωση όμως που οι εφαρμογές αυτές είναι συναφείς, μπορούν να δημιουργήσουν μία έκθεση PIA αλλά να συμπεριλάβουν αναλυτικά και ρητά στην έκθεση PIA τις διαφορές των εφαρμογών. Ομοίως, και στην περίπτωση που επαναχρησιμοποιείται μία εφαρμογή RFID με τον ίδιο τρόπο αλλά σε περισσότερα προϊόντα, και πάλι μπορούν να δημιουργήσουν μία έκθεση PIA για όλα τα προϊόντα και όχι ξεχωριστά για κάθε προϊόν.

Ολοκληρώνοντας, αξίζει να αναφερθεί ότι η Ομάδα εργασίας του άρθρου 29, τον Απρίλιο του 2017, σε κείμενό της παρέθεσε ως παράδειγμα προς εφαρμογή για τον υπεύθυνο επεξεργασίας, το εν λόγω πλαίσιο PIA σε περίπτωση που χρειαστεί να κάνει εκτίμηση των επιπτώσεων ενός τεχνολογικού προϊόντος στην ιδιωτική ζωή. Συγκεκριμένα, επειδή το άρθρο 35[243] του Κανονισμού 2016/679, που επιβάλλει την εκτίμηση αντικτύπου, δεν ορίζει ποια διαδικασία οφείλει να ακολουθήσει ο υπεύθυνος επεξεργασίας, η Ομάδα εργασίας του άρθρου 29 εξέδωσε "Κατευθυντήριες γραμμές για την εκτίμηση του αντίκτυπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και

[243] Στο άρθρο 35 παρ.1 του Κανονισμού 2016/679 καθορίστηκε ότι "*όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα*".

καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του Κανονισμού 2016/679"[244] και μέσα στο κείμενό της θέτει ως παράδειγμα την εφαρμογή του πλαισίου PIA σε περίπτωση που ο σχεδιασμός επεξεργασίας ενέχει πολύ υψηλό κίνδυνο.

Μάλιστα, υπάρχουν και δωρεάν διαθέσιμα εργαλεία στο διαδίκτυο για να την διεξαγωγή της ΕΑΠΔ. Συγκεκριμένα, αρχικά δημιουργήθηκε ένα σχετικό εργαλείο από τον οργανισμό GS1[245], ένα διεθνή μη κερδοσκοπικό οργανισμό ο οποίος ασχολείται με το σχεδιασμό και την εφαρμογή διεθνών προτύπων, ως βοήθημα για τη συμμόρφωση με την απαίτηση στη σύσταση της Επιτροπής του 2009[246] εκτίμησης των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων σχετικά με τη χρήση της τεχνολογίας RFID στις διάφορες εφαρμογές. Το συγκεκριμένο εργαλείο είναι ευκόλως προσβάσιμο και απλό στη χρήση του καθώς το μόνο που χρειάζεται να έχει κάποιος είναι έναν υπολογιστή με εγκατεστημένο το excel και πρόσβαση στο διαδίκτυο. Και ένα άλλο αντίστοιχο εργαλείο το οποίο δημιουργήθηκε από τη γαλλική Αρχή Προστασίας Προσωπικών Δεδομένων[247] σε συμμόρφωση με το άρθρο 35 του ΓΚΠΔ, προκειμένου να βοηθήσει τους υπεύθυνους επεξεργασίας στη διεξαγωγή της ΕΑΠΔ. Το εργαλείο αυτό χρειάζεται εγκατάσταση σε ηλεκτρονικό υπολογιστή αλλά είναι εύκολο στη χρήση του καθώς είναι διαθέσιμο σε 14 γλώσσες, συμπεριλαμβανομένης και της ελληνικής.

[244] Βλ. "Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του Κανονισμού 2016/679", WP 248 αναθ. 01, σελ. 26, διαθέσιμο στο https://www.lawspot.gr/sites/default/files/images/nea/misc/wp29-dpia.pdf στα ελληνικά και στο http://ec.europa.eu/newsroom/document.cfm?doc_id=47711 στα αγγλικά

[245] Το εργαλείο είναι διαθέσιμο στο https://www.gs1.org/standards/epc-rfid/pia

[246] Σύσταση της Επιτροπής της 12ης Μαΐου 2009 για την εφαρμογή αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων στις εφαρμογές που υποστηρίζονται από ραδιοσυχνική αναγνώριση [κοινοποιηθείσα υπό τον αριθμό Ε(2009) 3200] (2009/387/ΕΚ), Επίσημη Εφημερίδα της ΕΕ αριθ. L 122/47 της 16.5.2009, διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009H0387&from=EN.

[247] Το εργαλείο είναι διαθέσιμο στο https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

6. Η προστασία των προσωπικών δεδομένων στην ελληνική έννομη τάξη

Σύμφωνα με την εισηγητική έκθεση στο σχέδιο νόμου “Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα”[248], στις τεχνολογικά προηγμένες κοινωνίες, όπως την ελληνική, οι γενικές διατάξεις περί προστασίας της προσωπικότητας πλέον δεν αρκούν αλλά επιβάλλονται ειδικές ρυθμίσεις οι οποίες ταυτόχρονα θα διασφαλίζουν τον φιλελεύθερο και δικαιοκρατικό χαρακτήρα της τεχνολογικής ανάπτυξης. Σε αυτό το κεφάλαιο παρουσιάζεται συνοπτικά το ελληνικό νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων.

Ο Έλληνας νομοθέτης το 1997 ακολουθώντας τις υποδείξεις της Οδηγίας 95/46/ΕΚ του άρθρου 32 παρ. 1, θέσπισε το νόμο 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και αργότερα το 2019 ακολουθώντας τις υποδείξεις του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679 (ΓΚΠΔ) θέσπισε το νόμο 4624/2019 (ΦΕΚ 137/Α/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» με τον οποίο καταργείται με επιφυλάξεις ο νόμος 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

[248] Η εισηγητική έκθεση στο σχέδιο νόμου "Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα" προς τη Βουλή των Ελλήνων είναι διαθέσιμη στο https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjs8bnQ8bLgAhWrwosKHecMDG8QFjAAegQIAhAC&url=https%3A%2F%2Fwww.hellenicparliament.gr%2FUserFiles%2F2f026f42-950c-4efc-b950-340c4fb76a24%2FNOM_NOM_EE_2472_UA23.DOC&usg=AOvVaw1PHmEzX_CO02xG0wRBCGNp . Επίσης βλ. σε Γιαννακούλα, Α., Μηλαπίδου, Μ., (επιμ.). (2017). Προσωπικά δεδομένα. (Σειρά: Ειδικοί Ποινικοί Νόμοι), , σελ. 163, Αθήνα : Νομική Βιβλιοθήκη.

6.1. Συνταγματική κατοχύρωση

Η προστασία των προσωπικών δεδομένων αποτελεί πρωταρχική υποχρέωση της πολιτείας και έχει συνταγματική κατοχύρωση, κυρίως στο άρθρο 9Α και στα άρθρα 2 παρ. 1 και 5 παρ. 1 του ελληνικού Συντάγματος[249]. Ειδικότερα, με το άρθρο 9Α[250] προστατεύει το δικαίωμα της πληροφορικής αυτοδιάθεσης, δηλαδή το δικαίωμα της προστασίας των προσωπικών δεδομένων από τη συλλογή, την επεξεργασία και τη χρήση τους, ιδίως με ηλεκτρονικά μέσα. Στο άρθρο 2 παρ. 1[251] επιβάλλει το σεβασμό της αξίας του ανθρώπου και την προστασία του και αποτελεί τη βάση για την κοινωνική συμβίωση και στο άρθρο 5 παρ. 1[252] κατοχυρώνεται το δικαίωμα της ελεύθερης ανάπτυξης της προσωπικότητας, της συμμετοχής στην οικονομική, κοινωνική και πολιτική ζωή της χώρας και το δικαίωμα της πληροφορικής αυτοδιάθεσης, εφόσον βέβαια δεν προσβάλλει τα δικαιώματα των άλλων και δεν παραβιάζει το Σύνταγμα.

Επίσης, αξίζει να αναφερθεί ότι στην εποχή του διαδικτύου όπου το δικαίωμα του καθενός να πληροφορεί και να πληροφορείται είναι απαραίτητο για τη διαμόρφωση και την έκφραση προσωπικής άποψης, το άρθρο 5Α[253] του Συντάγματος κατοχυρώνει το γενικό δικαίωμα στην ελεύθερη πληροφόρηση καθώς και το δικαίωμα συμμετοχής στην Κοινωνία της

[249] Το Σύνταγμα της Ελλάδος, όπως αναθεωρήθηκε με το ψήφισμα της 27ης Μαΐου 2008 της Η' Αναθεωρητικής Βουλής των Ελλήνων, είναι διαθέσιμο στο http://www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/

[250] Για περισσότερες πληροφορίες σχετικά με το άρθρο 9Α βλ. Σωτηρόπουλος, Β. (2006). Η συνταγματική προστασία των προσωπικών δεδομένων, ό.π. σελ.53 και Σαατζίδου-Παντελιάδου Ε. (2007). Νέοι κανόνες δικαίου στο πλαίσιο της Νέας Οικονομίας – Ηλεκτρονική επεξεργασία δεδομένων οικονομικής συμπεριφοράς, ό.π. σελ. 50.

[251] Για περισσότερες πληροφορίες βλ. Δαγτόγλου, Π. (2012). Συνταγματικό Δίκαιο, Ατομικά Δικαιώματα, Τέταρτη Ενημερωμένη Έκδοση, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, σελ. 1115-1123, Σωτηρόπουλος, Β. (2006). Η συνταγματική προστασία των προσωπικών δεδομένων, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, σελ. 42 και Σαατζίδου-Παντελιάδου, Ε. (2007). Νέοι κανόνες δικαίου στο πλαίσιο της Νέας Οικονομίας – Ηλεκτρονική επεξεργασία δεδομένων οικονομικής συμπεριφοράς, Θεσσαλονίκη, σελ. 42.

[252] Για περισσότερες πληροφορίες σχετικά με το άρθρο 5§1 βλ. Δαγτόγλου, Π. (2012). Συνταγματικό Δίκαιο, Ατομικά Δικαιώματα, ό.π., σελ. 1124-1132, Σωτηρόπουλος, Β. (2006). Η συνταγματική προστασία των προσωπικών δεδομένων, ό.π. σελ.44. Επίσης βλ. Σαατζίδου-Παντελιάδου, Ε. (2007). Νέοι κανόνες δικαίου στο πλαίσιο της Νέας Οικονομίας – Ηλεκτρονική επεξεργασία δεδομένων οικονομικής συμπεριφοράς, Θεσσαλονίκη, σελ. 45.

[253] Για περισσότερες πληροφορίες σχετικά με το άρθρο 5Α βλ. Αλεξανδροπούλου–Αιγυπτιάδου, Ε. (2016). Προσωπικά δεδομένα, εκδ. Νομική Βιβλιοθήκη, σελ. 35 και ιδίως σημ. 16 και Σαατζίδου-Παντελιάδου Ε. (2007). Νέοι κανόνες δικαίου στο πλαίσιο της Νέας Οικονομίας – Ηλεκτρονική επεξεργασία δεδομένων οικονομικής συμπεριφοράς, ό.π. σελ. 47.

Πληροφορίας, όπου οι προσωπικές πληροφορίες πλέον είναι βασικές προκειμένου να ληφθούν αποφάσεις σχεδόν σε όλους τους τομείς της ανθρώπινης δραστηριότητας. Το δικαίωμα αυτό φαίνεται να συγκρούεται με το δικαίωμα 9Α του Συντάγματος.

Τέλος, με το άρθρο 25[254], το οποίο συνδέεται άμεσα με το άρθρο 9Α, επαναδιατυπώνεται η υποχρέωση του κράτους για τη λήψη θετικών μέτρων που να εξασφαλίζουν την ανεμπόδιστη άσκηση των δικαιωμάτων. Επίσης, η εξασφάλιση του δικαιώματος του ατόμου στα προσωπικά του δεδομένα, οδήγησε στη συνταγματική κατοχύρωση ανεξάρτητης διοικητικής αρχής με το άρθρο 101Α.

6.2. Ο προϊσχύων νόμος 2472/1997

Ο Έλληνας νομοθέτης ακλουθώντας τις υποδείξεις της Οδηγίας 95/46/ΕΚ του άρθρου 32 παρ. 1, θέσπισε το νόμο 2472/1997[255] για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ο οποίος εποπτεύεται από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Αντικείμενο του ν. 2472/1997, όπως αναφέρεται στο άρθρο 1, είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Με το νόμο αυτό λοιπόν ο οποίος εφαρμόζεται και "*υπερισχύει ως ειδικότερος (lex specialis) στα ζητήματα επεξεργασίας προσωπικών δεδομένων*"[256], εισάγεται στην ελληνική έννομη τάξη ένα γενικό σύστημα προστασίας των προσωπικών

[254] Για περισσότερες πληροφορίες σχετικά με το άρθρο 25 βλ. Σαατζίδου-Παντελιάδου Ε (2007). Νέοι κανόνες δικαίου στο πλαίσιο της Νέας Οικονομίας – Ηλεκτρονική επεξεργασία δεδομένων οικονομικής συμπεριφοράς, ό.π. σελ. 60-63.

[255] Ο ν. 2472/1997 είναι διαθέσιμος στην ιστοσελίδα της Αρχής Προστασίας Προσωπικών δεδομένων http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL. Επίσης, παρουσίαση του νόμου με όλες τις τροποποιήσεις που έχει υποστεί (ν. 3471/2006 και ν. 3917/2011) και με πίνακα βιβλιογραφίας και νομολογίας για κάθε άρθρο βλ. Γιαννακούλα, Α., Μηλαπίδου, Μ., (επιμ.). (2017). Προσωπικά δεδομένα. (Σειρά: Ειδικοί Ποινικοί Νόμοι), σελ: 3-111.

[256] Βλ. Ιγγλεζάκης, Ι. (2006). Προστασία προσωπικών δεδομένων στο σύστημα πληροφοριών ''Τειρεσίας'', εκδ. Σάκκουλα Αθήνα-Θεσσαλονίκη, σελ. 32, με παραπέρα παραπομπές στην υποσημ. 52.

δεδομένων και προστατεύονται τα δικαιώματα και οι θεμελιώδεις ελευθερίες των ατόμων κυρίως της ιδιωτικής ζωής.

Προσωπικά δεδομένα, όπως ορίζονται στο άρθρο 2 του νόμου, νοείται "*κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων*". Επίσης, ο νόμος στο ίδιο άρθρο διακρίνει τα ευαίσθητα δεδομένα[257], δηλαδή αυτά που "*αφορούν τη φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση, την υγεία[258], την κοινωνική πρόνοια και την ερωτική ζωή, τα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και τη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων*". Και εννοείται πως όλα τα υπόλοιπα δεδομένα, όπως για παράδειγμα το όνομα, το επώνυμο, η κατοικία, το επάγγελμα, η οικογενειακή και η περιουσιακή κατάσταση, οι καταναλωτικές συνήθειες, ο μισθός, οι τραπεζικοί λογαριασμοί, η IP διεύθυνση[259] κ.ά., είναι απλά δεδομένα[260]. Τέλος, αξίζει να τονισθεί πως σύμφωνα με το νόμο τα

[257] Σχετικά με τη ρύθμιση της επεξεργασίας των ευαίσθητων δεδομένων βλ. Ιγγλεζάκης, Ι. (2003). Ευαίσθητα Προσωπικά Δεδομένα. Η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και οι συνέπειές της, εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη, ISBN 960-301-736-1, ISBN-13 978-960-301-736-3

[258] Σχετικά με τα προσωπικά δεδομένα υγείας βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2019). Διασυνοριακή ροή δεδομένων υγείας, Βιοηθικοί προβληματισμοί IV: Δεδομένα υγείας και γενετικά δεδομένα, Εκδ. Παπαζήση, Κίτσος, Π., Γιαννουκάκου, Αικ., Αλεξανδροπούλου, Ε. (2014). Η ηλεκτρονική υγεία την εποχή των Big και Open Data (ενόψει και των ρυθμίσεων της Πρότασης Κανονισμού της ΕΕ για την προστασία των προσωπικών δεδομένων), ΔiΜΕΕ 11/2014, σελ: 2-12, Kitsos, P., Yiannoukakou, Aik., Nikita, M., Milossi, M. (2013). Big and Open Data Privacy Risks in Health Sector. Developing a Trend or Establishing the Future?, 5th Conference on E-Democracy, Security, Privacy and Trust in a Digital World, Athens, December 2013, Millosi, M. (2012). Privacy protection in e-Health environment, in Bottis,M., (edit.). Privacy and Surveillance-current aspects and future perspectives, Proceedings of the Liss-Cost seminar in Athens, Greece "Surveillance in Academia", 2012 plus selected papers from ICIL 2011 and 2012 in Corfu, Greece, ed. Nomiki Bibliothiki Group, pp. 164-186, Κανελλοπούλου-Μπότη Μ. (2010). Η προστασία του απορρήτου και των προσωπικών δεδομένων σε ηλεκτρονικά ιατρικά αρχεία, σε Λαμπρινουδάκη, Κ.-Μήτρου, Λ.-Γκρίτζαλη, Σ.-Κάτσικα,Σ., Προστασία της ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, εκδ. Παπασωτηρίου, Αθήνα, σελ: 567.

[259] Βλ. Γνωμοδότηση 2/2002 σχετικά με τη χρήση μοναδικών αναγνωριστικών στον τηλεπικοινωνιακό τερματικό εξοπλισμό: το παράδειγμα του IPv6, διαθέσιμη στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp58_el.pdf και Αλεξανδροπούλου-Αιγυπτιάδου Ε. (2016). Προσωπικά Δεδομένα, ό.π., σελ: 46, ιδίως υποσημείωση 54.

[260] Περισσότερες πληροφορίες σχετικά με την έννοια των προσωπικών δεδομένων βλ. Αλεξανδροπούλου Ε. (2007), Προσωπικά Δεδομένα: Η νομική ρύθμιση της ηλεκτρονικής επεξεργασίας τους, ό.π. σελ: 33-37 και Αλεξανδροπούλου-Αιγυπτιάδου Ε. (2016). Προσωπικά Δεδομένα, ό.π., σελ: 43-52.

δεδομένα οικονομικής συμπεριφοράς[261] δε συμπεριλαμβάνονται στα ευαίσθητα προσωπικά δεδομένα.

6.3. Ο πρόσφατος νόμος 4624/2019

Ο Έλληνας νομοθέτης λαμβάνοντας υπόψη τις υποδείξεις του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679 (ΓΚΠΔ), θέσπισε το νόμο 4624/2019[262] με τον οποίο καταργείται με επιφυλάξεις ο νόμος 2472/1997 (βλ. άρθρο 84 του ν. 4624/2019).

Ο σκοπός του νέου αυτού νόμου, όπως αναφέρεται στο άρθρο 1, είναι τριπλός και αφορά πρώτον την αντικατάσταση του νομοθετικού πλαισίου που ρυθμίζει τη συγκρότηση και λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, δεύτερον τη λήψη μέτρων 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 των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ (ΓΚΠΔ) και τρίτον την ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης - πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου.

---

[261] Σχετικά με τα δεδομένα οικονομικής συμπεριφοράς βλ. Αλεξανδροπούλου-Αιγυπτιάδου,Ε. (2016). Επεξεργασία προσωπικών δεδομένων στον τραπεζικό χώρο με έμφαση στην Τειρεσίας Α.Ε., Πρακτικά 7ου Συνεδρίου ΕΕΝ e-Θέμις, Πιστωτικά Ιδρύματα: Νομικές & Θεσμικές Όψεις, Θεσσαλονίκη, εκδ. Νομική Βιβλιοθήκη, Αθήνα 2018, σελ. 35-52, Μυλώση, Μ., Αλεξανδροπούλου, Ε. (2015). Προσωπικά δεδομένα οικονομικής συμπεριφοράς και ηλεκτρονική επεξεργασία τους από την ΤΕΙΡΕΣΙΑΣ ΑΕ, ΔΙΜΕΕ 1/2015, σελ. 25-37, Μυλώση, Μ. (2014). Η έννομη προστασία των δεδομένων οικονομικής συμπεριφοράς από την αθέμιτη ηλεκτρονική επεξεργασία τους-Συγκριτική μελέτη της νομικής ρύθμισης σε Ελλάδα και Γαλλία, Διδακτορική Διατριβή, Πανεπιστήμιο Μακεδονίας, Θεσσαλονίκη.

[262] Ο ν. 4624/2019 τέθηκε σε εφαρμογή στις 29/08/2019 και είναι διαθέσιμος στην ιστοσελίδα της Αρχής Προστασίας Προσωπικών δεδομένων https://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=66,121,83,229,125,127,247,242

Ο νόμος χωρίζεται σε 4 κεφάλαια. Το Κεφάλαιο Α΄(άρθρα 1-8) στο οποίο οριοθετείται ο σκοπός και το πεδίο εφαρμογής του νόμου, εισάγεται ο ορισμός του δημοσίου και ιδιωτικού φορέα και προσδιορίζονται ρυθμίσεις για τον ορισμό Υπευθύνου Προστασίας Δεδομένων σε δημόσιους φορείς. Το Κεφάλαιο Β΄ (άρθρα 9-20) στο οποίο καθορίζεται ότι η εποπτεία της εφαρμογής των διατάξεων του ΓΚΠΔ, του νόμου και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στην Ελληνική Επικράτεια ασκείται από την Αρχή[263] που έχει συσταθεί με το ν. 2472/1997[264]. Το Κεφάλαιο Γ΄ (άρθρα 21-42) στο οποίο περιλαμβάνονται τα συμπληρωματικά μέτρα εφαρμογής του ΓΚΠΔ για την επεξεργασία δεδομένων προσωπικού χαρακτήρα εκ των οποίων τα σημαντικότερα είναι οι ρυθμίσεις για το έγκυρο της συγκατάθεσης των ανηλίκων, για την επεξεργασία ειδικών κατηγοριών δεδομένων, για την απαγόρευση της επεξεργασίας γενετικών δεδομένων για σκοπούς ασφάλισης υγείας και ζωής, για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπό διαφορετικό από αυτόν για τον οποίο έχουν συλλεχθεί, για την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο χώρο των εργασιακών σχέσεων, για την επεξεργασία και ελευθερία έκφρασης και πληροφόρησης, για τη διαπίστευση των φορέων που χορηγούν πιστοποιήσεις καθώς και η πρόβλεψη συστήματος ποινικών και διοικητικών κυρώσεων. Και τέλος το Κεφάλαιο Δ΄ (άρθρα 43-82) στο οποίο ενσωματώνεται στην εθνική νομοθεσία η Οδηγία 2016/680.

[263] Σεχτικά με την Αρχή, βλ. Μήτρου Λ., Η Αρχή Προστασίας Προσωπικών δεδομένων, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή 1999, επίσης βλ. Σωτηρόπουλος, Β. (2006). Η συνταγματική προστασία των προσωπικών δεδομένων, ό.π. σελ. 129-137

[264] Βλ. άρθρο 15 του ν. 2472/1997

IV. ΜΕΡΟΣ ΤΡΙΤΟ

Εφαρμογές της τεχνολογίας RFID. Συγκριτική επισκόπηση νομοθετικών πρωτοβουλιών σε ΕΕ και ΗΠΑ.

Σε αυτό το μέρος της διατριβής παρουσιάζεται περιπτωσιολογία εφαρμογών της τεχνολογίας RFID. Συγκεκριμένα, παρουσιάζονται νομοσχέδια, νόμοι και γνώμες που έχουν δημοσιευτεί κατά περιόδους στην Ευρωπαϊκή Ένωση και στις Ηνωμένες Πολιτείες της Αμερικής σχετικά με τρεις χαρακτηριστικούς τομείς εφαρμογής της τεχνολογίας RFID που αφορούν α) την εμφύτευση RFID ετικέτας στο ανθρώπινο σώμα, β) τη χρήση της τεχνολογίας RFID στα ηλεκτρονικά διαβατήρια και γ) τη χρήση της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου. Για κάθε μία από τις τρεις παραπάνω περιπτώσεις, στο τέλος κάθε κεφαλαίου παρατίθενται τα συμπεράσματα που έχουν προκύψει.

1. Εμφύτευση RFID ετικέτας στο ανθρώπινο σώμα

Η εμφύτευση RFID ετικέτας στο ανθρώπινο σώμα εφαρμόστηκε για πρώτη φορά το 1998 κατά την εκτέλεση του ερευνητικού έργου “Cyborg 1.0”[265]. Συγκεκριμένα, ο καθηγητής Kevin Warwick του τμήματος Cybernetic στο πανεπιστήμιο Reading (στο Ηνωμένο Βασίλειο) δέχτηκε να εμφυτευτεί στον πήχη του χεριού του μία ετικέτα RFID. Με αυτό τον τρόπο παρακολουθούνταν οι κινήσεις του καθηγητή μέσα στο τμήμα, ενώ ο ίδιος μπορούσε να διαχειριστεί πόρτες, φώτα και άλλους υπολογιστές πολύ εύκολα χωρίς να κουνήσει το χέρι του.

[265] Βλ. Friggieri, A., Michael, K. & Michael, M. G. (2009). The legal ramifications of microchipping people in the United States of America- a state legislative comparison. IEEE International Symposium on Technology and Society (pp. 1-8). Los Alamitos, USA: IEEE, σελ. 1. Επίσης, για περισσότερες πληροφορίες σχετικά με το ερευνητικό έργο βλ. http://www.kevinwarwick.com/project-cyborg-1-0/ και το βιβλίο Warwick K., I, Cyborg. UK: Century, 2002.

Μετέπειτα, το 2004 στο Μεξικό εμφυτεύτηκαν RFID ετικέτες (VeriChip[266]), κόστους 150 δολάρια η μία, στον Γενικό Εισαγγελέα Rafael Macedo de la Concha και στους 160 υπαλλήλους της Εισαγγελίας[267]. Σκοπός της συγκεκριμένης εφαρμογής ήταν η ελεγχόμενη πρόσβαση σε χώρους ασφαλείας για να γνωρίζουν ανά πάσα στιγμή ποιος είχε πρόσβαση σε ευαίσθητα δεδομένα, προκειμένου να αντιμετωπίσουν προβλήματα διαφθοράς που είχαν παρατηρηθεί από τους ιδίους.

Επίσης, από το 2004 έως το 2008, εφαρμόστηκε η εμφύτευση RFID ετικέτας στο ανθρώπινο σώμα και σε ένα από τα πιο διάσημα club στη Βαρκελώνη, το Baja Beach Club. Συγκεκριμένα, εμφυτεύανε RFID ετικέτα (VeriChip, κόστους 100 δολάρια το ένα) σε όσους VIP πελάτες τους το επιθυμούσαν για να τους διευκολύνουν στις κινήσεις τους μέσα στο club. Δηλαδή, για να έχουν ανά πάσα στιγμή πρόσβαση στους χώρους του club και να εκτελούν πληρωμές ηλεκτρονικά και αυτόματα, μειώνοντας έτσι και τον κίνδυνο να είναι θύματα κλοπής[268]. Αξίζει να σημειωθεί ότι στη συγκεκριμένη περίπτωση το εμφύτευμα RFID πρόσδιδε κοινωνικό κύρος στα υποκείμενα[269]. Όταν εισέρχονταν στο club και σκαναριζόταν η ετικέτα RFID, ακουγόταν σε όλο το club ένας χαρακτηριστικός ήχος (μπιπ) και το όνομά τους εμφανιζόταν σε μία μεγάλη οθόνη. Επομένως, οι υπόλοιποι πελάτες του club καταλάβαιναν πως το συγκεκριμένο άτομο είναι κάποιος VIP και αντιδρούσαν με θαυμασμό.

Σε αυτό το κεφάλαιο εξετάζεται η σχετική νομοθεσία και οι σχετικές πρωτοβουλίες αναφορικά με την εμφύτευση RFID ετικετών στο ανθρώπινο σώμα στην Ευρωπαϊκή Ένωση και στις Ηνωμένες Πολιτείες της Αμερικής.

---

[266] Το VeriChip είναι μία ετικέτα RFID τύπου γυάλινος σωλήνας (βλ. Μέρος πρώτο, υποκεφάλαιο 3.3.1.3), ο οποίος έχει το μέγεθος ενός κόκκου ρυζιού και τοποθετείται κάτω από το δέρμα.

[267] Βλ. The Associated Press "Microchips implanted in Mexican officials. Attorney general, prosecutors carry security pass under their skin", July 2004, διαθέσιμο στο http://www.nbcnews.com/id/5439055/ns/technology_and_science-tech_and_gadgets/t/microchips-implanted-mexican-officials/#.WrHn1ee-nIU

[268] Βλ. Michael, K., Michael, M. G. (2010, June). The diffusion of RFID implants for access control and epayments: A case study on Baja Beach Club in Barcelona. In Technology and Society (ISTAS). In IEEE International Symposium on Technology and Society, σελ. 245.

[269] Βλ. Michael, K., Michael, M. G. (2010, June). The diffusion of RFID implants.., ό.π..

1.1. Ευρωπαϊκή Ένωση

Μέχρι σήμερα δεν έχει υπάρξει στην Ευρωπαϊκή Ένωση νομοθεσία σχετική με την εμφύτευση RFID ετικέτας στο ανθρώπινο σώμα. Το μόνο κείμενο σε ισχύ που θα μπορούσε να θεωρηθεί ως ένα σημείο σχετικό, είναι η Οδηγία του Συμβουλίου[270] για την προσέγγιση των νομοθεσιών των κρατών μελών σχετικά με τα ενεργά εμφυτεύσιμα ιατρικά βοηθήματα το 1990. Βέβαια είναι αυτονόητο ότι η τεχνολογία RFID δεν εμπίπτει στο σκοπό της παραπάνω Οδηγίας, παρά μόνο όσον αφορά τις βασικές απαιτήσεις ασφάλειας για την εμφύτευση όπως ορίζονται στο παράρτημα Ι της Οδηγίας. Επομένως, στον ευρωπαϊκό χώρο τα ζητήματα ιδιωτικότητας που προκύπτουν από την εμφύτευση RFID ετικέτας στο ανθρώπινο σώμα εμπίπτουν στο πεδίο του νόμου περί προστασίας προσωπικών δεδομένων (ΓΚΠΔ).

Τον Ιανουάριο του 2018 έγινε μία μελέτη[271] για την Επιτροπή του Ευρωπαϊκού Κοινοβουλίου Απασχόλησης και Κοινωνικών Υποθέσεων (Employment and Social Affairs Committee) σχετικά με την εμφύτευση RFID ετικέτας σε εργαζομένους. Σε αυτήν, αναφέρεται ότι οι εμφυτευμένες RFID ετικέτες σε ανθρώπους σε οποιαδήποτε εφαρμογή, έχουν υπολογιστεί από 2.000 έως 10.000 παγκοσμίως, χωρίς όμως να έχει γίνει κάποια συστηματική καταγραφή αυτών. Ενώ μάλιστα στις περισσότερες περιπτώσεις λέγεται ότι γίνεται με τη συγκατάθεση του υποκειμένου, δεν μπορεί να είναι σίγουρο εάν υπήρξαν πιέσεις για να δεχτούν ή ευνοϊκότερες συνθήκες υπέρ αυτών που θα δεχόντουσαν την εμφύτευση. Πολλές φορές η ανάγκη των ανθρώπων για την εύρεση εργασίας για παράδειγμα, μπορεί να υπερισχύσει τυχόν ενδοιασμών που μπορεί να έχουν προκειμένου να δεχθούν έναν τέτοιο όρο στη σύμβασή

[270] Οδηγία του Συμβουλίου της 20ης Ιουνίου 1990 για την προσέγγιση των νομοθεσιών των κρατών μελών σχετικά με τα ενεργά εμφυτεύσιμα ιατρικά βοηθήματα (90/385/ΕΟΚ), Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, Αριθ. L 189/17, διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31990L0385 και η τροποποίησή της με την Οδηγία 2007/47/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 5ης Σεπτεμβρίου 2007 για την τροποποίηση της Οδηγίας 90/385/ΕΟΚ του Συμβουλίου για την προσέγγιση των νομοθεσιών των κρατών μελών σχετικά με τα ενεργά εμφυτεύσιμα ιατρικά βοηθήματα, της Οδηγίας 93/42/ΕΟΚ του Συμβουλίου για τα ιατροτεχνολογικά προϊόντα και της Οδηγίας 98/8/ΕΚ για τη διάθεση βιοκτόνων στην αγορά, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης L 247/2, διαθέσιμη στο http://eur-lex.europa.eu/legal-content/GA/ALL/?uri=CELEX:32007L0047.

[271] Graveling R., Winski Th., Dixon K. (2018). The use of chip implants for workers, ό.π..

τους. Επομένως είναι αναγκαίο να εξασφαλιστεί η προστασία των υποκειμένων από τέτοια ενδεχόμενα[272].

Στην ίδια μελέτη τονίζεται ότι εφόσον η εμφύτευση RFID ετικέτας σε ανθρώπους, είτε είναι εργαζόμενοι, είτε πρόκειται για κάποια άλλη εφαρμογή, έχει άμεση σχέση με τη συλλογή, την αποθήκευση και την επεξεργασία δεδομένων προσωπικού χαρακτήρα, τότε εμπίπτει στο πεδίο του νόμου περί προστασίας προσωπικών δεομένων. Ειδικότερα, επισημαίνεται ότι ο νέος Κανονισμός 2016/679 (ΓΚΠΔ) δίνει ιδιαίτερη βαρύτητα στη λήψη συγκατάθεσης και συγκεκριμένα στο άρθρο 7 παρ. 1 του νόμου περί προϋποθέσεων συγκατάθεσης, ορίζει ότι ο υπεύθυνος επεξεργασίας πρέπει να "*είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε για την επεξεργασία των δεδομένων του προσωπικού χαρακτήρα*". Μάλιστα, η παραπάνω μελέτη αναφέρει αναλυτικά ότι οι προϋποθέσεις που πρέπει να καλύπτονται από τον υπεύθυνο επεξεργασίας σε τέτοιες περιπτώσεις σύμφωνα με τον Κανονισμό 2016/679 (ΓΚΠΔ) είναι[273]:

I. η συγκατάθεση πρέπει να είναι συγκεκριμένη και πριν την παροχή της συγκατάθεσης το υποκείμενο των δεδομένων να ενημερώνεται σχετικά με το δικαίωμα ανάκλησης της συγκατάθεσής του ανά πάσα στιγμή (άρθρο 7, παρ. 3)
II. η συγκατάθεση πρέπει να δίνεται ελεύθερα από το υποκείμενο, με βούληση και εν πλήρει επιγνώσει (άρθρο 4 (11)),
III. η συγκατάθεση πρέπει να είναι σαφής και το υποκείμενο των δεδομένων να εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια (άρθρο 4 (11)). Επί παραδείγματι, με τη συμπλήρωση ενός τετραγωνιδίου κατά την επίσκεψη σε διαδικτυακή ιστοσελίδα, την επιλογή των επιθυμητών τεχνικών ρυθμίσεων για υπηρεσίες της κοινωνίας των πληροφοριών ή μια δήλωση ή συμπεριφορά που δηλώνει σαφώς, στο συγκεκριμένο πλαίσιο, ότι το υποκείμενο των

[272] Βλ. Glasser, D. J., Goodman, K. W., Einspruch, N. G. (2007). Chips, tags and scanners: Ethical challenges for radio frequency identification. Ethics and Information Technology, Vol. 9(2), pp. 101-109 και Graveling R., Winski Th., Dixon K. (2018). The use of chip implants for workers, ό.π. σελ. 28.
[273] Βλ. Graveling R., Winski Th., Dixon K. (2018). The use of chip implants for workers, ό.π. σελ. 20 και υποσημείωση 19.

δεδομένων αποδέχεται την πρόταση επεξεργασίας των οικείων δεδομένων προσωπικού χαρακτήρα (αιτιολογική σκέψη 31),

IV. για την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, το υποκείμενο των δεδομένων πρέπει να παράσχει ρητή συγκατάθεση (άρθρο 9)[274],

V. εάν η συγκατάθεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα (άρθρο 7, παρ. 2):

    I. το αίτημα για συγκατάθεση πρέπει να υποβάλλεται κατά τρόπο ώστε να είναι σαφώς διακριτό από τα άλλα θέματα,

    II. σε κατανοητή και εύκολα προσβάσιμη μορφή και

    III. χρησιμοποιώντας σαφή και απλή διατύπωση

Ακόμη και στην περίπτωση που ένας άνθρωπος, για παράδειγμα στον εργασιακό χώρο, δεχθεί εθελοντικά να του εμφυτεύσουνε μία RFID ετικέτα, ο υπεύθυνος επεξεργασίας, που στην συγκεκριμένη περίπτωση θα είναι ο εργοδότης του, οφείλει να συμμορφωθεί με καθεμία από τις παραπάνω προϋποθέσεις.

Πέραν όμως από τη συλλογή των προσωπικών δεδομένων μετά την εμφύτευση της RFID ετικέτας σε ένα υποκείμενο, σημαντικό είναι να καθοριστεί τί θα ισχύει και όταν αφαιρεθεί το εμφύτευμα από το υποκείμενο. Σε ποιον θα ανήκει η ετικέτα, σε ποιον θα ανήκουν τα συλλεχθέντα δεδομένα και ποια θα είναι η επιτρεπόμενη χρονική διάρκεια τήρησης των δεδομένων, διασφαλίζοντας έτσι τη μείωση του κινδύνου προσβολής της προσωπικότητας του υποκειμένου[275].

[274] Στην περίπτωση όπου δεν είναι δυνατόν να προσδιορίζεται πλήρως ο σκοπός της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας κατά τον χρόνο συλλογής των δεδομένων, τα υποκείμενα των δεδομένων θα πρέπει να μπορούν να δώσουν τη συγκατάθεσή τους για ορισμένους τομείς της επιστημονικής έρευνας (Κανονισμός 2016/679 (ΓΚΠΔ), αιτιολογική σκέψη (33)).

[275] Σχετικά με την ιδιοκτησία των δεδομένων μετά την αφαίρεση της RFID ετικέτας στον εργασιακό χώρο βλ. Graveling R., Winski Th., Dixon K. (2018). The use of chip implants for workers, ό.π. σελ. 24.

1.2. Ηνωμένες Πολιτείες της Αμερικής

Σε αντίθεση με την Ευρωπαϊκή Ένωση, στις Ηνωμένες Πολιτείες της Αμερικής, ναι μεν δεν υπάρχει νομοθετική πρωτοβουλία σε ομοσπονδιακό επίπεδο, αλλά έχουν υπάρξει νομοσχέδια και έχουν υιοθετηθεί νόμοι σε πολιτειακό επίπεδο σχετικά με την εμφύτευση RFID ετικέτας, ή μικροτσίπ, στον άνθρωπο. Μελετώντας νομοσχέδια από το 2006 έως και το 2017, παρατηρείται ότι ολοένα και περισσότερες πολιτείες ευαισθητοποιούνται και δραστηριοποιούνται επί του θέματος.

Στον παρακάτω πίνακα καταγράφονται οι 12 πολιτείες της Αμερικής στις οποίες έχουν γίνει νομικές προσπάθειες για την απαγόρευση της εμφύτευσης RFID ετικέτας σε άνθρωπο.

Πίνακας 15 Νομοσχέδια και νόμοι σχετικά με την απαγόρευση εμφύτευσης RFID στις Ηνωμένες Πολιτείες της Αμερικής

α/α	Πολιτεία	Έτος	Νομοσχέδιο	Νόμος
1	Ουισκόνσιν	2006	AB 290 , Act 482	Wis. Stats. §146.25
2	Καλιφόρνια	2007	SB 362	Civil Code § 52.7
3	Κολοράντο	2007	HB 07-1082	-
4	Φλόριντα	2007	SB 2220	-
5	Βόρεια Ντακότα	2007 / 2007	SB 2415	Cent. Code §12.1-15-06
6	Οκλαχόμα	2008 / 2014	SB 47	Stat. §63-1-1430
7	Βιρτζίνια	2009	HB 53	-
8	Τζόρτζια	2008 / 2009	HB 38, SB 235	-
9	Γιούτα	2011	H.B. 224	Utah Code 77-23a-4.5
10	Νεβάδα	2017	SB 109	-
11	Οχάιο	2006	SB 349 (για την προστασία των εργαζομένων)	-
12	Μιζούρι	2008	H.B. 2041	Rev. Stat. Section 285.035.1 (για την προστασία των εργαζομένων)

Στο Ουισκόνσιν, με το νομοσχέδιο AB 290[276] που προτάθηκε το 2006, προστέθηκε στη νομοθεσία το τμήμα 146.25[277] με το οποίο απαγορεύτηκε η υποχρεωτική εμφύτευση μικροτσίπ στον άνθρωπο. Επίσης ορίστηκε ότι οι

[276] AB 209, Relating to: prohibiting the required implanting of a microchip in an individual and providing a penalty, διαθέσιμο στο http://docs.legis.wisconsin.gov/2005/proposals/ab290

[277] Wis. Stats. §146.25, Required implanting of microchip prohibited, διαθέσιμο στο https://docs.legis.wisconsin.gov/statutes/statutes/146/25

παραβάτες θα τιμωρούνται με πρόστιμο έως 10.000 δολάρια και για κάθε μέρα που συνεχίζεται η παράβαση θα θεωρείται ξεχωριστό αδίκημα.

Στην Καλιφόρνια, το 2007, με το νομοσχέδιο SB 362[278] προστέθηκε στον αστικό κώδικα η §52.7[279] στην οποία απαγορεύει την εμφύτευση οποιασδήποτε συσκευής ταυτοποίησης, με τρόπο υποχρεωτικό και σε περίπτωση παράβασης καθορίζει πρόστιμο έως και 10.000 δολάρια, καθώς και 1.000 δολάρια για κάθε μέρα που συνεχίζεται η παράβαση. Ως συσκευή ταυτοποίησης ορίζεται οποιαδήποτε συσκευή έχει τη δυνατότητα, είτε παθητικά, είτε ενεργητικά, να μεταβιβάζει προσωπικά δεδομένα (Civ. Code 52.7 (h)(1)). Ενώ περαιτέρω ορίζει ότι με τον όρο προσωπικά δεδομένα εννοούνται πληροφορίες οι οποίες μπορούν να χρησιμοποιηθούν είτε μεμονωμένα, είτε συνδυαστικά για την αναγνώριση ενός ατόμου, όπως οι παρακάτω (Civ.Code 52.7 (h)(3)):

1. Όνομα ή επίθετο
2. Διεύθυνση
3. Τηλέφωνο
4. E-mail, πρωτόκολλο διαδικτύου (IP) ή ιστοσελίδα.
5. Ημερομηνία γέννησης
6. Αριθμός διπλώματος οδήγησης ή ταυτότητας
7. Οποιοσδήποτε μοναδικός αριθμός αναγνώρισης που καταγράφεται στο δίπλωμα οδήγησης ή στην ταυτότητα που έχει εκδοθεί σύμφωνα με το Section 13000 του Κώδικα Οχημάτων (Vehicle Code)
8. Αριθμός λογαριασμού τραπέζης, χρεωστικής κάρτας ή άλλου χρηματοπιστωτικού ιδρύματος
9. Οποιαδήποτε μοναδικό προσωπικό αναγνωριστικό περιέχεται σε ασφάλεια υγείας
10. Θρησκεία
11. Ιθαγένεια

[278] SB 362, διαθέσιμο στο http://www.leginfo.ca.gov/pub/07-08/bill/sen/sb_0351-0400/sb_362_bill_20071012_chaptered.html

[279] Civil Code-CIV, DIVISION 1. PERSONS [38 - 86], PART 2. PERSONAL RIGHTS [43 - 53.7], 52.7, διαθέσιμο στο https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=52.7.

12. Φωτογραφία
13. Δακτυλικά αποτυπώματα ή άλλων βιομετρικά αναγνωριστικά
14. Αριθμός μητρώου κοινωνικής ασφάλισης
15. Οποιαδήποτε μοναδικά προσωπικά αναγνωριστικά

Επίσης, σημαντική είναι και η προσθήκη της §52.7(g) στην οποία αναφέρεται πως η εισαγωγή της §52.7 στον αστικό κώδικα δεν τροποποιεί την υπάρχουσα νομοθεσία σχετικά με τα δικαιώματα των γονέων και των κηδεμόνων ανηλίκων. Επομένως, αφήνει να εννοηθεί πως οι έχοντες την επιμέλεια ανηλίκων μπορούν να επιτρέψουν την εμφύτευση συσκευής ταυτοποίησης κάτω από ορισμένες προϋποθέσεις, όπως ορίζονται στον Κώδικα Οικογενειακού Δικαίου της Καλιφόρνια (§6922 και §6924, California Family Code)[280].

Στο Κολοράντο, το 2007, με το νομοσχέδιο HB 07-1082[281], προστίθεται ένα καινούριο τμήμα στη νομοθεσία με το οποίο απαγορεύεται η υποχρεωτική εμφύτευση μικροτσίπ γενικότερα, στον άνθρωπο. Επίσης καθορίζεται πως η παράβαση θεωρείται πλημμέλημα τρίτου βαθμού[282], όπου στην περίπτωση του Κολοράντο εννοείται ότι οι παραβάτες θα τιμωρούνται με χρηματική ποινή όχι κάτω από 50 δολάρια (ελάχιστη ποινή) ή φυλάκιση έως 6 μήνες και 750 δολάρια ή και τα δύο (μέγιστη ποινή).

Στη Φλόριντα, το 2007, με το νομοσχέδιο SB 2220[283], ορίστηκε ως κακούργημα τρίτου βαθμού[284], με ποινή φυλάκισης έως 5 έτη και χρηματική ποινή 5.000 δολάρια, η εμφύτευση μικροτσίπ ή οποιασδήποτε παρόμοιας

[280] Βλ. Friggieri, A., Michael, K., Michael, M. G. (2009). The legal ramifications of microchipping people in the United States of America- a state legislative comparison, In IEEE International Symposium on Technology and Society, σελ: 7.

[281] HB 07-1082, A bill for an Act concerning a prohibition on requiring an individual to be implanted with a microchip, διαθέσιμο στο http://www.leg.state.co.us/clics/clics2007a/csl.nsf/fsbillcont/CBC12C68118CE43787257251007B703D?Open&file=1082_01.pdf

[282] Ποινές για πλημμελήματα όπως ορίζονται στο Κολοράντο, βλ. https://www.colorado.gov/pacific/sites/default/files/14%20MISD%20INTRO.pdf

[283] SB 2202, an Act relating to implanted microchips; prohibiting the implanting of a microchip or similar monitoring device into a person without providing full disclosure regarding the device and obtaining the person's informed written consent; providing a penalty; providing an effective date, διαθέσιμο στο http://archive.flsenate.gov/data/session/2007/Senate/bills/billtext/pdf/s2220.pdf

[284] Ποινές για κακουργήματα όπως ορίζονται στη Φλόριντα, βλ. https://www.criminaldefenselawyer.com/resources/criminal-defense/state-felony-laws/florida-felony-class.htm

συσκευής παρακολούθησης σε άνθρωπο, χωρίς την ενημέρωση του υποκειμένου και τη λήψη γραπτής συγκατάθεσης.

Αξίζει να τονιστεί ότι στη Βόρεια Ντακότα, το 2007, με το νομοσχέδιο 2415[285] γίνεται αναφορά συγκεκριμένα στην τεχνολογία RFID. Ειδικότερα, προστέθηκε στη νομοθεσία η §12.1-15-06[286] σχετικά με την απαγόρευση εμφύτευσης μικροτσίπ που χρησιμοποιεί συγκεκριμένα την τεχνολογία RFID. Η παράβαση θεωρείται πλημμέλημα πρώτου βαθμού[287] και επομένως οι παραβάτες θα τιμωρούνται έως ένα έτος φυλάκισης ή/και 3.000 δολάρια χρηματική ποινή.

Ομοίως και στη Γιούτα λίγο αργότερα, το 2011, με το νομοσχέδιο HB 0224[288], προστέθηκε στη νομοθεσία η §77-23a-4.5[289] στην οποία ορίζονται κυρώσεις στην περίπτωση που η εμφύτευση συσκευής αναγνώρισης συγκεκριμένα με τη χρήση της τεχνολογίας RFID γίνεται με υποχρεωτικό τρόπο. Αναλυτικότερα, η παράβαση θεωρείται πλημμέλημα πρώτου βαθμού και οι παραβάτες θα τιμωρούνται με χρηματική ποινή έως 10.000 δολάρια και για κάθε μέρα που δεν αφαιρούν ή δεν απενεργοποιούν το εμφύτευμα με 1.000 δολάρια ανά ημέρα.

Στην Οκλαχόμα με το νομοσχέδιο SB 47[290] του 2008, προστέθηκε το 2013 στη νομοθεσία η §63-1-1430[291] με την οποία απαγορεύτηκε η υποχρεωτική εμφύτευση μικροτσίπ ή και οποιοδήποτε μόνιμο σημάδι στον

[285] SB 2415, an Act to create and enact a new section to chapter 12.1-15 of the North Dakota Century Code, relating to implanted microchips in individuals; and to provide a penalty, διαθέσιμο στο http://www.legis.nd.gov/assembly/60-2007/session-laws/documents/CRMLC.pdf#CHAPTER122

[286] Cent. Code §12.1-15-06, Implanting microchips prohibited, διαθέσιμο στο http://www.legis.nd.gov/cencode/t12-1c15.pdf?20131220122657

[287] Ποινές για πλημμελήματα όπως ορίζονται στη Βόρεια Ντακότα, βλ. Cent. Code §12.1-32-01, διαθέσιμο στο http://www.legis.nd.gov/cencode/t12-1c32.pdf

[288] H.B. 224 Radio Frequency Identification, διαθέσιμο στο https://le.utah.gov/~2011/bills/static/HB0224.html

[289] Utah Code, §77-23a-4.5, Implanting an electronic identification device – Penalties, διαθέσιμο στο https://le.utah.gov/xcode/Title77/Chapter23A/C77-23a-S4.5_1800010118000101.pdf

[290] SB 47, An Act relating to public health and safety; prohibiting the forced implantation of a microchip or other permanent mark; authorizing the State Department of Health to impose a fine in certain circumstances; providing for codification; and providing an effective date, διαθέσιμο στο http://webserver1.lsb.state.ok.us/2007-08bills/SB/SB47_ENR.RTF

[291] Oklahoma Statutes Title 63. Public health and safety, §63-1-1430, διαθέσιμο στο http://webserver1.lsb.state.ok.us/OK_Statutes/CompleteTitles/os63.rtf

άνθρωπο. Οι παραβάτες θα τιμωρούνται με πρόστιμο έως 10.000 δολάρια και για κάθε μέρα που συνεχίζεται η παράβαση θα θεωρείται ξεχωριστό αδίκημα.

Στη Βιρτζίνια, το 2009 με το νομοσχέδιο HB 53[292], ορίζεται ότι είναι παράνομο συγκεκριμένα ένας ασφαλιστικός φορέας (insurer) να θέτει ως όρο ασφάλισης, ή ένας εργοδότης να θέτει ως προϋπόθεση από τον εργαζόμενο για τη σύναψη σύμβασης εργασίας, να φέρει μία συσκευή αναγνώρισης/παρακολούθησης είτε εμφυτευμένη, είτε μόνιμα ή ημι-μόνιμα ενσωματωμένη στο σώμα, στο δέρμα, στα δόντια, στα μαλλιά ή στα νύχια του υποκειμένου για να υπόκειται σε παρακολούθηση ή η συσκευή να χρησιμοποιείται ως βοήθημα για παρακολούθηση. Οι παραβάτες και στις δύο παραπάνω περιπτώσεις θα υπόκεινται σε αστική ποινή (civil penalty) ύψους 500 δολαρίων.

Στη Τζόρτζια, το 2009 προτάθηκε το νομοσχέδιο SB 235[293], το οποίο είναι γνωστό ως “Microchip Consent Act of 2009”. Σε αυτό, πέραν από κάποιους ορισμούς που δόθηκαν για να προστεθούν στο νόμο (τι εννοείται με τον όρο εμφύτευση, μικροτσίπ, υποκείμενο και υποχρεώνω), ορίζεται ότι κανένας άνθρωπος δεν πρέπει να υποχρεούται να εμφυτευθεί μικροτσίπ στο σώμα του (SB 235, b), οι παραβάτες θα διώκονται για πλημμέλημα[294] (1.000 δολάρια χρηματική ποινή ή/και 1 έτος φυλάκιση) (SB 235, c), τα υποκείμενα που υπέστησαν υποχρεωτικά την εμφύτευση μπορούν να ασκήσουν αγωγή για αποζημίωση (SB 235, d) και η οικειοθελής εμφύτευση θα πρέπει να γίνεται μόνο από γιατρό και υπό την εποπτεία του Ιατρικού Συμβουλίου (Georgia Composite Medical Board) (SB 235, e).

Προσφάτως, το 2017, στη Νεβάδα προτάθηκε το νομοσχέδιο SB 109[295] με το οποίο απαγορεύτηκε η υποχρεωτική εμφύτευση μικροτσίπ ή και οποιοδήποτε μόνιμο σημάδι ταυτοποίησης στον άνθρωπο. Η παράβαση

[292] HB 53 Human tracking devices; unlawful use thereof by insurer or employer, διαθέσιμο στο https://lis.virginia.gov/cgi-bin/legp604.exe?101+sum+HB53

[293] SB 235, Microchip Consent Act of 2009, διαθέσιμο στο http://www.legis.ga.gov/legislation/en-US/display/20092010/SB/235

[294] Ποινές για πλημμελήματα όπως ορίζονται στη Τζόρτζια βλ. https://www.criminaldefenselawyer.com/resources/georgia-misdemeanor-crimes-class-and-sentences.htm

[295] SB 109, διαθέσιμο στο https://www.leg.state.nv.us/Session/79th2017/Bills/SB/SB109.pdf

θεωρείται κακούργημα τρίτου βαθμού[296] και οι παραβάτες τιμωρούνται με φυλάκιση 1 έως 5 έτη ή/και χρηματική ποινή έως 10.000 δολάρια.

Ενώ τέλος στο Οχάιο το 2006 (SB 349[297]) και στο Μιζούρι το 2008 (Missouri Revised Statutes §285.035.1[298]) παρόμοια νομοσχέδια και νόμοι αντίστοιχα για την εμφύτευση RFID ετικέτας στην πρώτη περίπτωση και παρόμοιων τεχνολογιών στη δεύτερη περίπτωση στο ανθρώπινο σώμα, γράφτηκαν αποκλειστικά για την προστασία των εργαζομένων. Απαγορεύουν δηλαδή στους εργοδότες να επιβάλλουν στους εργαζομένους την εμφύτευση συσκευής αναγνώρισης για οποιοδήποτε λόγο. Επομένως, όπως είναι αυτονόητο δεν απαγορεύουν ρητά την εμφύτευση από άλλους, όπως την πολιτειακή κυβέρνηση, τους γιατρούς και τους γονείς και κηδεμόνες ανηλίκων[299]. Περαιτέρω, με νόμο στο Μιζούρι δίνεται ο ορισμός της συσκευής ταυτοποίησης και η παράβαση χαρακτηρίζεται ως πλημμέλημα πρώτου βαθμού, ενώ οι παραβάτες τιμωρούνται με φυλάκιση μέχρι ενός έτους ή/και χρηματική ποινή που δεν υπερβαίνει τα 2.000 δολάρια[300].

Συνοψίζοντας, λαμβάνοντας υπόψη όλες τις παραπάνω περιπτώσεις ανά πολιτεία, προκύπτουν τα παρακάτω:

- όλα τα νομοσχέδια ή νόμοι καλύπτουν τους πολίτες σε πολιτειακό επίπεδο
- τα νομοσχέδια ή νόμοι αφορούν γενικότερα την εμφύτευση συσκευών ταυτοποίησης ή εμφύτευση μικροτσίπ, με εξαίρεση τις πολιτείες Βόρεια Ντακότα, Γιούτα και Οχάιο, οι οποίες αναφέρονται συγκεκριμένα στη χρήση της τεχνολογίας RFID,
- στην Καλιφόρνια και στο Μιζούρι, δίνεται ο ορισμός της συσκευής ταυτοποίησης,

[296] Ποινές για κακουργήματα όπως ορίζονται στη Νεβάδα, βλ. https://law.justia.com/codes/nevada/2010/title15/chapter193/nrs193-130.html

[297] S. B. No. 349, διαθέσιμο στο http://archives.legislature.state.oh.us/JournalText126/SJ-07-18-06.pdf. Επίσης βλ. https://www.acluohio.org/archives/press-releases/newly-introduced-bill-would-protect-privacy

[298] MO Rev Stat §285.035, Microchip technology, employer not to require employees to be implanted - violation, penalty, διαθέσιμο στο http://revisor.mo.gov/main/OneSection.aspx?section=285.035&bid=14972&hl

[299] Βλ. Friggieri, A., Michael, K., Michael, M. G. (2009). The legal ramifications.., ό.π. σελ. 5.

[300] Ποινές για πλημμελήματα όπως ορίζονται στο Μιζούρι, βλ. https://carvercantin.com/missouri-misdemeanor/

- οι παραβάσεις χαρακτηρίζονται στις περισσότερες περιπτώσεις πταίσματα ή πλημμελήματα, ενώ σε δύο περιπτώσεις χαρακτηρίζονται κακούργημα (Φλόριντα και Νεβάδα) και οι παραβάτες τιμωρούνται με πρόστιμο ή χρηματική ποινή αντίστοιχα ή/και φυλάκιση. Συγκεκριμένα παρατηρήθηκε ότι σε αρκετές πολιτείες τα πρόστιμα/χρηματική ποινή είναι έως 10.000 δολάρια (Ουισκόνσιν, Καλιφόρνια, Γιούτα, Οκλαχόμα και Νεβάδα), ενώ σε άλλες τα πρόστιμα/χρηματική ποινή είναι πολύ μικρότερα (Οχάιο και Κολοράντο). Βέβαια για να χαρακτηριστεί εάν είναι μεγάλο ή όχι ένα πρόστιμο/χρηματική ποινή, πρέπει να ληφθεί υπόψη και το βιοτικό επίπεδο των πολιτών[301],
- στην Καλιφόρνια και στη Γιούτα, πέρα από τη χρηματική ποινή λόγω της παράβασης, προβλέπεται και περαιτέρω χρηματική ποινή 1.000 δολαρίων για κάθε ημέρα που δεν αφαιρείται ή δεν απενεργοποιείται το εμφύτευμα, ενώ στην Οκλαχόμα και στο Ουισκόνσιν και για κάθε μέρα που συνεχίζεται η παράβαση θα θεωρείται ξεχωριστό αδίκημα,
- στην Καλιφόρνια, αφήνει να εννοηθεί πως οι γονείς και οι κηδεμόνες ανηλίκων μπορούν να επιτρέψουν την εμφύτευση συσκευής ταυτοποίησης κάτω από ορισμένες προϋποθέσεις,
- στη Φλόριντα, είναι η μοναδική περίπτωση στην οποία αναφέρεται ότι είναι απαραίτητη η ενημέρωση αλλά και η γραπτή συγκατάθεση του υποκειμένου,
- στο Οχάιο και στο Μιζούρι το νομοσχέδιο και ο νόμος αντίστοιχα στοχεύουν αποκλειστικά στην προστασία των εργαζομένων.

[301] Βλ. Friggieri, A., Michael, K., Michael, M. G. (2009). The legal ramifications.., ό.π. σελ. 7.

1.3. Συμπεράσματα σχετικά με την υπάρχουσα νομοθεσία για την εμφύτευση RFID ετικέτας στο ανθρώπινο σώμα

Η εμφύτευση RFID ετικέτας στο ανθρώπινο σώμα δεν είναι καινούριο γεγονός, αφού για πρώτη φορά έγινε γνωστό πως εφαρμόστηκε το 1998 κατά την εκτέλεση ερευνητικού έργου. Μάλιστα, σύμφωνα με έρευνα που έχει γίνει, έκτοτε έχουν παρατηρηθεί έως και 10.000 εφαρμογές παγκοσμίως.

Όπως μελετήθηκε στο παραπάνω υποκεφάλαιο, στις Ηνωμένες Πολιτείες της Αμερικής, προκειμένου να προστατέψουν τους πολίτες τους από τα ζητήματα ιδιωτικότητας που προκύπτουν με την εμφύτευση RFID ετικέτας στο ανθρώπινο σώμα, είχαν αρχίσει να δραστηριοποιούνται για πρώτη φορά το 2006 όπου σε πολιτειακό επίπεδο δημοσιεύτηκε νόμος ο οποίος απαγορεύει την υποχρεωτική εμφύτευση μικροτσίπ σε άνθρωπο. Και από τότε μέχρι και σήμερα έχει δημοσιευτεί σχετικός νόμος σε 6 πολιτείες και σχετικό νομοσχέδιο σε άλλες 6 πολιτείες.

Αντίθετα, στην Ευρωπαϊκή Ένωση δεν έχει υπάρξει ούτε σχετική νομοθεσία, ούτε νομοσχέδιο. Η μόνη δραστηριοποίηση που παρατηρήθηκε είναι μία μελέτη που έγινε για την Επιτροπή του Ευρωπαϊκού Κοινοβουλίου Απασχόλησης και Κοινωνικών Υποθέσεων τον Ιανουάριο του 2018 σχετικά με την εμφύτευση RFID ετικέτας συγκεκριμένα σε εργαζομένους. Η μελέτη κατέληξε στο συμπέρασμα ότι εφόσον η εμφύτευση έχει άμεση σχέση με τη συλλογή, την αποθήκευση και την επεξεργασία δεδομένων προσωπικού χαρακτήρα, τότε εμπίπτει στο πεδίο του νόμου περί προστασίας προσωπικών δεδομένων (ΓΚΠΔ) ο οποίος δίνει ιδιαίτερη βαρύτητα στη λήψη συγκατάθεσης από το υποκείμενο.

Αυτό όμως που δεν προβλέπεται ξεκάθαρα είναι τι θα ισχύει όταν θα λήξει η σύμβαση εργασίας[302]. Καταρχήν πρέπει να ενημερωθεί το υποκείμενο ότι πρέπει να αφαιρεθεί το εμφύτευμα, να αποφασιστεί με ποιον τρόπο θα

[302] Σχετικά με την ιδιοκτησία των δεδομένων μετά την αφαίρεση της RFID ετικέτας στον εργασιακό χώρο βλ. Graveling R., Winski Th., Dixon K. (2018). The use of chip implants for workers, ό.π. σελ. 24.

αφαιρεθεί, σε ποιον θα ανήκει η ευθύνη για την αφαίρεση, σε ποιον θα ανήκει η RFID ετικέτα μετά την αφαίρεση, μήπως πρέπει να καταστραφεί και αν ναι με ποιο τρόπο, σε ποιον θα ανήκουν τα συλλεχθέντα δεδομένα μετά την αφαίρεση και ποια θα είναι η επιτρεπόμενη χρονική διάρκεια τήρησης των δεδομένων (μετά την αφαίρεση). Όλα αυτά είναι ερωτήματα τα οποία πρέπει να απαντηθούν με σαφή και κατανοητό τρόπο προκειμένου να διασφαλιστεί η μείωση του κινδύνου προσβολής της προσωπικότητας του υποκειμένου.

Επίσης, δεν είναι ξεκάθαρο πώς θα εξασφαλιστεί η προστασία των υποκειμένων σε περίπτωση που έχουν δεχθεί ψυχολογικές πιέσεις προκειμένου να αποδεχθούν την εμφύτευση της RFID ετικέτας. Είναι γεγονός, κυρίως στη σημερινή εποχή, πως η ανάγκη των ανθρώπων για την εύρεση και σύναψη σύμβασης εργασίας, σε συνδυασμό με την ελλιπή ενημέρωση για τις επιπτώσεις στην ιδιωτικότητά τους, μπορεί να τους οδηγήσει να δεχθούν παρά τη πραγματική θέλησή τους. Επίσης, τα προνόμια και οι ευνοϊκότερες συνθήκες που μπορεί να προσφέρουν σε όσους δεχθούν την εμφύτευση της RFID ετικέτας μπορεί να είναι παραπλανητικά και σε συνδυασμό και πάλι με την ελλιπή ενημέρωση μπορεί να οδηγήσουν το υποκείμενο να το δεχθεί.

Από όλα τα παραπάνω είναι φανερό πως, όπως στις Ηνωμένες Πολιτείες της Αμερικής, έτσι και στην Ευρώπη πρέπει να αναληφθούν άμεσα πρωτοβουλίες για την προστασία του υποκειμένου συγκεκριμένα από την υποχρεωτική εμφύτευση μικροτσίπ ταυτοποίησης, όπως π.χ. με την τεχνολογία RFID, λαμβάνοντας υπόψη και τις περιπτώσεις όπου τα υποκείμενα μπορεί να δεχθούν ψυχολογική πίεση, και μάλιστα σε οποιαδήποτε εφαρμογή. Η εμφύτευση RFID ετικέτας στο ανθρώπινο σώμα είναι ένα γεγονός το οποίο δεν θα αργήσει να απασχολήσει τον ευρωπαϊκό χώρο καθώς τα οφέλη του είναι ισχυρά, αλλά πρέπει να ληφθεί υπόψη πως και οι επιπτώσεις στην ιδιωτικότητα είναι σοβαρές και πιθανόν μη αναστρέψιμες.

Μάλιστα, στη συγκεκριμένη περίπτωση πρέπει να ληφθεί σοβαρά υπόψη ότι μπορεί να δημιουργηθούν και σοβαρά προβλήματα κοινωνικής περιθωριοποίησης και στιγματισμού των ανθρώπων που δέχτηκαν την εμφύτευση RFID ετικέτας στο σώμα τους. Ενδέχεται να ενταχθούν σε μία

κατηγορία ανθρώπων την οποία με την πάροδο του χρόνου θα την απομονώσουν με αποτέλεσμα να περιοριστούν οι ελευθερίες τους και πιθανόν να θιγεί και η αξιοπρέπειά τους. Ένα από τα χειρότερα σενάρια το οποίο μπορεί να συμβεί είναι να φοβούνται να παρευρίσκονται και να δραστηριοποιούνται μαζί τους και άλλοι άνθρωποι φοβούμενοι μήπως έτσι εκτεθούν και οι ίδιοι στους πιθανούς κινδύνους, όπως την παρακολούθηση.

Συμπερασματικά, κρίνεται αναγκαίο καταρχήν να πραγματοποιηθεί κατάλληλη πληροφόρηση των πολιτών σχετικά με τις τεχνολογίες ταυτοποίησης, όπως η RFID, ευαισθητοποίηση των πολιτών σχετικά με την εμφύτευση στο ανθρώπινο σώμα μίας τέτοιας τεχνολογίας και ενημέρωση για τη σημαντικότητα του ζητήματος και το μέγεθος των επιπτώσεων που μπορεί να επιφέρει στην ιδιωτικότητά τους. Επίσης, οφείλει ο νομοθέτης να απαγορεύσει την υποχρεωτική εμφύτευση RFID ετικέτας στον άνθρωπο για οποιοδήποτε λόγο και όχι μόνο στον εργασιακό χώρο και να ορίσει αυστηρές κυρώσεις σε περιπτώσεις παραβάσεων.

Στην περίπτωση που είναι απαραίτητο ένας άνθρωπος να δεχθεί την εμφύτευση RFID ετικέτας, για παράδειγμα για ιατρικούς σκοπούς, θα πρέπει πέρα από την ενημέρωση του υποκειμένου με σαφή και κατανοητό τρόπο να λαμβάνεται και η γραπτή του συγκατάθεσή του. Ταυτόχρονα θα πρέπει να διασφαλίζεται πως θα τηρούνται απόλυτα και οι αρχές της επεξεργασίας, όπως ορίζονται στο άρθρο 5 στο ΓΚΠΔ σύμφωνα με τις οποίες τα προσωπικά δεδομένα θα πρέπει α) να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο («νομιμότητα, αντικειμενικότητα και διαφάνεια»), β) να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς («περιορισμός του σκοπού»), γ) να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»), δ) να είναι ακριβή και, όταν είναι αναγκαίο, να επικαιροποιούνται λαμβάνοντας όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας («ακρίβεια»), ε) να διατηρούνται

υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα («περιορισμός της περιόδου αποθήκευσης») και στ) να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»).

2. Χρήση της τεχνολογίας RFID στα ηλεκτρονικά διαβατήρια

Τα ηλεκτρονικά (ή αλλιώς βιομετρικά) διαβατήρια είναι η ψηφιακή μορφή των αντίστοιχων κλασσικών χάρτινων διαβατηρίων, τα οποία δύναται να προσφέρουν μεγαλύτερη αξιοπιστία για την αυθεντικότητά τους και ταυτόχρονα την αλάνθαστη εξακρίβωση και ταυτοποίηση των υποκειμένων.

Μετά την τρομοκρατική επίθεση της 11ης Σεπτεμβρίου το 2001, η Επιτροπή της ΕΕ κλήθηκε από τα κράτη μέλη να λάβει άμεσα μέτρα για την αύξηση της ασφάλειας των διαβατηρίων και την καταπολέμηση της δημιουργίας πλαστών διαβατηρίων. Ενόψει λοιπόν των γεγονότων, γεννήθηκε η ανάγκη υλοποίησης και χρήσης ηλεκτρονικών διαβατηρίων με την ενσωμάτωση μάλιστα βιομετρικών χαρακτηριστικών, όπως τα δακτυλικά αποτυπώματα, καθώς και η χρήση μίας κοινής τεχνολογίας, όπως η RFID[303], για την επίτευξη παγκόσμιας διαλειτουργικότητας αυτών.

Ταυτόχρονα όμως, κρίνεται άκρως απαραίτητο να τεθούν και νομικοί περιορισμοί για την εξασφάλιση της προστασίας των προσωπικών δεδομένων του κατόχου του ηλεκτρονικού διαβατηρίου. Σε αυτό το κεφάλαιο μελετάται η σχετική νομοθεσία και οι σχετικές προτάσεις για την έκδοση

[303] Λεπτομέρειες σχετικά με την εφαρμογή της τεχνολογίας RFID στα ηλεκτρονικά διαβατήρια βλ. Nikita, M., (2012). RFID chips and EU e-passports: the end of privacy, ό.π. και παραπέρα βιβλιογραφία.

ηλεκτρονικών διαβατηρίων στην Ευρωπαϊκή Ένωση και στις Ηνωμένες Πολιτείες της Αμερικής.

2.1. Ευρωπαϊκή Ένωση

Μελετώντας τα βήματα που έγιναν στην Ευρωπαϊκή Ένωση για την καταπολέμηση των πλαστών διαβατηρίων και ταυτόχρονα την προστασία των αποθηκευμένων προσωπικών δεδομένων σε αυτά, παρατηρούμε τις παρακάτω ενέργειες. Η πρώτη κινητοποίηση έγινε το 2003 όταν η Ομάδα εργασίας του άρθρου 29 εξέδωσε έγγραφο εργασίας[304] σχετικά με τα στοιχεία βιομετρίας[305], εξαιτίας της ταχείας εξέλιξης των τεχνολογιών βιομετρίας και της εκτεταμένης εφαρμογής αυτών σε αυτοματοποιημένες διαδικασίες για σκοπούς επαλήθευσης, εξακρίβωσης και αναγνώρισης της ταυτότητας προσώπων. Σκοπός του εγγράφου ήταν να συμβάλλει στην αποτελεσματική εφαρμογή των εθνικών διατάξεων περί προστασίας δεδομένων σε τέτοια συστήματα όπως εγκρίθηκαν βάσει της Οδηγίας 95/46/ΕΚ, τονίζοντας τη σπουδαιότητα της απόλυτης τήρησης των αρχών προστασίας των δεδομένων.

Στο παραπάνω έγγραφο, σημαντική είναι η υπόδειξη της Ομάδας εργασίας του άρθρου 29 σχετικά με το γεγονός ότι η συλλογή δακτυλικών αποτυπωμάτων προηγουμένως χρησιμοποιούνταν για σκοπούς επιβολής του δικαίου, όπως στο πλαίσιο ανακρίσεων, και για τη διαπίστωση εγκληματικής δραστηριότητας[306,307], ενώ η συλλογή τους υπόκειντο σε νομικούς

[304] Πρόκειται για το "Έγγραφο εργασίας σχετικά με τα στοιχεία βιομετρίας" της Ομάδας εργασίας του άρθρου 29 το οποίο εγκρίθηκε την 1η Αυγούστου 2003, 12168/03/EL, WP 80, διαθέσιμο στο http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_el.pdf

[305] Σχετικά με τις βιομετρικές εφαρμογές και τη συμβατότητά τους με την προστασία των προσωπικών δεδομένων βλ. Ιγγλεζάκης, Ι. (2009). Οι εφαρμογές της βιομετρικής τεχνολογίας και η συμβατότητά τους με την προστασία των προσωπικών δεδομένων, ΣΥΝήΓΟΡΟΣ 76/2009, σελ: 77-79.

[306] Ομοίως είχε ειπωθεί και σε απόφαση της ελληνικής ΑΠΔΠΧ (Αριθ. Πρωτ.:510/17/15-05-2000, διαθέσιμη στο http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=174,76,127,28,65,254,126,231) σχετικά με την εισαγωγή του δακτυλικού αποτυπώματος στις ελληνικές ταυτότητες, ότι κατά την κοινή αντίληψη, το αποτύπωμα (η "σήμανση") συνδέεται με την υποψία ή διαπίστωση εγκληματικής δραστηριότητας ("σεσημασμένοι"), η απόδοση της οποίας έστω και εν δυνάμει στο σύνολο του ελληνικού λαού, υπερβαίνει το αναγκαίο μέτρο και προσβάλλει την προστατευόμενη από το Σύνταγμα αξία του ανθρώπου.

περιορισμούς[308]. Επομένως, δεν αποκλείεται εάν στα ηλεκτρονικά διαβατήρια αποθηκεύονται ψηφιακά δακτυλικά αποτυπώματα, οι κάτοχοί τους να ενταχθούν στην κατηγορία των υπόπτων για διάπραξη εγκλημάτων[309].

Την ίδια χρονιά, στο Ευρωπαϊκό Συμβούλιο της Θεσσαλονίκης (19-20/06/2003) σχετικά με τη διαμόρφωση κοινής πολιτικής για την παράνομη μετανάστευση, τα εξωτερικά σύνορα, την επιστροφή των παράνομων μεταναστών και τη συνεργασία με τρίτες χώρες, κατέληξε στο συμπέρασμα ότι απαιτείται μια συνεκτική προσέγγιση της ΕΕ όσον αφορά τη χρήση βιομετρικών αναγνωριστικών στοιχείων ή βιομετρικών δεδομένων σε έγγραφα των υπηκόων τρίτων χωρών, σε διαβατήρια των πολιτών της ΕΕ και σε συστήματα πληροφοριών (VIS και SIS II).

Ένα χρόνο μετά, το Συμβούλιο της Ευρωπαϊκής Ένωσης εκτιμώντας τις προδιαγραφές του Διεθνούς Οργανισμού Πολιτικής Αεροπορίας (ICAO)[310], ιδίως εκείνες που ορίζονται στο έγγραφο Doc 9303 το σχετικό με τα αναγνώσιμα από μηχάνημα ταξιδιωτικά έγγραφα, εξέδωσε τον Κανονισμό 2252/2004[311] σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων[312] στα διαβατήρια και τα

[307] Το 2005, η Ομάδα εργασίας του άρθρου 29 σε γνώμη της σχετικά με την ενσωμάτωση βιομετρικών στοιχείων στα διαβατήρια (Γνώμη 3/2005, 1710-01/05/EL-Αναθ., WP 112, 04/09/12, σελ: 10/14) εξέφρασε και πάλι τις επιφυλάξεις της σχετικά με τους κινδύνους ηθικής τάξεως λόγω του ότι η χρήση των δακτυλικών αποτυπωμάτων γινόταν μέχρι τότε ως επί το πλείστον για την εξακρίβωση εγκληματικής δραστηριότητας, αλλά και ότι υπάρχει κίνδυνος να στιγματιστούν τα άτομα που δεν μπορούν να υποβληθούν σε βιομετρικές εξετάσεις (όπως οι ανάπηροι).

[308] Βλ. Iglezakis, I. (2013). EU Data Protection Legislation and Case-Law with Regard to Biometric Applications, in Bottis, M. (edit.), Proceedings of the 3rd ISIL 2010 - An Information Law for the 21st century, ed. Nomiki Bibliothiki, σελ. 42.

[309] Βλ. Παναγοπούλου-Κουτνατζή, Φ. (2013). Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας: Σκέψεις με αφορμή την απόφαση ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012), ΔiΜΕΕ 4/2013, σελ. 491 και Μαντζούφας, Π. (2010). Βιοπολιτική και βιομετρία, διαθέσιμο στο https://www.constitutionalism.gr/1828-biopolitiki-kai-biometria/.

[310] Αναλυτικότερα βλ. Μέρος τρίτο, υποκεφάλαιο 2.2.

[311] Κανονισμός (ΕΚ) αριθ. 2252/2004 του Συμβουλίου της 13ης Δεκεμβρίου 2004 σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών (ΕΕ L 385, 29/12/2004, σελ: 1 - 6), διαθέσιμος στο http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=uriserv:OJ.L_.2004.385.01.0001.01.ELL&toc=OJ:L:2004:385:TOC. Αξίζει να αναφερθεί ότι ο Κανονισμός 2252/2004, πριν την τροποποίησή του, στο άρθρο 1 παράγραφο 2 προέβλεπε να περιλαμβάνονται στα διαβατήρια και στα ταξιδιωτικά έγγραφα η εικόνα του προσώπου του κατόχου και τα δακτυλικά του αποτυπώματα. Λόγω όμως αντιδράσεων, τροποποιήθηκε και διευκρινίστηκε ότι προβλέπεται η ενσωμάτωση μόνο δύο επίπεδων δακτυλικών αποτυπωμάτων.

[312] Στο νέο Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ), στο άρθρο 4 ορίστηκε ότι βιομετρικά δεδομένα είναι "*δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική*

ταξιδιωτικά έγγραφα των κρατών μελών, ο οποίος τροποποιήθηκε από τον Κανονισμό 444/2009[313]. Συγκεκριμένα, στο άρθρο 1 του Κανονισμού 444/2009 (ΕΕ L 142, σ. 1, και διορθωτικό ΕΕ L 188, σ. 127) ορίζεται ότι «*τα διαβατήρια και τα ταξιδιωτικά έγγραφα περιλαμβάνουν μέσο αποθήκευσης υψηλής ασφαλείας το οποίο περιέχει εικόνα προσώπου. Τα κράτη μέλη περιλαμβάνουν επίσης την ενσωμάτωση δύο επίπεδων δακτυλικών αποτυπωμάτων υπό μορφή που εξασφαλίζει τη διαλειτουργικότητα. Τα δεδομένα ενσωματώνονται κατά τρόπο ασφαλή και το μέσο αποθήκευσης διαθέτει επαρκή χωρητικότητα και ικανότητα προκειμένου να διασφαλίζεται η ακεραιότητα, η αυθεντικότητα και η εμπιστευτικότητα των δεδομένων*»[314].

Με τον παραπάνω Κανονισμό προβλέπεται γενική υποχρέωση παροχής δύο δακτυλικών αποτυπωμάτων (των δύο δεικτών του αριστερού και του δεξιού χεριού), τα οποία αποθηκεύονται σε ανεπαφικό πλινθίο του διαβατηρίου ή του ταξιδιωτικού εγγράφου και με τον τρόπο αυτό εξασφαλίζεται μεγαλύτερη ασφάλεια των διαβατηρίων και των ταξιδιωτικών εγγράφων και καθιερώνεται ένας πιο αξιόπιστος σύνδεσμος μεταξύ του κατόχου και του διαβατηρίου ή του ταξιδιωτικού εγγράφου, συμβάλλοντας κατ' αυτόν τον τρόπο σημαντικά στη μέριμνα για την προστασία των διαβατηρίων και των ταξιδιωτικών εγγράφων από δόλια χρήση τους (ΕΕ L 142, σελ.1, αιτιολογικές σκέψεις 2 και 3).

Εφόσον λοιπόν με τον παραπάνω Κανονισμό ορίζεται ότι τα ψηφιακά διαβατήρια πέρα από την εικόνα προσώπου θα ενσωματώνουν και την ψηφιακή πληροφορία δύο δακτυλικών αποτυπωμάτων του κατόχου,

---

επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα".

[313] Κανονισμός (ΕΚ) αριθ. 444/2009 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 28 Μαΐου 2009 , για την τροποποίηση του Κανονισμού (ΕΚ) αριθ. 2252/2004 του Συμβουλίου σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών (ΕΕ L 142), διαθέσιμος στο http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=uriserv:OJ.L_.2009.142.01.0001.01.ELL&toc=OJ:L:2009:142:TOC

[314] Αρχικά, στο σχετικό σχέδιο Κανονισμού (COM(2004)116-τελικό, διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2004:0116:FIN) που υπέβαλε η Ευρωπαϊκή Επιτροπή πρότεινε την υποχρεωτική ενσωμάτωση στα διαβατήρια μόνο την εικόνα του προσώπου, ενώ η ενσωμάτωση των δακτυλικών αποτυπωμάτων μπορούσε να γίνει βάσει εθνικής νομοθεσίας.

εγείρονται σημαντικά ερωτήματα σχετικά με την προστασία των προσωπικών δεδομένων του κατόχου.

Καταρχήν, παρατηρείται ότι ο Κανονισμός περιλαμβάνει ειδικές διατάξεις για την προστασία των δεδομένων. Συγκεκριμένα, στο άρθρο 4 παρ. 1 του Κανονισμού αναγνωρίζεται το δικαίωμα επαλήθευσης των δεδομένων προσωπικού χαρακτήρα που περιέχονται στο διαβατήριο από το υποκείμενο καθώς επίσης και η δυνατότητα διόρθωσης ή απάλειψης αυτών. Επομένως, προκειμένου το υποκείμενο να μπορεί να ασκήσει αυτό το δικαίωμα είναι αυτονόητο πως οι Αρχές πρέπει να παρέχουν κατάλληλους αναγνώστες σε ευκόλως προσβάσιμα σημεία έτσι ώστε το υποκείμενο να έχει πρόσβαση στα δεδομένα του που είναι αποθηκευμένα στην ετικέτα του διαβατηρίου (μέσω της σάρωσης) και να μπορεί να ζητήσει και τη διόρθωση ή τη διαγραφή αυτών[315]. Επίσης, στην παρ. 3 (β) του ίδιου άρθρου ορίζεται ότι η χρήση των βιομετρικών δεδομένων περιορίζεται στην εξακρίβωση της ταυτότητας του κατόχου και συγκεκριμένα μόνο όπου "*είναι υποχρεωτική δια νόμου η επίδειξη διαβατηρίου"*. Συνεπώς, ο Κανονισμός απαγορεύει τη χρήση των δεδομένων για άλλο σκοπό χωρίς την ενημέρωση του υποκειμένου των δεδομένων[316].

Ωστόσο, στον Κανονισμό δεν απαγορεύεται η αποθήκευση των βιομετρικών στοιχείων που θα περιλαμβάνονται στα διαβατήρια και στα ταξιδιωτικά έγγραφα σε μία κεντρική βάση δεδομένων, θέμα το οποίο υπάγεται αποκλειστικά στην εθνική νομοθεσία[317]. Ο λόγος που δεν απαγορεύτηκε η αποθήκευσή τους είναι για να αποτραπεί η έκδοση διαβατηρίων από τους πολίτες με διαφορετικά ονόματα[318]. Γεγονός όμως που

[315] Βλ. Kosta, E. (2006). The use of RFID chips on Identification Documents, Proceedings of the 2nd Greek National Conference with International Participation: Electronic democracy - challenges of the digital era, Athens, σελ. 475 και Hornung G. (2007), The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards, SCRIPTed, Vol. 4 (3), σελ. 253 και Nikita, M., (2012). RFID chips and EU e-passports: the end of privacy, ό.π. σελ. 2016.

[316] Βλ. Hornung G. (2007), The European Regulation on Biometric Passports: Legislative Procedures.., ό.π. σελ. 253.

[317] Η Ομάδα εργασίας του άρθρου 29 σε γνώμη της σχετικά με την εφαρμογή του εν λόγω Κανονισμού (Γνώμη 3/2005, 1710-01/05/EL-Αναθ., WP 112, 04/09/12, σελ: 10/14) εξέφρασε τις επιφυλάξεις της για τη συγκρότηση μίας κεντρικής ευρωπαϊκής ή εθνικής βάσης βιομετρικών δεδομένων η οποία έρχεται σε αντίθεση με τη θεμελιώδη αρχή της αναλογικότητας καθώς και τους κινδύνους τεχνικής φύσεως που σχετίζονται με τη χρήση του ανεπαφικού πλινθίου.

[318] Βλ. Ιγγλεζάκης, Ι. (2010). Ο Κανονισμός 2252/2004 για τα βιομετρικά διαβατήρια και οι ρήτρες διασφάλισης της προστασίας προσωπικών δεδομένων. ΣΥΝήΓΟΡΟΣ 78/2010, σελ: 81-83.

τελικά θα έχει ως αποτέλεσμα τη δημιουργία μίας βάσης δεδομένων με μεγάλο όγκο πληροφοριών και "*δυναμική που μπορεί να οδηγήσει σε καταχρήσεις εκ μέρους των αρχών*"[319].

Η ανάγκη για την απαγόρευση μιας τέτοιας πράξης είναι μεγάλη διότι "*η σύσταση κεντρικής τράπεζας δεδομένων θα παραβίαζε το σκοπό και την αρχή της αναλογικότητας*[320]*. Θα αύξανε επίσης τον κίνδυνο κατάχρησης και διολίσθησης της χρήσης για άλλους σκοπούς. Τέλος θα αύξανε τον κίνδυνο χρησιμοποίησης των βιομετρικών αναγνωριστικών στοιχείων ως "κλειδιών πρόσβασης" σε διάφορες τράπεζες δεδομένων και στη συνέχεια διασύνδεσης στοιχείων*»[321]. Επιπροσθέτως, ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων με γνωμοδότησή του το 2008[322], έκρινε πως σε μία τέτοια περίπτωση "*παρουσιάζ[ονται] επιπλέον κίνδυνοι για την προστασία των προσωπικών δεδομένων, όπως η ανάπτυξη άλλων σκοπών που δεν προβλέπονται στον κανονισμό, ή ακόμα και επιδρομές αλίευσης στη βάση δεδομένων που θα είναι δύσκολο να περιοριστούν*" (παρ. 27) και συνέστησε στην Επιτροπή να θέσει νέα μέτρα εναρμόνισης προκειμένου να εφαρμοστεί η χρήση μόνο αποκεντρωμένης αποθήκευσης στο ασύρματο ολοκληρωμένο κύκλωμα του διαβατηρίου (παρ. 28)[323].

---

[319] Βλ. Ιγγλεζάκης, Ι. (2010). Ο Κανονισμός 2252/2004 για τα βιομετρικά διαβατήρια και οι ρήτρες διασφάλισης της προστασίας προσωπικών δεδομένων. ΣΥΝήΓΟΡΟΣ 78/2010, σελ: 82.

[320] Αναφορικά με την αρχή της αναλογικότητας βλ. Ορφανουδάκη Σ. (2003). Η αρχή της αναλογικότητας, σειρά: μελέτες συνταγματικού δικαίου και Πολιτειολογίας, Αθήνα-Θεσσαλονίκη.

[321] Το Συμβούλιο δεν έλαβε υπόψη την προτεινόμενη τροποποίηση του Κοινοβουλίου σχετικά με την απαγόρευση συγκρότησης κεντρικών τραπεζών δεδομένων διαβατηρίων της Ευρωπαϊκής Ένωσης και εγγράφων ταξιδιών που περιέχουν όλα τα βιομετρικά στοιχεία των κατόχων διαβατηρίων της ΕΕ και άλλα δεδομένα. Βλ. νομοθετικό ψήφισμα του Ευρωπαϊκού Κοινοβουλίου σχετικά με την πρόταση της Επιτροπής για Κανονισμό του Συμβουλίου που αφορά τη θέσπιση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια των πολιτών της ΕΕ (COM(2004)0116 – C5-0101/2004 – 2004/0039(CNS)), τροπολογία 5, διαθέσιμο στο http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A6-2004-0028+0+DOC+XML+V0//EL#title1.

[322] Γνωμοδότηση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων σχετικά με την πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την τροποποίηση του Κανονισμού (ΕΚ) αριθ .2252/2004 του Συμβουλίου σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών (2008/C 200/01), διαθέσιμη στο https://edps.europa.eu/sites/edp/files/publication/08-03-26_biometrics_passports_el.pdf

[323] Νωρίτερα, και η Ομάδα εργασίας του άρθρου 29 σε γνώμη της είχε εκφράσει τις επιφυλάξεις της για μία κεντρική ευρωπαϊκή ή εθνική βάση βιομετρικών δεδομένων. Βλ. Γνώμη 3/2005 σχετικά με την εφαρμογή του Κανονισμού (ΕΚ) αριθ. 2252/2004 του Συμβουλίου, της 13ης Δεκεμβρίου 2004, σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών (ΕΕ L 385, 29/12/2004, σελ: 1 - 6),

Επιπρόσθετα, στα ηλεκτρονικά διαβατήρια εξαιτίας της αποθήκευσης προσωπικών δεδομένων προκύπτει και η ανάγκη να διασφαλίζεται η ακρίβειά τους[324]. Η αρχή της ακρίβειας των δεδομένων ορίζεται στο άρθρο 5 (δ) του ΓΚΠΔ, στην περίπτωση όμως των βιομετρικών δεδομένων πρέπει να ληφθεί υπόψη πως είναι πιθανόν τα δακτυλικά αποτυπώματα με την πάροδο των χρόνων να αλλάξουν λόγω διάφορων παραγόντων, όπως γενετικοί παράγοντες, η γήρανση, το περιβάλλον ή επαγγελματικοί λόγοι (κυρίως όσοι εκτελούν χειρωνακτικές εργασίες είναι πιθανόν να έχουν κοψίματα και μώλωπες)[325].

Στην περίπτωση λοιπόν όπου τα αποθηκευμένα βιομετρικά δεδομένα στα ψηφιακά διαβατήρια δεν είναι επίκαιρα και ακριβή, μπορεί να συντελέσουν σε λανθασμένη απόρριψη ή σε λανθασμένη αποδοχή των υποκειμένων[326] και για τις περιπτώσεις αυτές η ύπαρξη εφεδρικών συστημάτων στα σημεία όπου πραγματοποιούνται οι έλεγχοι των διαβατηρίων[327]. Μία τέτοια περίπτωση, όπου τα αποθηκευμένα προσωπικά δεδομένα δεν ήταν ακριβή, και συγκεκριμένα τα δακτυλικά αποτυπώματα, οδήγησαν στην παράνομη κράτηση του υποκειμένου για πάνω από δύο εβδομάδες επειδή κατηγορήθηκε ότι συμμετείχε σε βομβιστική επίθεση, είναι η περίπτωση του Mayfield εναντίον των Ηνωμένων Πολιτειών της Αμερικής[328].

διαθέσιμη στο http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp112_el.pdf

[324] Βλ. Bustard, J. (2015). The Impact of EU Privacy Legislation on Biometric System Deployment: Protecting citizens but constraining applications. IEEE Signal Processing Magazine, Vol. 32(5), σελ. 9.

[325] Βλ. Betzel, M. (2005). Privacy Year in Review: Recent Changes in the Law of Biometrics. ISJLP, 1, p. 522 και Παναγοπούλου-Κουτνατζή, Φ. (2013). Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας.., ό.π. σελ. 484.

[326] Βλ. Iglezakis, I. (2013). EU Data Protection Legislation and Case-Law with Regard to Biometric Applications, in Bottis, M. (edit.), Proceedings of the 3rd ISIL 2010 - An Information Law for the 21st century, ed. Nomiki Bibliothiki, σελ. 43 και Kindt, E. (2007). Biometric applications and the data protection legislation, Datenschutz and Datensicherheit, Vol. 31 (3), σελ. 168.

[327] Βλ. Ιγγλεζάκης, Ι. (2010). Ο Κανονισμός 2252/2004 για τα βιομετρικά διαβατήρια.., ό.π. σελ. 83 και Hornung G. (2007). The European Regulation on Biometric Passports: Legislative Procedures.., ό.π. σελ.258.

[328] Περισσότερες λεπτομέρειες σχετικά με την υπόθεση Mayfield v. US, No. 07-35865 βλ. https://caselaw.findlaw.com/us-9th-circuit/1499231.html. Επίσης, βλ. Bustard, J. (2015). The Impact of EU Privacy Legislation on Biometric System Deployment: Protecting citizens but constraining applications. IEEE Signal Processing Magazine, Vol. 32(5), σελ. 14.

Ένα χρόνο μετά την έκδοση του Κανονισμού, το 2005, παρατηρήθηκε ότι μέσα στις δέκα προτεραιότητες που ορίστηκαν από την Επιτροπή στο Πρόγραμμα της Χάγης[329] προκειμένου να ενισχυθεί η ελευθερία, η ασφάλεια και η δικαιοσύνη, συμπεριλήφθηκε και η εισαγωγή των βιομετρικών αναγνωριστικών στοιχείων στα ταξιδιωτικά έγγραφα, τις θεωρήσεις, τις άδειες διαμονής, τα διαβατήρια των πολιτών της ΕΕ και τα συστήματα πληροφόρησης για την ενίσχυση της ασφάλειας αυτών διατηρώντας παράλληλα τον απόλυτο σεβασμό των θεμελιωδών δικαιωμάτων. Με αυτό τον τρόπο επιτυγχάνεται ολοκληρωμένος έλεγχος της πρόσβασης στο έδαφος της Ένωσης και επομένως εξασφαλίζεται η ελεύθερη κυκλοφορία των προσώπων χωρίς περιορισμούς.

Ολοκληρώνοντας, αξίζει να σημειωθεί και η υπόθεση C-291/12 του 2012, όπου το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ) ερωτήθηκε[330] εάν είναι έγκυρη η παραπάνω υποχρέωση που επιβάλλει ο Κανονισμός 2252/2004 στα κράτη μέλη να εκδίδουν διαβατήρια που περιλαμβάνουν υποχρεωτικά ψηφιακά δακτυλικά αποτυπώματα και εικόνα του προσώπου[331]. Πιο συγκεκριμένα, ο M. Schwarz, Γερμανός υπήκοος, αιτήθηκε από τις αρμόδιες υπηρεσίες του κρατιδίου Bochum τη χορήγηση διαβατηρίου, αρνούμενος όμως να δεχτεί την υποχρεωτική λήψη των ψηφιακών δακτυλικών του αποτυπωμάτων ισχυριζόμενος ότι προσβάλλεται το θεμελιώδες δικαίωμα σεβασμού της ιδιωτικής ζωής και πιο συγκεκριμένα της προστασίας των δεδομένων προσωπικού χαρακτήρα, το οποίο καθιερώνει ο Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (άρθρα 7 και

[329] Το Ευρωπαϊκό Συμβούλιο το 2005 ενέκρινε το πολυετές Πρόγραμμα της Χάγης, το οποίο διαδέχεται το Πρόγραμμα του Τάμπερε, για την ενίσχυση της ελευθερίας, της ασφάλειας και της δικαιοσύνης, διαθέσιμο στο http://ec.europa.eu/transparency/regdoc/rep/1/2005/EL/1-2005-184-EL-F1-1.Pdf

[330] Απόφαση του Δικαστηρίου (τέταρτο τμήμα) της 17ης Οκτωβρίου 2013 Michael Schwarz κατά Stadt Bochum, «Προδικαστική παραπομπή – Χώρος ελευθερίας, ασφάλειας και δικαιοσύνης – Διαβατήριο με βιομετρικά στοιχεία – Ψηφιακά δακτυλικά αποτυπώματα – Κανονισμός (ΕΚ) 2252/2004 – Άρθρο 1, παράγραφος 2 – Κύρος – Νομική βάση – Διαδικασία έκδοσης – Άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης – Δικαίωμα στην ιδιωτική ζωή – Δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα – Αναλογικότητα», διαθέσιμο στο http://curia.europa.eu/juris/liste.jsf?language=el&num=C-291/12

[331] Αναλυτικότερα σχετικά με την υπόθεση βλ. Ιγγλεζάκης Ι. (2013). Διαβατήρια με βιομετρικά στοιχεία και προστασία προσωπικών δεδομένων στη νομολογία του ΔΕΕ (Με αφορμή την απόφαση ΔΕΕ στην υπόθεση C-291/12), Συνήγορος 100/2013, σελ: 71-73 και Παναγοπούλου-Κουτνατζή Φ. (2013). Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας: Σκέψεις με αφορμή την απόφαση ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012), ΔiΜΕΕ 4/2013, σελ. 482-492.

8 αντίστοιχα). Το αίτημα του M. Schwarz απορρίφτηκε και γι' αυτό μετέπειτα υποβλήθηκε αίτηση στο ΔΕΕ για την επίλυση της ένδικης διαφοράς μεταξύ του M. Schwarz και του κρατιδίου Bochum.

Το ΔΕΕ επισήμανε πως από τα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης προκύπτει ότι κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα από τρίτο μπορεί να αποτελέσει προσβολή των δικαιωμάτων σεβασμού της ιδιωτικής ζωής και προστασίας των δεδομένων προσωπικού χαρακτήρα (βλ. απόφαση ΔΕΕ, παρ. 25) και παράλληλα από το άρθρο 1 παρ. 2, του Κανονισμού 2252/2004 ότι η λήψη των ψηφιακών δακτυλικών αποτυπωμάτων καθώς και η καταχώρησής τους στο ενσωματωμένο μέσο αποθήκευσης του διαβατηρίου αποτελούν επεξεργασία δεδομένων προσωπικού χαρακτήρα (βλ. απόφαση ΔΕΕ, παρ. 29). Επομένως, αυτό που πρέπει να εξεταστεί είναι εάν η προσβολή αυτή των δικαιωμάτων είναι δικαιολογημένη (βλ. απόφαση ΔΕΕ, παρ. 30).

Σύμφωνα με την απόφαση του ΔΕΕ, τελικά δεν προκύπτει κανένα στοιχείο δυνάμενο να θίγει το κύρος του άρθρου 1 παρ. 2 του Κανονισμού (ΕΚ) 2252/2004. Συγκεκριμένα, το Δικαστήριο διαπίστωσε ότι η λήψη και αποθήκευση των ψηφιακών δακτυλικών αποτυπωμάτων αποτελούν πρόσφορα μέτρα εκπλήρωσης των επιδιωκόμενων σύμφωνα με τον Κανονισμό 2252/2004 σκοπών και, ως εκ τούτου, του σκοπού αποτροπής της παράνομης εισόδου προσώπων στο έδαφος της Ένωσης, ο οποίος είναι σκοπός γενικού συμφέροντος αναγνωρισμένος από την Ένωση (βλ. απόφαση ΔΕΕ, παρ. 45 και 38). Ενώ συγχρόνως δεν έχουν επισημανθεί άλλες εναλλακτικές μέθοδοι[332], πέραν της μεθόδου λήψης ψηφιακών δακτυλικών αποτυπωμάτων, οι οποίες να εκπληρώνουν τον σκοπό

[332] Η μοναδική πραγματική εναλλακτική της λήψης ψηφιακών δακτυλικών αποτυπωμάτων λύση που προβλήθηκε κατά την ενώπιον του Δικαστηρίου διαδικασία είναι η λήψη εικόνας της ίριδας του ματιού. Από κανένα σημείο της υποβληθείσας στο Δικαστήριο δικογραφίας όμως δεν προκύπτει ότι η διαδικασία αυτή θίγει τα προστατευόμενα από τα άρθρα 7 και 8 του Χάρτη δικαιώματα λιγότερο από τη λήψη ψηφιακών δακτυλικών αποτυπωμάτων, βλ. Απόφαση ΔΕΕ, παρ. 51, ό.π. σημ. 330. Επίσης, είναι γεγονός ότι το τεχνολογικό επίπεδο της μεθόδου που στηρίζεται στην αναγνώριση της ίριδας δεν είναι εξίσου υψηλό με εκείνο της μεθόδου που στηρίζεται στη λήψη ψηφιακών δακτυλικών αποτυπωμάτων, ενώ ταυτόχρονα αποτελεί σήμερα διαδικασία με σαφώς υψηλότερο κόστος, βλ. Απόφαση ΔΕΕ, παρ. 52, ό.π. σημ. 330.

προστασίας των διαβατηρίων από δόλια χρήση και συγχρόνως να προσβάλλουν σε μικρότερο βαθμό τα δικαιώματα που κατοχυρώνονται στα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (βλ. απόφαση ΔΕΕ, παρ. 53).

Τέλος, αξίζει να σχολιαστεί πως τον Απρίλιο του 2012, απασχόλησε και τέθηκε σε συζήτηση με την Ευρωπαϊκή Επιτροπή και τους ευρωβουλευτές το γεγονός ότι παρόλο που "*τα νέα ηλεκτρονικά διαβατήρια που εκδίδονται στην ΕΕ περιλαμβάνοντας κρυπτογραφημένα δεδομένα είναι αδύνατον να παραχαραχθούν, ωστόσο ο αριθμός των πλαστών διαβατηρίων που κυκλοφορούν στην Ευρώπη εκτιμάται πως παραμένει τεράστιος*"[333]. Συγκεκριμένα, αναφέρεται το παράδειγμα της Γαλλίας όπου από 500.000 έως 1 εκατομμύριο από τα 6,5 εκατομμύρια βιομετρικά διαβατήρια που υπάρχουν στη Γαλλία είναι πλαστογραφημένα, έχοντας αποκτηθεί με βάση πλαστά έγγραφα. Επομένως, το πρόβλημα έγκειται στις μεθόδους που χρησιμοποιούνται για τη συλλογή των βιομετρικών δεδομένων.

2.1.1. Η περίπτωση της Γαλλίας

Η Γαλλία, σε συμμόρφωση με τον Κανονισμό 2252/2004, αρχικά εξέδωσε διάταγμα το 2005 (Décret n°2005-1726 du 30 décembre 2005 relatif aux passeports όπως τροποποιήθηκε από το Décret No. 2008-426 du 30 avril 2008)[334] σύμφωνα με το οποίο στα ηλεκτρονικά διαβατήρια θα αποθηκεύονταν πέρα από τη ψηφιακή εικόνα του κατόχου και 8 δακτυλικά αποτυπώματα, ενώ τα δεδομένα όλων των ψηφιακών διαβατηρίων θα αποθηκεύονταν σε μία κεντρική βάση δεδομένων η οποία ονομάστηκε TES[335] (άρθρα 18 και 19).

[333] Βλ. Επικαιρότητα Ευρωπαϊκό Κοινοβούλιο, Βιομετρικά διαβατήρια: διαβατήριο για απάτη;, διαθέσιμο στο http://www.europarl.europa.eu/news/el/headlines/society/20120413STO42897/biometrika-diabateria-diabaterio-gia-apate

[334] Γαλλικό διάταγμα σχετικό με τα ηλεκτρονικά διαβατήρια, διαθέσιμο στο https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000018763666&dateTexte=vig

[335] Σύμφωνα με το άρθρο 18, σκοπός δημιουργίας μίας τέτοιας κεντρικής βάσης δεδομένων για την αποθήκευση των δεδομένων όλων των ψηφιακών διαβατηρίων είναι η ευκολότερη επεξεργασία των

Η έκδοση όμως του παραπάνω διατάγματος προκάλεσε την έντονη αντίδραση της γαλλικής αρχής προστασίας δεδομένων CNIL και της γαλλικής ένωσης ανθρωπίνων δικαιωμάτων (LDH) οι οποίες ζήτησαν την κατάργηση τους διατάγματος καθώς παραβιάζει την αρχή της αναλογικότητας. Έτσι λοιπόν, τα προαναφερόμενα άρθρα καταργήθηκαν με νέο διάταγμα το 2016[336] και πλέον η ψηφιακή εικόνα του κατόχου και μόνο δύο δακτυλικά αποτυπώματα αποθηκεύονται σε ανέπαφο μικροτσίπ που εμπεριέχεται στο ηλεκτρονικό διαβατήριο.

2.1.2. Η περίπτωση της Γερμανίας

Αντίθετα στη Γερμανία ο νόμος περί διαβατηρίων της 19ης Απριλίου 1986 (Passgesetz, BGBl. I S. 537) όπως τροποποιήθηκε τελευταία από το άρθρο 2 του νόμου της 7ης Ιουλίου 2017 (BGBl. I S. 2310)[337], ορίζει ότι σε συμμόρφωση με τον Κανονισμό 2252/2004 το διαβατήριο πρέπει να διαθέτει ηλεκτρονικό μέσο αποθήκευσης στο οποίο (πέραν από άλλες πληροφορίες) θα αποθηκεύονται η φωτογραφία και δύο μόνο δακτυλικά αποτυπώματα του κατόχου (§4(3) και §4(4)).

Επίσης, αξίζει να αναφερθεί πως ο γερμανικός νόμος περί διαβατηρίων προέβλεψε και ορίζει ρητά ότι δε θα δημιουργηθεί κεντρική βάση δεδομένων για την αποθήκευση των παραπάνω βιομετρικών δεδομένων (§4(3)), τα δακτυλικά αποτυπώματα που είναι αποθηκευμένα στην αρχή έκδοσης του διαβατηρίου πρέπει να διαγράφονται το αργότερο μετά την παραλαβή του διαβατηρίου από τον αιτούντα (§16(2)) και τέλος ότι τα βιομετρικά δεδομένα χρησιμοποιούνται μόνο για τον έλεγχο της γνησιότητας του διαβατηρίου και

αιτήσεων για την έκδοση των διαβατηρίων και μετέπειτα των παραδόσεων και των ανανεώσεων αυτών και κυρίως η αντιμετώπιση της πλαστογράφησης και της παραποίησης αυτών, ενώ ο χρόνος διατήρησης των προσωπικών δεδομένων ορίστηκε 15 έτη για τους ενήλικες και 10 έτη για τους ανήλικους (άρθρο 24).

[336] Καταργήθηκαν με το διάταγμα Décret n°2016-1460 du 28 octobre 2016 - art. 27, διαθέσιμο στο https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=5CE9DA1F73D124B24CBAA6C2033AAE72.tplgfr22s_2?cidTexte=JORFTEXT000033318345&idArticle=LEGIARTI000033326526&dateTexte=20161030&categorieLien=id#LEGIARTI000033326526

[337] Γερμανικός νόμος περί διαβατηρίων, Paßgesetz vom 19. April 1986 (BGBl. I S. 537), das zuletzt durch Artikel 2 des Gesetzes vom 7. Juli 2017 (BGBl. I S. 2310) geändert worden ist, διαθέσιμος στο http://www.gesetze-im-internet.de/pa_g_1986/BJNR105370986.html

την ταυτοποίηση του κατόχου και πρέπει να σβήνονται αμέσως μετά την ολοκλήρωση της εξέτασης.

2.2. Ηνωμένες Πολιτείες της Αμερικής

Μετά την επίθεση της 11ης Σεπτεμβρίου το 2001, οι Αμερικανικές αρχές άρχισαν να δίνουν ιδιαίτερη σημασία στη διασφάλιση της γνησιότητας των διαβατηρίων και των εγγράφων ταυτοποίησης προκειμένου να μπορούν να εντοπίζουν αποτελεσματικότερα τους τρομοκράτες. Οι πρώτες ενέργειες έγιναν συγκεκριμένα μετά από 8 μήνες, το Μάιο του 2002, όταν υπογράφτηκε μία μεταρρύθμιση του νόμου για την ενίσχυση της ασφάλειας των συνόρων (The Enhanced Border Security and Visa Reform Act of 2002, H.R. 3525).

Μία από τις διατάξεις του προαναφερόμενου νόμου, η οποία είναι εξέχουσας σημασίας για την ασφάλεια των συνόρων, είναι η απαίτηση όλα τα διαβατήρια και τα έγγραφα ταυτοποίησης που χρησιμοποιούνται για την είσοδο στις Ηνωμένες Πολιτείες της Αμερικής να είναι αναγνώσιμα από μηχανήματα, να μη μπορούν να αλλοιωθούν και να εμπεριέχουν βιομετρικά χαρακτηριστικά[338]. Η μεταρρύθμιση αυτή του νόμου είναι ένας από τους σημαντικότερους παράγοντες ο οποίος οδήγησε και στην υιοθέτηση της τεχνολογίας RFID στα ηλεκτρονικά διαβατήρια και στα έγγραφα ταυτοποίησης, όχι μόνο στις Ηνωμένες Πολιτείες αλλά και παγκοσμίως[339].

Τα βιομετρικά χαρακτηριστικά αποθηκεύονται σε μία κεντρική βάση δεδομένων (Consular Consolidated Database) η οποία χρησιμοποιείται από το γραφείο Προξενικών Υποθέσεων στο Υπουργείο Εξωτερικών των Ηνωμένων Πολιτειών της Αμερικής και αυτή τη στιγμή είναι μία από τις μεγαλύτερες αποθήκες δεδομένων παγκοσμίως. Η βάση αυτή περιλαμβάνει πληροφορίες όπως ονόματα, διευθύνσεις, ημερομηνίες γέννησης, βιομετρικά δεδομένα (δακτυλικά αποτυπώματα και εικόνες προσώπου), φυλή, αριθμούς

[338] Enhanced Border Security and Visa Entry Reform Act, 2002 (Public Law 107-173), Congressional and Administrative News, 2002-07, No. 5, pp. 543-565, νόμος διαθέσιμος στο https://www.congress.gov/107/plaws/publ173/PLAW-107publ173.pdf. Επίσης, για περισσότερες πληροφορίες βλ. http://cis.org/EnhancedBorderSecurityVisaReformAct2002-HR3525.

[339] Βλ. Nogueira, M., Greis, N. (2009). Uses of RFID Technology in US Identification Documents, Institute for Homeland Security Solutions.

ταυτότητας και τη χώρα προέλευσης ατόμων που ζουν στις Ηνωμένες Πολιτείες της Αμερικής και τους αιτούντες θεώρηση (visa)[340]. Συγκεκριμένα λέγεται πως διαθέτει πάνω από 290 εκατομμύρια αρχεία διαβατηρίων και 184 εκατομμύρια θεωρήσεις visa[341].

Το 2006, ο Διεθνής Οργανισμός Πολιτικής Αεροπορίας (International Civil Aviation Organization, ICAO) του οποίου η αποστολή είναι να «*ορίζει διεθνή πρότυπα και κανονισμούς που είναι απαραίτητοι για την ασφάλεια, την αποδοτικότητα και την τακτικότητα των εναέριων μεταφορών*»[342] και με την οποία συνεργάζονται οι Ηνωμένες Πολιτείες της Αμερικής[343], προέβλεψε τα πρότυπα και τους κανονισμούς για τα ηλεκτρονικά διαβατήρια με τη δυνατότητα αποθήκευσης βιομετρικών χαρακτηριστικών σε ένα κείμενο το οποίο εξελίσσεται με την πάροδο του χρόνου και προσαρμόζεται ανάλογα με τις ανάγκες που προκύπτουν (ICAO Doc 9303, 2006). Συγκεκριμένα, σχετικά με την ψηφιοποίηση και αποθήκευση των βιομετρικών χαρακτηριστικών, καθόρισε ως απαραίτητη την αποθήκευση ψηφιακής φωτογραφίας για την αναγνώριση του προσώπου, ενώ ως προαιρετική την ψηφιοποίηση του δακτυλικού αποτυπώματος και της ίριδος[344]. Επίσης, για την επίτευξη παγκόσμιας διαλειτουργικότητας καθόρισε και μία Λογική Δομή Δεδομένων (Logical Data Structure, LDS) για την αποθήκευση των υποχρεωτικών και των προαιρετικών δεδομένων σε ένα ανέπαφο ολοκληρωμένο σύστημα[345] (όπως το RFID).

Ειδικότερα, σε ένα τεχνικό κείμενό του ο Διεθνής Οργανισμός Πολιτικής Αεροπορίας[346], προβλέπει τα ελάχιστα απαιτούμενα χαρακτηριστικά τα οποία

[340] Βλ. Privacy Impact Assessment (PIA). Consular Consolidated Database (CCD), Version 4, Last Updated: July 17, 2015, διαθέσιμο στο https://www.state.gov/documents/organization/242316.pdf
[341] Βλ. https://en.wikipedia.org/wiki/Consular_Consolidated_Database#Size_estimates
[342] Για περισσότερες πληροφορίες σχετικά με τη Διεθνή Οργάνωση Πολιτικής Αεροπορίας (International Civil Aviation Organization, ICAO), βλ. http://www.unric.org/el/index.php?option=com_content&view=article&id=10372&catid=25:-----un-system-directory&Itemid=32 και http://www.icao.int/about-icao/Pages/default.aspx
[343] Για περισσότερες πληροφορίες σχετικά με τη συνεργασία των ΗΠΑ με την ICAO βλ. https://icao.usmission.gov/mission/icao/
[344] Βλ. ICAO Doc 9303 (2006), Machine readable travel documents. Specifications for electronically enabled passports with biometric identification capability, part 1, volume 2, 6th Edition, σελ. II-3.
[345] Βλ. ICAO Doc 9303 (2006), ό.π. εικόνα III-1, σελ. III-6.
[346] ICAO Technical Report (2004), Biometrics deployment of machine readable travel documents. Development and specification of globally interoperable biometric standards for machine assisted

οφείλει να καλύπτει η τεχνολογία που θα χρησιμοποιηθεί για τα εν λόγω ηλεκτρονικά διαβατήρια προκειμένου να επιτυγχάνεται υψηλή ταχύτητα, μεγάλη χωρητικότητα και υψηλή προστασία. Κατέληξε ότι τα ασύρματα ολοκληρωμένα κυκλώματα είναι τα μόνα που προσφέρουν με ασφάλεια γρήγορη, ανέπαφη και χωρίς οπτική επαφή επικοινωνία και 15-20kB χωρητικότητα. Δηλαδή μία τεχνολογία όπως η RFID.

Αξίζει να αναφερθεί πως σε ορισμένες πολιτείες της Αμερικής, οι νομοθέτες προκειμένου να προστατέψουν τους πολίτες τους από την παράνομη ανάγνωση των ταυτοτήτων τους και επομένως την παραβίαση της ιδιωτικότητάς τους, όρισαν ποινές σε πολιτειακό επίπεδο για όσους εκ προθέσεως διαβάσουν από απόσταση ένα ηλεκτρονικό έγγραφο ταυτοποίησης χωρίς την ενημέρωση και τη λήψη συγκατάθεσης του κατόχου. Συγκεκριμένα, παρατηρείται ότι στον αστικό κώδικα της Καλιφόρνια, όπως προστέθηκε το 2008, στο τμήμα 1798.79[347] (a) ορίζεται ποινή στην περίπτωση που κάποιος εκ προθέσεως διαβάσει ή προσπαθήσει να διαβάσει ένα έγγραφο προσωπικής ταυτοποίησης ενός ατόμου που χρησιμοποιεί την τεχνολογία RFID χωρίς την ενημέρωση και τη λήψη συγκατάθεσης αυτού. Αντίστοιχα στο τμήμα (b) ορίζεται ποινή στην περίπτωση που κάποιος εν γνώσει του αποκαλύψει πληροφορίες που μπορεί να βλάψουν την ακεραιότητα του λειτουργικού συστήματος. Και στις δύο περιπτώσεις, ως ποινή καθορίζεται είτε η φυλάκιση μέχρι ενός έτους, είτε χρηματική ποινή όχι μεγαλύτερη από 1.500 δολάρια, είτε και τα δύο. Επίσης, ορίζονται και εξαιρέσεις όπως στην περίπτωση όπου η ανάγνωση γίνεται για άμεση νοσηλεία σε περίπτωση καταστροφής, από επαγγελματίες υγείας για λόγους που σχετίζονται με την υγεία ή την ασφάλεια του κατόχου, εάν ο κάτοχος βρίσκεται στη φυλακή, ή είναι υπό κράτηση, ή βρίσκεται σε ψυχιατρικό κέντρο και από κυβερνητικούς υπαλλήλους προκειμένου να ταυτοποιηθεί ο κάτοχος σε περίπτωση απώλειας διαβατηρίου ή αστυνομικής έρευνας.

---

identity confirmation using machine readable travel documents, Version 2.0, ICAO TAG MRTD/NTWG, σελ. 31.

[347] Βλ. Civil Code, Title 1.80, Identification Documents [1798.79-1798.795], διαθέσιμο στο https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.80.&part=4.&chapter=&article=

Στην Ουάσιγκτον, το 2008 προστέθηκε στον Αναθεωρημένο Κώδικα της Ουάσιγκτον, στο κεφάλαιο για τα έγγραφα ταυτοποίησης, το τμήμα 9A.58.020[348], στο οποίο ορίζεται πως οποιοσδήποτε εκ προθέσεως διαβάσει από απόσταση τις πληροφορίες που είναι αποθηκευμένες σε ένα έγγραφο ταυτοποίησης ενός υποκειμένου, συμπεριλαμβανομένου του μοναδικού κωδικού ταυτοποίησης, χωρίς την ενημέρωση και συγκατάθεση αυτού, θα κριθεί ένοχος για κακούργημα τρίτου βαθμού[349]. Επίσης, στο τμήμα αυτό ορίζονται και εξαιρέσεις που αίρουν τον άδικο χαρακτήρα της πράξης όπως στην περίπτωση που η ανάγνωση γίνεται για τη διευκόλυνση διέλευσης των συνόρων, καλόπιστα για λόγους ασφαλείας, στα πλαίσια πειράματος ή επιστημονικής έρευνας, ή και ακούσια με τον όρο ότι δεν διαβιβάζονται σε τρίτους, δεν χρησιμοποιούνται για κανένα σκοπό και δεν αποθηκεύονται (καταστρέφονται αμέσως).

Στη Νεβάδα, το 2009 προστέθηκε στον Αναθεωρημένο Κώδικα της Νεβάδα, στο κεφάλαιο για τις παράνομες πράξεις σχετικά με τα έγγραφα ταυτοποίησης, το τμήμα 205.46515[350] στο οποίο ορίζεται πως οποιοσδήποτε εκ προθέσεως και με σκοπό τη διάπραξη απάτης, κλοπή ταυτότητας ή οποιασδήποτε άλλης παράνομης πράξης (a) συλλέγει, αποθηκεύει ή διαβάζει πληροφορίες με τη χρήση ραδιοσυχνοτήτων από το έγγραφο ταυτοποίησης χωρίς την ενημέρωση και προηγούμενη συγκατάθεση του κατόχου, ή (b) διατηρεί, χρησιμοποιεί ή αποκαλύπτει πληροφορίες οι οποίες γνωρίζει πως έχουν ανακτηθεί με τη χρήση ραδιοσυχνοτήτων χωρίς την ενημέρωση και προηγούμενη συγκατάθεση του κατόχου, (c) θα κριθεί ένοχος για κακούργημα τρίτου βαθμού[351].

Στην Αλαμπάμα, το 2012 προστέθηκε στον ποινικό κώδικα, στα αδικήματα που σχετίζονται με την κλοπή, στο τμήμα παραβίασης

[348] Βλ. Revised Code of Washington (RCW) 9A.58.020, διαθέσιμο στο http://app.leg.wa.gov/RCW/default.aspx?cite=9A.58.020

[349] Στην Ουάσιγκτον, τα κακουργήματα τρίτου βαθμού τιμωρούνται με ποινή φυλάκισης έως 5 έτη και χρηματική ποινή μέχρι 10.000 δολάρια, βλ. https://www.criminallawfirmseattle.com/Criminal-Defense/Felonies-Misdemeanors.aspx.

[350] Βλ. NRS 205.46515, διαθέσιμο στο https://www.leg.state.nv.us/NRS/NRS-205.html#NRS205Sec46515

[351] Στη Νεβάδα, τα κακουργήματα τρίτου βαθμού τιμωρούνται με ποινή φυλάκισης για τουλάχιστον 1 έτος έως και 5 έτη και χρηματική ποινή που δεν υπερβαίνει τα 10.000 δολάρια, εκτός εάν επιβληθεί μεγαλύτερο πρόστιμο με νόμο, βλ. https://www.leg.state.nv.us/NRS/NRS-193.html#NRS193Sec130

προσωπικών δεδομένων, το 13A-8-113[352], στο οποίο ορίζεται ότι (a1 και a2) οποιοσδήποτε εν γνώσει και εκ προθέσεως κατέχει, χρησιμοποιεί ή προσπαθήσει να χρησιμοποιήσει μία συσκευή ανάγνωσης για να αποκτήσει πρόσβαση, να διαβάσει, να ανακτήσει ή να αποθηκεύσει, είτε προσωρινά, είτε μόνιμα, αποθηκευμένες πληροφορίες, ή και να εισάγει κωδικοποιημένα δεδομένα, σε έγγραφο ταυτοποίησης με τη χρήση της τεχνολογίας RFID, (b) θα κριθεί ένοχος για κακούργημα τρίτου βαθμού[353] και (c) η συσκευή θα κατάσχεται και θα καταστρέφεται ως λαθραία (contraband).

Τέλος, στο Ιλινόις, το 2015, προστέθηκε στον ποινικό κώδικα, στα ποινικά αδικήματα που σχετίζονται με τη κλοπή ταυτότητας, το τμήμα 16-30[354] στο οποίο ορίζεται πως ένα πρόσωπο διαπράττει κλοπή ταυτότητας όταν εν γνώσει του χρησιμοποιεί, κατέχει ή μεταβιβάζει συσκευή RFID η οποία μπορεί να διαβάζει ή να επεξεργάζεται προσωπικά δεδομένα ταυτοποίησης από μία ετικέτα RFID ή έναν αναμεταδότη και θα κριθεί ένοχος για κακούργημα τρίτου βαθμού[355].

2.2.1. Real ID Act (2005)

Παράλληλα, για την καταπολέμηση της τρομοκρατίας, το 2005 ψηφίστηκε και ο ομοσπονδιακός νόμος “Real ID Act of 2005”[356] προκειμένου να βελτιωθεί η ασφάλεια των αδειών οδήγησης και των εγγράφων προσωπικής ταυτοποίησης. Ο ομοσπονδιακός αυτός νόμος αρχικά έδινε 3 χρόνια περιθώριο, έως το 2008, στις πολιτείες να συμμορφωθούν τουλάχιστον με τις ελάχιστες απαιτήσεις του νόμου, όπως τα δεδομένα που

[352] Βλ. AL Code § 13A-8-113 (2012), διαθέσιμο στο https://law.justia.com/codes/alabama/2012/title-13a/chapter-8/section-13a-8-113/

[353] Στην Αλαμπάμα, τα κακουργήματα τρίτου βαθμού τιμωρούνται με ποινή φυλάκισης τουλάχιστον ενός έτους και μίας ημέρας έως και δέκα έτη. Οι χρηματικές ποινές μπορούν να φτάσουν μέχρι και 15.000 δολάρια. Βλ. http://www.bradfordladner.net/criminal-punishment-alabama-sentences-and-fines/

[354] Βλ. 720 ILCS 5/16-30 διαθέσιμο στο http://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=072000050HArt%2E+16%2C+Subdiv%2E+15&ActID=1876&ChapterID=53&SeqStart=40100000&SeqEnd=41000000

[355] Στο Ιλινόις, τα κακουργήματα τρίτου βαθμού τιμωρούνται με ποινή φυλάκισης από 2 έως 5 έτη ή/και χρηματική ποινή έως 25.000 δολάρια. Βλ. https://andrewnickel.com/felony-illinois/

[356] REAL ID Act – Title II, improved security for drivers' licenses and personal identification cards, H.R.1268, διαθέσιμο στο https://www.dhs.gov/xlibrary/assets/real-id-act-text.pdf

πρέπει να αποθηκεύονται[357] (§202 (b), 1-8) αλλά και η τεχνολογία η οποία θα χρησιμοποιηθεί (§202 (b), 9) για την αποθήκευσή τους πρέπει να είναι διαδεδομένη και αναγνώσιμη από μηχανήματα. Ο νόμος δεν όριζε ποια τεχνολογία πρέπει να χρησιμοποιηθεί, αλλά η επικρατέστερη είναι η RFID.

Αυτό που αξίζει να τονιστεί είναι ότι με την εφαρμογή του παραπάνω ομοσπονδιακού νόμου, υπήρξαν έντονες αντιδράσεις από την πλευρά των πολιτειών, κυρίως εξαιτίας της προτεινόμενης τεχνολογίας για την εφαρμογή του. Ειδικότερα, εκφράστηκαν έντονες ανησυχίες πως η χρήση μιας τέτοιας κοινής και αναγνώσιμης από μηχανήματα τεχνολογίας καθώς και η αποθήκευση των δεδομένων σε μία βάση δεδομένων προσπελάσιμη και από άλλες πολιτείες αλλά και από την ομοσπονδιακή κυβέρνηση εμπεριέχει κινδύνους για την ιδιωτικότητα και την ασφάλεια των αποθηκευμένων δεδομένων, όπως η χρήση αυτών για άλλους σκοπούς πέρα από τους νόμιμους ή ακόμη και η κλοπή και πώληση αυτών σε τρίτους. Στον παρακάτω πίνακα (βλ. Πίνακας 16) παρουσιάζονται 24 πολιτείες οι οποίες κατά τα έτη 2007-2008 εξέδωσαν πολιτειακό νομοσχέδιο και ζήτησαν την ανάκληση του “Real ID Act of 2005” αρνούμενες να τον εφαρμόσουν[358].

[357] Βλ. REAL ID Act – Title II, ό.π. sec. 202, Minimum document requirements and issuance standards for federal recognition, (b), σελ: 1-2.

[358] Βλ. EPIC, National ID and the REAL ID Act. State Legislation Rejecting REAL ID, διαθέσιμο στο https://epic.org/privacy/id_cards/ και Ferguson, R. B. (2007). DHS confirms Real ID Act regulations coming; States rebel, διαθέσιμο στο http://www.eweek.com/c/a/Mobile-and-Wireless/DHS-Confirms-Real-ID-Act-Regulations-Coming-States-Rebel

Πίνακας 16 Νομοσχέδια πολιτειών που απέρριψαν τον REAL ID Act of 2005

α/α	Πολιτεία	Έτος	Νομοσχέδιο
1	Αλάσκα	2008	SB 202
2	Νότια Ντακότα	2008	SCR 7
3	Τένεσσι	2008	SJR 0248
4	Νότια Καρολίνα	2007	S 449
5	Νεμπράσκα	2007	LR 28
6	Νιου Χάμσαϊρ	2007	HB 685
7	Οκλαχόμα	2007	SB 464
8	Ιλινόις	2007	HJR 0027
9	Μιζούρι	2007	HCR 20
10	Νεβάδα	2007	AJR 6
11	Κολοράντο	2007	HJR 1047
12	Τζόρτζια	2007	SB 5
13	Χαβάη	2007	SCJ 31
14	Νότια Ντακότα	2007	SCR 4040
15	Ουάσινγκτον	2007	SB 5087
16	Μοντάνα	2007	HB 287
17	Αρκάνσας	2007	SCR 22
18	Αϊντάχο	2008	HB 606
19	Μέιν	2007	SP 113
20	Γιούτα	2008	HB 449
21	Λουιζιάνα	2008	HB 715
22	Βιρτζίνια	2009	SB 1431
23	Μινεσότα	2008	HF 3807
24	Αριζόνα	2008	HB 2677

Το Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ (Department of Homeland Security, DHS) απαντά[359] στις επιφυλάξεις αυτές ότι δεν πρόκειται να δημιουργηθεί μία εθνική βάση δεδομένων όπου η ομοσπονδιακή κυβέρνηση αλλά και η κάθε πολιτειακή κυβέρνηση θα έχουν πρόσβαση. Θα υπάρχει έλεγχος ποιος έχει πρόσβαση στη βάση και κάτω υπό ποιες συνθήκες επιτρέπεται η πρόσβαση.

Για όσες πολιτείες δεν είχαν συμμορφωθεί ακόμη με την εφαρμογή του νόμου, το 2013 προτάθηκε ένα σχέδιο σταδιακής εφαρμογής με το οποίο δόθηκε παράταση ανά πολιτεία.[360] Σύμφωνα με το σχέδιο αυτό, από 1

[359] Βλ. Department of Homeland Security, REAL ID and You: Rumor Control, διαθέσιμο στο https://www.dhs.gov/real-id-and-you-rumor-control

[360] Βλ. https://www.dhs.gov/real-id και https://www.dhs.gov/real-id-public-faqs

Οκτωβρίου 2020, όλοι οι πολίτες θα πρέπει να κατέχουν είτε ένα έγγραφο ταυτοποίησης που να συμμορφώνεται με το νόμο, είτε κάποιο άλλο αποδεκτό έγγραφο ταυτοποίησης, όπως το διαβατήριο, για πρόσβαση σε ομοσπονδιακές εγκαταστάσεις, είσοδο σε πυρηνικούς σταθμούς και επιβίβαση σε εμπορικά αεροσκάφη.

2.3. Συμπεράσματα σχετικά με την υπάρχουσα νομοθεσία για τη χρήση της τεχνολογίας RFID στα ηλεκτρονικά διαβατήρια

Μετά την τρομοκρατική επίθεση της 11ης Σεπτεμβρίου το 2001, δημιουργήθηκε η ανάγκη χρήσης ηλεκτρονικών διαβατηρίων με την ενσωμάτωση βιομετρικών χαρακτηριστικών όπως τα δακτυλικά αποτυπώματα και η χρήση μίας κοινής τεχνολογίας όπως η RFID για την επίτευξη της παγκόσμιας διαλειτουργικότητάς τους.

Όπως μελετήθηκε στις παραπάνω υποενότητες, στις Ηνωμένες Πολιτείες της Αμερικής, οι Αμερικανικές αρχές μετά την τρομοκρατική επίθεση ενεργοποιηθήκαν άμεσα και μέσα σε 8 μήνες προτάθηκε και υπογράφτηκε μία μεταρρύθμιση του ισχύοντα νόμου για την ενίσχυση της ασφάλειας των συνόρων η οποία απαιτεί όλα τα διαβατήρια και τα έγγραφα ταυτοποίησης που χρησιμοποιούνται για την είσοδο στις Ηνωμένες Πολιτείες της Αμερικής να είναι αναγνώσιμα από μηχανήματα, να μη μπορούν να αλλοιωθούν και να εμπεριέχουν βιομετρικά χαρακτηριστικά. Αντίστοιχα και στην Ευρωπαϊκή Ένωση, εκτιμώντας ότι απαιτείται συνεκτική προσέγγιση της ΕΕ όσον αφορά τη χρήση βιομετρικών αναγνωριστικών στοιχείων ή βιομετρικών δεδομένων σε διαβατήρια των πολιτών της ΕΕ, το 2004 εκδόθηκε ο Κανονισμός 2252/2004 σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών. Και στις δύο περιπτώσεις λοιπόν, ορίστηκε απαραίτητη η χρήση βιομετρικών χαρακτηριστικών στα διαβατήρια για την ταυτοποίηση των κατόχων και η αποθήκευση αυτών σε ανέπαφο

ολοκληρωμένο σύστημα αναγνώσιμο από μηχανήματα, όπως η τεχνολογία RFID.

Όσον αφορά τα ζητήματα που προκύπτουν από τους νομικούς περιορισμούς που έχουν τεθεί ή που είναι ανάγκη να τεθούν για την εξασφάλιση της προστασίας των προσωπικών δεδομένων του κατόχου του ηλεκτρονικού διαβατηρίου, τίθεται έντονος προβληματισμός για τη μη απαγόρευση δημιουργίας κεντρικής βάσης δεδομένων για την αποθήκευση των βιομετρικών δεδομένων. Ειδικότερα, παρατηρήθηκε πως στις Ηνωμένες Πολιτείες της Αμερικής έχει δημιουργηθεί η μεγαλύτερη βάση δεδομένων στον κόσμο στην οποία αποθηκεύονται τα στοιχεία των κατόχων διαβατηρίων των πολιτών και θεωρήσεων (visa). Ενώ και στον ευρωπαϊκό Κανονισμό δεν απαγορεύεται πουθενά η αποθήκευση των βιομετρικών στοιχείων που θα περιλαμβάνονται στα διαβατήρια και στα ταξιδιωτικά έγγραφα σε μία κεντρική βάση δεδομένων και επομένως το θέμα υπάγεται αποκλειστικά στην εθνική νομοθεσία[361]. Κάτι τέτοιο όμως παραβιάζει την αρχή του σκοπού και την αρχή της αναλογικότητας και αυξάνει τον κίνδυνο κατάχρησης των δεδομένων και για άλλους σκοπούς μη προβλεπόμενους καθώς αυξάνει και τον κίνδυνο αλίευσης αυτών.

Παράλληλα, ένα ακόμη ζήτημα εξαιρετικής σημασίας που προκύπτει από τη συλλογή των δακτυλικών αποτυπωμάτων ως το βιομετρικό χαρακτηριστικό που επιλέχτηκε για την αλάνθαστη εξακρίβωση και ταυτοποίηση των κατόχων των διαβατηρίων είναι η ανάγκη να διασφαλίζεται η ακρίβειά τους[362]. Είναι γεγονός πως τα δακτυλικά αποτυπώματα μπορεί είτε

[361] Βλ. υπ' αριθ. 17/2014, 127/2012, 57/2010, 31/2010, 56/2009, 52/2008, 50/2007, 59/2005, 39/2004, 52/2003, 9/2003 και 245/9/2000 αποφάσεις της ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων αναφορικά με τη χρήση βιομετρικών συστημάτων και την τήρηση βάσεων δεδομένων. Η Αρχή επιτρέπει την εγκατάσταση βιομετρικών συστημάτων όταν πρόκειται αποκλειστικά για ερευνητικούς σκοπούς (αφού δεν αντίκειται στις διατάξεις του ν.2472/1997), εφόσον όμως τα βιομετρικά δεδομένα που έχουν συλλεχθεί καταστραφούν στο ελάχιστο δυνατό χρονικό διάστημα που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας. Επίσης, επιτρέπει την εγκατάσταση βιομετρικών συστημάτων σε χώρους υψηλών απαιτήσεων ασφαλείας, εφόσον όμως έχει προηγηθεί ανάλυση επικινδυνότητας και έχουν ληφθεί τα κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας. Ενώ στις περιπτώσεις όπου έκρινε πως ο έλεγχος μπορεί να πραγματοποιηθεί και με άλλα ηπιότερα εναλλακτικά μέσα, όπως οι μαγνητικές κάρτες χωρίς βιομετρικά δεδομένα, αποφάνθηκε πως η εγκατάσταση ενός τέτοιου συστήματος είναι παράνομη.

[362] Βλ. Bustard, J. (2015). The Impact of EU Privacy Legislation on Biometric System Deployment.., ό.π. σελ. 9.

με την πάροδο των χρόνων να αλλοιωθούν λόγω διάφορων παραγόντων, όπως γενετικοί παράγοντες, η γήρανση, το περιβάλλον ή επαγγελματικοί λόγοι (κυρίως όσοι εκτελούν χειρωνακτικές εργασίες είναι πιθανόν να έχουν κοψίματα και μώλωπες) επομένως να μην είναι αντιπροσωπευτικά[363], είτε να συντελέσουν σε λανθασμένη ταυτοποίηση του υποκειμένου, όπως έγινε στην υπόθεση Mayfield εναντίον των Ηνωμένων Πολιτειών ο οποίος κατηγορήθηκε ότι συμμετείχε σε βομβιστική επίθεση και κρατήθηκε πάνω από δύο εβδομάδες[364]. Για τέτοιες περιπτώσεις, όπου τα δεδομένα μπορεί να μην είναι ακριβή, προτείνεται η ύπαρξη εφεδρικών συστημάτων στα σημεία όπου πραγματοποιούνται οι έλεγχοι των διαβατηρίων[365].

Επίσης, τέθηκε και ο προβληματισμός ότι δεν αποκλείεται οι κάτοχοι των ηλεκτρονικών διαβατηρίων να ενταχθούν στην κατηγορία των υπόπτων για διάπραξη εγκλημάτων, καθώς η συλλογή των δακτυλικών αποτυπωμάτων προηγουμένως χρησιμοποιούνταν για σκοπούς επιβολής του δικαίου, όπως στο πλαίσιο ανακρίσεων, και για τη διαπίστωση εγκληματικής δραστηριότητας[366].

Ακόμη, σχολιάστηκε πως προκειμένου το υποκείμενο να μπορεί να ασκήσει το δικαίωμα επαλήθευσης των δεδομένων προσωπικού χαρακτήρα που περιέχονται στο διαβατήριό του και τη δυνατότητα διόρθωσης ή απάλειψης αυτών όπως ορίζεται στο άρθρο 4 παρ. 1 του σχετικού Κανονισμού, οι Αρχές οφείλουν να παρέχουν κατάλληλους αναγνώστες και σε ευκόλως προσβάσιμα σημεία έτσι ώστε να μπορεί ανά πάσα στιγμή το υποκείμενο να έχει πρόσβαση στα δεδομένα που είναι αποθηκευμένα στην

[363] Βλ. Betzel, M. (2005). Privacy Year in Review: Recent Changes in the Law of Biometrics. ISJLP, 1, p. 522 και Παναγοπούλου-Κουτνατζή, Φ. (2013). Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας.., ό.π. σελ. 484.
[364] Βλ. Bustard, J. (2015). The Impact of EU Privacy Legislation on Biometric System Deployment.., ό.π. σελ. 14.
[365] Βλ. Ιγγλεζάκης, Ι. (2010). Ο Κανονισμός 2252/2004 για τα βιομετρικά διαβατήρια.., ό.π. σελ. 83 και Hornung G. (2007). The European Regulation on Biometric Passports: Legislative Procedures.., ό.π. 258.
[366] Βλ. Παναγοπούλου-Κουτνατζή, Φ. (2013). Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας.., ό.π. σελ. 491.

ετικέτα του διαβατηρίου του (μέσω της σάρωσης) καθώς και να μπορεί να ζητήσει τη διόρθωση ή τη διαγραφή αυτών[367].

Προβληματισμοί επίσης τίθενται και για την επιλογή της τεχνολογίας RFID, εάν όντως είναι η πιο κατάλληλη και η πιο ασφαλής για να χρησιμοποιηθεί στα ηλεκτρονικά διαβατήρια ως το μέσο αποθήκευσης των βιομετρικών δεδομένων. Ένας από τους σημαντικότερους παράγοντες ο οποίος οδήγησε στην υιοθέτηση της τεχνολογίας RFID στα ηλεκτρονικά διαβατήρια και στα έγγραφα ταυτοποίησης παγκοσμίως είναι η μεταρρύθμιση του νόμου για την ενίσχυση της ασφάλειας των συνόρων στις Ηνωμένες Πολιτείες καθώς και οι οδηγίες του ICAO σε τεχνικό του κείμενο όπου καθόρισε τα ελάχιστα απαιτούμενα χαρακτηριστικά τα οποία οφείλει να καλύπτει η τεχνολογία που θα χρησιμοποιηθεί στα ηλεκτρονικά διαβατήρια. Συγκεκριμένα, ο ICAO κατέληξε ότι τα ασύρματα ολοκληρωμένα κυκλώματα είναι τα μόνα που προσφέρουν με ασφάλεια γρήγορη, ανέπαφη και χωρίς οπτική επαφή επικοινωνία και 15-20kB χωρητικότητα, δηλαδή μία τεχνολογία όπως η RFID. Η τεχνολογία RFID ως προϋπάρχουσα τεχνολογία που αφορούσε άλλες εφαρμογές δεν σχεδιάστηκε για την προστασία των αποθηκευμένων δεδομένων των διαβατηρίων. Ίσως λοιπόν να ήταν εύλογο η δημιουργία μίας νέας μορφής τεχνολογίας η οποία από το σχεδιασμό της ακόμη θα λαμβάνει υπόψη της την προστασία της ιδιωτικότητας (privacy by design) με πρόσθετα χαρακτηριστικά ασφαλείας[368], που να αφορά τα διαβατήρια.

3. Χρήση της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου

Η χρήση της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου για τον εντοπισμό των προϊόντων είναι ιδιαίτερα ελκυστική καθώς προσφέρει πληθώρα πλεονεκτημάτων στους εμπόρους αλλά και στους καταναλωτές.

[367] Βλ. Kosta, E. (2006). The use of RFID chips on Identification Documents, ό.π., σελ. 475 και Hornung G. (2007). The European Regulation on Biometric Passports.., ό.π. σελ. 253.
[368] Βλ. Nikita, M., (2012). RFID chips and EU e-passports: the end of privacy?, ό.π.

Όσο περνάνε τα χρόνια και η τεχνολογία RFID εφαρμόζεται σε όλο και περισσότερες περιπτώσεις αναδεικνύοντας τα θετικά της χαρακτηριστικά υπέρ των καταναλωτών, τόσο και οι καταναλωτές συνηθίζουν καταρχήν στην ύπαρξη αυτής αλλά και στη χρήση της στην καθημερινή τους ζωή καθώς αναμένεται να ενσωματωθεί σε όλα τα προϊόντα.

Αυτό όμως που γεννά προβληματισμό είναι τι γίνεται στην περίπτωση που με τη χρήση της τεχνολογίας RFID συνδέεται ο ίδιος καταναλωτής με το προϊόν που αγοράζει. Χρησιμοποιώντας την τεχνολογία RFID ανά προϊόν, δίνεται η δυνατότητα στους εμπόρους να συγκεντρώνουν στοιχεία για τους καταναλωτές, να παρακολουθούν τις καταναλωτικές τους κινήσεις, να δημιουργήσουν το καταναλωτικό τους προφίλ σιωπηρά χωρίς τη συναίνεσή τους και ακόμη και να διαβιβάσουν τα στοιχεία που έχουν συγκεντρώσει σε τρίτους. Μάλιστα, εφόσον οι καταναλωτές χρησιμοποιήσουν έστω και μία φορά την πιστωτική τους κάρτα για την αγορά των προϊόντων οι έμποροι μπορούν πολύ εύκολα να συνδέσουν το καταναλωτικό τους προφίλ και με τα προσωπικά τους στοιχεία και το πρόβλημα να γίνει εντονότερο.

Για παράδειγμα, έστω πως ένας καταναλωτής έχει αγοράσει ένα προϊόν, όπως ένα ρολόι ή μία τσάντα, από ένα κατάστημα που χρησιμοποιεί την τεχνολογία RFID και δεν αφαιρεθεί η ετικέτα από το προϊόν κατά την αγορά. Όποτε αυτός ο καταναλωτής επισκέπτεται ένα οποιοδήποτε κατάστημα το οποίο έχει κατάλληλους RFID αναγνώστες φέροντας μαζί του το προϊόν αυτό, οι αναγνώστες θα μπορούν να διαβάσουν την ετικέτα του προϊόντος και να καταγράφουν στο σύστημα πως τους επισκέφτηκε ένας καταναλωτής με την τάδε ετικέτα και τι αγορές έκανε. Μετέπειτα, χρησιμοποιώντας κανόνες συσχέτισης[369], θα μπορούν να χτίζουν κάθε φορά σιγά σιγά το καταναλωτικό προφίλ των καταναλωτών σιωπηρά. Μάλιστα, το ρολόι και η τσάντα είναι χαρακτηριστικά παραδείγματα καθώς στα ρολόγια ενσωματώνουν πολλές φορές την τεχνολογία RFID μέσα στο προϊόν και την χρησιμοποιούν ως ενδεικτικό για την εγγύηση του προϊόντος και στις τσάντες ως αντικλεπτικό σύστημα. Έτσι λοιπόν, με αυτό τον τρόπο τα δεδομένα

[369] Οι κανόνες συσχέτισης είναι μία τεχνική εξόρυξης δεδομένων από βάσεις δεδομένων για τη διατύπωση σχέσεων στα δεδομένα.

γίνονται διαθέσιμα, όχι μόνο σε αυτόν που πούλησε το προϊόν, αλλά σε οποιονδήποτε κατέχει κατάλληλους RFID αναγνώστες.

Όσον αφορά τα θέματα προσβολής της ιδιωτικότητας από τη χρήση της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου, «*το κουτί της Πανδώρας*» ανοίχτηκε για πρώτη φορά το 1997 όταν ο Kevin Ashton, μάνατζερ της Protect & Gamble, χρησιμοποίησε την τεχνολογία RFID για να επιλύσει το πρόβλημα διαχείρισης των αποθεμάτων ενός πολύ δημοφιλούς προϊόντος[370].

Σε αυτό το κεφάλαιο μελετάται η σχετική νομοθεσία και οι σχετικές νομοθετικές προτάσεις και κινήσεις που έχουν γίνει αναφορικά με τη χρήση της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου για την προστασία του καταναλωτή στην Ευρωπαϊκή Ένωση και στις Ηνωμένες Πολιτείες της Αμερικής.

3.1. Ευρωπαϊκή Ένωση

Όπως έχει ήδη προαναφερθεί, στην Ευρωπαϊκή Ένωση τα βήματα για τη δημιουργία ενός αποδεκτού πλαισίου για την ορθή χρήση της τεχνολογίας RFID ξεκίνησαν από το 2005, όταν η Ομάδα εργασίας του άρθρου 29 ενέταξε για πρώτη φορά στις δραστηριότητές της την ενασχόληση με την τεχνολογία RFID στον κλάδο λιανικής. Έκτοτε ακολούθησαν πολλές δράσεις για την αντιμετώπιση των προβλημάτων ιδιωτικότητας που προκύπτουν από τη χρήση της τεχνολογίας RFID στις διάφορες εφαρμογές, συμπεριλαμβανομένου και του τομέα του λιανικού εμπορίου[371].

Επιλέγοντας τις σημαντικότερες δράσεις που επηρέασαν σημαντικά συγκεκριμένα τον τομέα του λιανικού εμπορίου, αξίζει να αναφερθεί καταρχήν η εναρμόνιση των όρων για τη διάθεση και την αποτελεσματική χρήση ραδιοφάσματος για συσκευές RFID που λειτουργούν στη ζώνη υπερύψηλων

[370] Βλ. Stein, S. G. (2007). Where Will Consumers Find Privacy Protection from RFIDS: A Case for Federal Legislation. Duke Law & Technology Review, Vol. 1, σελ. 2.

[371] Λεπτομέρειες σχετικά με τα βήματα και τις δράσεις που εκτυλίχθηκαν για τη δημιουργία ενός πλαισίου για την προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές συστημάτων RFID στον ευρωπαϊκό χώρο, παρουσιάζονται στο δεύτερο μέρος στο Κεφάλαιο 4.

συχνοτήτων (ΕΕ αριθ. L 329/64) η οποία θα βοηθήσει στην εξάπλωση της τεχνολογίας σε όλη την Ευρώπη και ο τομέας του λιανικού εμπορίου θα είναι ο πρώτος στον οποίο θα παρατηρηθούν μεγάλες αλλαγές[372]. Επίσης, αξιοσημείωτη είναι η σύσταση ομάδας εμπειρογνωμόνων για τη ραδιοσυχνική αναγνώριση (RFID Expert Group) η οποία θα συνδράμει στην ανάπτυξη του διαλόγου μεταξύ οργανώσεων των καταναλωτών, φορέων της αγοράς, και εθνικών και ευρωπαϊκών αρχών, συμπεριλαμβανομένων των αρχών προστασίας δεδομένων (ΕΕ αριθ. L 176/25).

Έπειτα, το Μάιο του 2009, η Επιτροπή εξέδωσε σύσταση (ΕΕ αριθ. L 122/47) για την εφαρμογή των αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων σε εφαρμογές όπου χρησιμοποιείται η τεχνολογία RFID. Με τη σύσταση αυτή η Επιτροπή εξέδωσε και οδηγίες για τις εφαρμογές RFID συγκεκριμένα στον τομέα του λιανικού εμπορίου. Πιο συγκεκριμένα, πρότεινε (α) την ενημέρωση των φυσικών προσώπων από τους φορείς εκμετάλλευσης βάσει μίας κοινής ευρωπαϊκής σήμανσης σχετικά με την παρουσία ετικετών που είναι τοποθετημένες ή ενσωματωμένες στα προϊόντα, (β) την εκτίμηση της πιθανότητας οι ετικέτες που είναι τοποθετημένες ή ενσωματωμένες σε προϊόντα τα οποία έχουν πωληθεί σε καταναλωτές μέσω πωλητών λιανικής να αποτελούν απειλή για την προστασία της ιδιωτικής ζωής ή των δεδομένων προσωπικού χαρακτήρα (γ) την απενεργοποίηση[373] ή την αφαίρεση των ετικετών αμέσως και χωρίς χρέωση του καταναλωτή στο σημείο πώλησης, εκτός εάν ο καταναλωτής, αφού έχει προηγουμένως ενημερωθεί με ακριβή και εύκολα κατανοητό τρόπο σχετικά με τη χρήση τους, έχει συναινέσει να τις διατηρήσει ενεργές και (δ) τη διατήρηση των ετικετών ενεργών εφόσον δεν αποτελούν απειλή για την προστασία της ιδιωτικής ζωής ή των δεδομένων. Τέλος προέβλεψε ότι (ε) η απενεργοποίηση ή η αφαίρεση των ετικετών δεν συνεπάγεται μείωση ή παύση των νομικών υποχρεώσεων των πωλητών λιανικής διάθεσης ή των κατασκευαστών απέναντι στους καταναλωτές.

[372] Βλ. δελτίο τύπου (IP/06/1808), From alarms to medical implants: Commission frees frequencies for short range wireless devices across the EU, Brussels, 14 December 2006, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-06-1808_en.htm.

[373] Ως απενεργοποίηση των ετικετών νοείται οποιαδήποτε διαδικασία διακοπής της αλληλεπίδρασης μίας ετικέτας με το περιβάλλον της χωρίς να απαιτείται η ενεργή συμμετοχή του καταναλωτή. Και ο καταναλωτής πρέπει να είναι σε θέση να επιβεβαιώνει ότι η απενεργοποίηση ή αφαίρεση συνέβη πραγματικά (ΕΕ L 122/47).

Το επόμενο και σημαντικότερο ίσως βήμα έγινε το 2011, όταν προτάθηκε, από μία άτυπη «ομάδα εργασίας RFID» με εκπροσώπους του κλάδου της βιομηχανίας, ένα πλαίσιο εκτίμησης των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID[374], το οποίο πήρε και την έγκριση της Ομάδας εργασίας του άρθρου 29 και χρησιμοποιείται μέχρι σήμερα. Το πλαίσιο αυτό χαρακτηρίστηκε από την Αντιπρόεδρο της Ευρωπαϊκής Επιτροπής, Neelie Kroes, ως το πρώτο στο είδος του στην Ευρώπη.

3.2. Ηνωμένες Πολιτείες της Αμερικής

Σε αντίθεση με την Ευρωπαϊκή Ένωση, στις Ηνωμένες Πολιτείες της Αμερικής οι αντιδράσεις στη χρήση της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου ξεκίνησαν από το 2003. Λόγω της ελλιπούς προστατευτικής νομοθεσίας για τα προσωπικά δεδομένα, οι Αμερικανοί πολίτες είναι πολύ προσεκτικοί στους κινδύνους που εγκυμονεί η χρήση της εν λόγω τεχνολογίας στην ιδιωτικότητα[375].

Οι οργανισμοί πολιτικής ελευθερίας (Civil Liberty Organizations) ήδη από το 2003 ξεκίνησαν προσπάθειες για να περιορίσουν τη χρήση RFID ετικετών στα καταναλωτικά προϊόντα λόγω των αρνητικών επιπτώσεων στην ιδιωτικότητα, όταν η «Οργάνωση των Καταναλωτών κατά της προσβολής της ιδιωτικότητας και της αριθμητικής σήμανσης» (CASPIAN), η «Αμερικανική Ένωση Πολιτικών Ελευθεριών» (ACLU) και το «Κέντρο Πληροφοριών Ηλεκτρονικού Απορρήτου» (EPIC) δημοσίευσαν μία εργασία αναφορικά με τη στάση τους απέναντι στη χρήση της τεχνολογίας[376]. Στην εργασία αυτή, οι τρεις παραπάνω οργανισμοί, σεβόμενοι τα συμφέροντα των επιχειρήσεων για τον εντοπισμό των προϊόντων στην εφοδιαστική αλυσίδα, πρότειναν μία τριπλή δράση για την προστασία των καταναλωτών από την πιθανή παρακολούθησή τους. Πρότειναν λοιπόν πρώτον να γίνει επίσημη αξιολόγηση

[374] Αναλυτικά την παρουσίαση του πλαισίου εκτίμησης των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID βλ. παραπάνω Μέρος δεύτερο, Κεφάλαιο 5.
[375] Βλ. Αλεξανδροπούλου–Αιγυπτιάδου, Ε., Μαυρίδης, Ι. (2007). Η Προστασία των Προσωπικών Δεδομένων.., ό.π. σελ. 499.
[376] Βλ. Levary, R. R., Thompson, D., Kot, K., & Brothers, J. (2005). Radio frequency identification: Legal aspects. Rich. JL & Tech., Vol. 12, σελ. 4.

της τεχνολογίας με τη συμμετοχή όλων των ενδιαφερομένων μερών μαζί με τους καταναλωτές, δεύτερον η εφαρμογή της τεχνολογίας RFID να ακολουθεί τις Πρακτικές Δίκαιης Πληροφόρησης (Fair Information Practices) και τρίτον να απαγορευτούν ορισμένες πρακτικές χρήσης της.

Όσον αφορά το δεύτερο στάδιο, την εξατομίκευση των Πρακτικών Δίκαιης Πληροφόρησης στην περίπτωση της χρήσης της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου, πρότειναν κάποιες ελάχιστες κατευθυντήριες γραμμές βασισμένες στις αρχές αυτές και στις οδηγίες προστασίας προσωπικών δεδομένων του Ο.Ο.Σ.Α[377]. Συγκεκριμένα πρότειναν τις εξής εξατομικευμένες αρχές:

- διαφάνεια, δηλαδή οι φορείς εκμετάλλευσης της τεχνολογίας RFID οφείλουν να κοινοποιούν τις πολιτικές και τις πρακτικές που χρησιμοποιούν και αφορούν τη χρήση και τη συντήρηση των συστημάτων RFID και δεν πρέπει να διατηρούν μυστικές βάσεις δεδομένων. Οι καταναλωτές έχουν το δικαίωμα να γνωρίζουν πότε τα προϊόντα φέρουν ετικέτες RFID και τις τεχνικές προδιαγραφές αυτών. Η σήμανση πρέπει να είναι εμφανής και κατανοητή. Κάθε ανάγνωση ετικέτας RFID που λαμβάνει χώρα πρέπει να είναι διαφανής σε όλα τα ενδιαφερόμενα μέρη και δε θα πρέπει να συμβαίνει ποτέ καμία μυστική ανάγνωση.
- Προσδιορισμό του σκοπού, δηλαδή οι φορείς εκμετάλλευσης της τεχνολογίας RFID οφείλουν να προσδιορίσουν το σκοπό για τον οποίο χρησιμοποιούν τις ετικέτες RFID αλλά και τους αναγνώστες.
- Περιορισμό της συλλογής των δεδομένων, δηλαδή η συλλογή των δεδομένων πρέπει να περιορίζεται μονάχα στα αναγκαία για το συγκεκριμένο σκοπό.
- Λογοδοσία, θα πρέπει να θεσπιστεί ένας μηχανισμός λογοδοσίας. Οι φορείς εκμετάλλευσης της τεχνολογίας είναι υπεύθυνοι για την εφαρμογή της τεχνολογίας και των συσχετιζόμενων δεδομένων και είναι νομικά υπεύθυνοι για τη συμμόρφωση με τις εν λόγω αρχές. Ενώ

[377] Βλ. OECD Privacy Framework (2013), σελ. 14-15, διαθέσιμο στο http://www.oecd.org/internet/ieconomy/oecd_privacy_framework.pdf

πρέπει να υπάρχουν και φορείς, τόσο στη βιομηχανία όσο και στη κυβέρνηση, στους οποίους οι καταναλωτές θα μπορούν να υποβάλλουν τα παράπονά τους σε περιπτώσεις παραβιάσεων αυτών των διατάξεων.

- Ασφάλεια, δηλαδή εξασφάλιση των απαραίτητων μέτρων ασφαλείας για τη διασφάλιση της ακεραιότητας των δεδομένων κατά τη μετάδοση, στις βάσεις δεδομένων και στη πρόσβαση στο σύστημα. Μάλιστα, τα μέτρα αυτά θα πρέπει να αξιολογούνται από τρίτους έξω από την επιχείρηση και η αξιολόγηση να δημοσιευτεί.

Αναφορικά με το τρίτο στάδιο, την απαγόρευση ορισμένων πρακτικών από τη χρήσης της τεχνολογίας RFID, πρότειναν κάποιους περιορισμούς αλλά και παρέθεσαν και κάποια παραδείγματα αποδεκτών χρήσεών της. Οι περιορισμοί που πρότειναν είναι οι παρακάτω:

- την απαγόρευση των φορέων εκμετάλλευσης της τεχνολογίας να εξαναγκάζουν τους πελάτες τους να δέχονται είτε ενεργές, είτε ανενεργές ετικέτες RFID να παραμένουν προσκολλημένες στο προϊόντα αφού τα αγοράσουν,
- να δίνεται η δυνατότητα στους καταναλωτές να εντοπίζουν τους αναγνώστες και τις ετικέτες RFID και να τις αφαιρούν από μόνοι τους στα προϊόντα που αγοράζουν,
- η τεχνολογία RFID δεν πρέπει να χρησιμοποιείται για τον εντοπισμό των ατόμων εφόσον δεν έχουν ενημερωθεί και δεν έχουν δώσει γραπτή συγκατάθεση, καθώς η παρακολούθηση των ατόμων είτε άμεσα, είτε έμμεσα μέσω καταναλωτικών αγαθών και άλλων αντικειμένων δεν επιτρέπεται, και τέλος
- η τεχνολογία RFID δεν πρέπει ποτέ να εφαρμοστεί με τέτοιο τρόπο ώστε να εξαλείφει την ανωνυμία, όπως για παράδειγμα δεν πρέπει να ενσωματωθεί στα νομίσματα.

Παραδείγματα αποδεκτών χρήσεων της τεχνολογίας οι οποίες προσφέρουν σημαντικά πλεονεκτήματα υπέρ των καταναλωτών και των

οποίων η ιδιωτικότητα δεν κινδυνεύει εφόσον οι ετικέτες RFID είναι απενεργοποιημένες:

- η παρακολούθηση των φαρμακευτικών προϊόντων από το σημείο παρασκευής τους μέχρι το σημείο διανομής τους. Οι ετικέτες RFID μπορούν να βοηθήσουν σημαντικά στην αντιμετώπιση των ψευδεπίγραφων (counterfeit) φαρμάκων και να εξασφαλίσουν τη σωστή διαχείριση και διανομή τους, ενώ πρέπει να αφαιρούνται ή να απενεργοποιούνται πριν φτάσουν στα χέρια των καταναλωτών.
- Η παρακολούθηση των βιομηχανικών προϊόντων από τη στιγμή κατασκευής τους μέχρι να τοποθετηθούν στο ράφι προς πώληση. Οι ετικέτες RFID μπορούν να διασφαλίσουν ότι τα προϊόντα δε θα χαθούν ούτε θα κλαπούν κατά τη μετακίνησή τους μέσω της αλυσίδας εφοδιασμού. Σε αυτή την περίπτωση οι ετικέτες RFID πρέπει να βρίσκονται στο εξωτερικό τμήμα του προϊόντος και όχι σε μη ορατό σημείο και να αφαιρούνται πριν έρθει σε επαφή ο καταναλωτής με το προϊόν.
- Η παρακολούθηση αντικειμένων που φέρουν τοξικές ουσίες κατά την παράδοσή τους στο χώρο ταφής τους. Βέβαια σε αυτές τις περιπτώσεις οι ετικέτες RFID δεν είναι απαραίτητο να περιέχουν δεδομένα ανάγνωσης σε επίπεδο αντικειμένου, παρά μόνο ένα πιο γενικό μήνυμα ανακύκλωσης ή διάθεσης αποβλήτων.

Την ίδια χρονιά, η πρώτη και η μοναδική σε ομοσπονδιακό επίπεδο, νομοθετική προσπάθεια έγινε όταν η «Οργάνωση των Καταναλωτών κατά της προσβολής της ιδιωτικότητας και της αριθμητικής σήμανσης» (Consumer Against Supermarket Privacy Invasion and Numbering, CASPIAN)[378] κατέθεσε πρόταση ομοσπονδιακού νόμου γνωστή ως «RFID Right to Know

[378] Η CASPIAN είναι μία ομάδα προστασίας καταναλωτών η οποία ιδρύθηκε το 1999 με σκοπό την εκπαίδευση των καταναλωτών και τη δημιουργία καταναλωτικών συνηθειών που να προάγουν την προστασία της ιδιωτικότητας τους. Η χρήση προνομιακών καρτών σουπερ μάρκετ είναι μία από τις στρατηγικές μάρκετινγκ την οποία καταδικάζουν καθώς πληροφορίες σχετικά με προσωπικές λεπτομέρειες της ζωής μας, όπως το φαγητό που καταναλώνουμε, δεν πρέπει να αποθηκεύονται σε μία βάση δεδομένων και να υπόκεινται σε έλεγχο. Βλ. http://www.nocards.org/press/overview.shtml

Act of 2003»[379]. Σε αυτή την πρόταση νόμου προτάθηκε η εισαγωγή τριών απαιτήσεων για την αντιμετώπιση των προβλημάτων στην ιδιωτικότητα. Καταρχήν να απαιτείται στα προϊόντα που φέρουν ετικέτες RFID να υπάρχει ειδική σήμανση-ένδειξη (π.χ. μία ετικέτα) η οποία να δηλώνει το γεγονός αυτό. Συγκεκριμένα, η σήμανση αυτή πρέπει (α) να δηλώνει ότι η ετικέτα RFID που φέρει το συγκεκριμένο προϊόν μπορεί να μεταβιβάσει πληροφορίες ταυτοποίησης σε οποιοδήποτε ανεξάρτητο αναγνώστη, πριν και μετά την αγορά του προϊόντος και (β) να έχει τέτοιο μέγεθος και τύπο, να είναι τοποθετημένη σε τέτοιο σημείο και να έχει τέτοιο χρώμα ώστε να έρχεται σε αντίθεση με το φόντο του προϊόντος και να είναι εμφανής.

Δεύτερον, για την προστασία της ιδιωτικότητας των καταναλωτών προτάθηκαν μεταρρυθμίσεις και για τον περιορισμό της χρήσης της τεχνολογίας από τις επιχειρήσεις. Συγκεκριμένα, να μην επιτρέπεται οι επιχειρήσεις να συνδέουν ή να συνδυάζουν τα δεδομένα μιας ετικέτας RFID για άλλους σκοπούς πέρα από τη διευκόλυνση της διαχείρισης των αποθεμάτων, να μη μεταβιβάζουν τα δεδομένα αυτά σε τρίτους και να μη χρησιμοποιούν την τεχνολογία RFID για την ταυτοποίηση προσώπων.

Και τέλος, προτάθηκε και η εισαγωγή μεταρρυθμίσεων για την ορθή ενημέρωση των καταναλωτών και των επιχειρήσεων. Πιο συγκεκριμένα, προτάθηκε η δημιουργία και δημοσίευση εγγράφων με σκοπό την ενημέρωση των καταναλωτών, τα οποία θα περιγράφουν την τεχνολογία RFID και πώς μπορεί να χρησιμοποιηθεί από τις επιχειρήσεις, τους εμπόρους και τις κυβερνητικές υπηρεσίες για τη συλλογή προσωπικών δεδομένων. Και η δημιουργία και δημοσίευση εγγράφων με σκοπό την ενημέρωση των επιχειρήσεων, τα οποία θα υποστηρίζουν την προστασία της ιδιωτικότητας και θα εξηγούν στις επιχειρήσεις τι πρέπει να κάνουν για να συμμορφώνονται με τις διατάξεις του νόμου.

[379] Ο προτεινόμενος ομοσπονδιακός νόμος προτείνει την εισαγωγή σχετικών παραγράφων στον κώδικα των ΗΠΑ στους εξής τίτλους και παραγράφους: 15 U.S.C. §1453 (Fair Packaging and Labeling Program), 21 U.S.C. §321, §343, §352, §362 (Federal Food, Drug, and Cosmetic Act Relating to Misbranding), 27 U.S.C. §215 (Federal Alcohol Administration Act), 15 U.S.C. §1333 (Federal Cigarette Labeling and Advertising Act) και 15 U.S.C. Chapter 94 (Privacy of Title 15 of the U.S. Code), βλ. Al Malkawi M. H., Abussaud A. M. (2005) CPE542 Project, Security over the RFID, Appendix A, σελ: 17-21, διαθέσιμο στο http://www.just.edu.jo/~tawalbeh/cpe542/project/r10.pdf.

Επειδή όμως τελικά σε ομοσπονδιακό επίπεδο δεν κατέστη δυνατό να θεσπιστεί κάποια νομοθετική ρύθμιση για τη χρήση της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου, σε πολλές πολιτείες της Αμερικής έγιναν νομοθετικές προτάσεις οι οποίες προτείνουν παρόμοιες μεταρρυθμίσεις με αυτές του προαναφερόμενου προτεινόμενου νόμου προκειμένου να προστατέψουν τους πολίτες τους ως καταναλωτές σε πολιτειακό επίπεδο και μάλιστα φέρουν το ίδιο όνομα «RFID Right to Know Act». Ενώ σε κάποιες πολιτείες οι προτεινόμενες νομοθετικές προτάσεις μπορεί να διαφέρουν λίγο, άλλες να είναι πιο αυστηρές και άλλες πιο ήπιες, όπως θα δούμε παρακάτω, ο στόχος τους όμως σε όλες τις περιπτώσεις των προτεινόμενων νομοσχεδίων είναι η προστασία της ιδιωτικότητας των καταναλωτών και η αποφυγή καταχρήσεων της τεχνολογίας.

Η Γιούτα και το Μισούρι, ήταν από τις πρώτες πολιτείες που προσπάθησαν να περάσουν σε πολιτειακό επίπεδο νομοσχέδιο το οποίο πρότεινε μεταρρυθμίσεις παρόμοιες με τον προτεινόμενο ομοσπονδιακό. Συγκεκριμένα, η Γιούτα τον Ιανουάριο του 2004 με το νομοσχέδιο H.B. 251[380] και το Μισούρι τον Αύγουστο του 2004 με το νομοσχέδιο S.B. 867[381], πρότειναν τα προϊόντα που φέρουν την τεχνολογία RFID η οποία μπορεί να αναμεταδώσει πληροφορίες μέσω ενός αναγνώστη και πριν και μετά την αγορά του προϊόντος, να έχουν και μία ετικέτα που να δηλώνει την ύπαρξή της και η ετικέτα αυτή θα πρέπει να έχει τέτοιο μέγεθος, να είναι τοποθετημένη σε τέτοιο σημείο και εκτυπωμένη σε τέτοιο φόντο ώστε να ξεχωρίζει. Στην περίπτωση της Γιούτα ορίζεται πως σε κάθε αντίθετη περίπτωση οι έμποροι θα κατηγορηθούν για τη διάπραξη παραπλανητικής πράξης (deceptive act or practice by supplier). Όμως, οι παραπάνω προτεινόμενοι πολιτειακοί νόμοι είχαν την ίδια τύχη με τον προτεινόμενο ομοσπονδιακό και δεν εγκρίθηκαν.

Την ίδια χρονιά το Φεβρουάριο, στην Καλιφόρνια κατατέθηκε σχετικό νομοσχέδιο το οποίο υποχρέωνε τους φορείς εκμετάλλευσης της τεχνολογίας RFID να έχουν τη γραπτή συγκατάθεση του υποκειμένου πριν τη συλλογή

[380] Βλ. H.B. 251 (2004) «Radio Frequency Identification – Right to Know Act», διαθέσιμο στο https://le.utah.gov/~2004/bills/hbillint/HB0251.htm

[381] Βλ. S.B. 867 (2004) «RFID Right to Know Act of 2004», διαθέσιμο στο https://www.senate.mo.gov/04info/billtext/intro/sb867.htm

δεδομένων ταυτοποίησής του και πριν τη διαβίβαση αυτών σε τρίτους, την εξασφάλιση πρόσβασης και δυνατότητας διόρθωσης αυτών από τα υποκείμενα, την τήρηση των απαραίτητων μέτρων ασφαλείας καθώς και την υποχρέωση αφαίρεσης ή καταστροφής της ετικέτας πριν ο καταναλωτής φύγει από το κατάστημα. Παρότι το προτεινόμενο νομοσχέδιο τροποποιήθηκε[382] σε πιο ήπια μορφή[383], τελικά απορρίφθηκε με 8 αρνητικές ψήφους, καμία θετική ψήφο και 5 λευκές ψήφους.

Στο Νέο Μεξικό, τον Ιανουάριο του 2005 κατατέθηκε το νομοσχέδιο H.B. 215[384] το οποίο πέρα από την απαίτηση για τη σήμανση των προϊόντων που φέρουν την τεχνολογία RFID με ετικέτα η οποία θα είναι τοποθετημένη σε τέτοιο σημείο, μέγεθος και χρώμα ώστε να ξεχωρίζει και την αφαίρεση ή απενεργοποίηση των ετικετών RFID στο σημείο αγοράς με κόστος της επιχείρησης, προτείνει και την τοποθέτηση προειδοποιητικής πινακίδας σε κάθε είσοδο της επιχείρησης σε απόσταση όχι μεγαλύτερη από 10 πόδια (περίπου 3 μέτρα), στο ύψος των ματιών ώστε να είναι αναγνώσιμη από έναν μέσο αναγνώστη σε απόσταση 10 ποδιών (περίπου 3 μέτρων) και η οποία, εκτός άλλων, θα δηλώνει πως η επιχείρηση διαθέτει προϊόντα με RFID ετικέτες και υποχρεούται να τις αφαιρέσει ή να τις απενεργοποιήσει[385]. Επίσης, ορίζει ότι η επιχείρηση έχει την υποχρέωση, εφόσον συγκεντρώνει προσωπικά δεδομένα με τη χρήση ετικετών RFID, κατόπιν έγγραφου αιτήματος, να δίνει πρόσβαση στους ενδιαφερομένους στα αποθηκευμένα αυτά δεδομένα που τους αφορούν, καθώς και ότι δεν πρέπει να εξαναγκάζει τους καταναλωτές να κρατούν ενεργές τις ετικέτες RFID προκειμένου να μπορούν να επιστρέψουν το προϊόν εφόσον χρειαστεί και ούτε να τις

[382] Επίσης, βλ. τροποποιήσεις νομοσχεδίου S.B. 1834 «Radio frequency identification systems», διαθέσιμες στο https://leginfo.legislature.ca.gov/faces/billVersionsCompareClient.xhtml?bill_id=200320040SB1834&cversion=20030SB183499INT

[383] Βλ. Αλεξανδροπούλου–Αιγυπτιάδου, Ε., Μαυρίδης, Ι. (2007). Η Προστασία των Προσωπικών Δεδομένων.., ό.π. σελ. 499.

[384] Βλ. H.B. 215 (2005) «Radio Frequency Identification Right to Know Act», διαθέσιμο στο https://www.nmlegis.gov/Legislation/Legislation?Chamber=H&LegType=B&LegNo=215&year=05

[385] Το προτεινόμενο κείμενο για την προειδοποιητική πινακίδα είναι «This business carries items with radio frequency identification tags. New Mexico law requires that this business remove or disable all radio frequency identification tags before tagged items leave this business and requires this business to provide consumers, on request, with personal information gathered within the business. To file a request for personal information gathered on you through radio frequency identification tags used in this business, please contact the manager of this business», βλ. H.B. 215, ό.π. Section 3(A).

ενεργοποιεί χωρίς τη ρητή συγκατάθεσή τους. Το εν λόγω, αρκετά αυστηρό νομοσχέδιο αναβλήθηκε επ' αόριστον.

Στη Νέα Υόρκη, το 2009 προτάθηκαν δύο νομοσχέδια, το A.B. 274[386] το οποίο ορίζει απαραίτητη τη σήμανση με ετικέτες των προϊόντων που φέρουν την τεχνολογία RFID οι οποίες είναι τοποθετημένες σε εμφανή θέση και εκτυπωμένες σε τέτοιο μέγεθος και φόντο ώστε να ξεχωρίζουν και το S. 08196[387] το οποίο, πέρα από την υποχρεωτική σήμανση, ορίζει για κάθε κατάστημα λιανικής πώλησης, το οποίο χρησιμοποιεί την τεχνολογία RFID, να ενημερώνει σχετικά τους καταναλωτές, να αφαιρεί ή να απενεργοποιεί με δικό του κόστος όλες τις ετικέτες RFID πριν την έξοδο του καταναλωτή από το κατάστημα και να παρέχει τη δυνατότητα στους καταναλωτές, κατόπιν αιτήματος, τη δυνατότητα πρόσβασης στα αποθηκευμένα δεδομένα στην ετικέτα. Για μία ακόμη φορά όμως κανένα από τα προτεινόμενα νομοσχέδια δεν εγκρίθηκε.

Και στην Ουάσιγκτον, το 2009 προτάθηκαν δύο νομοσχέδια, το H.B. 1006[388] το οποίο ορίζει υποχρεωτική τη σήμανση των προϊόντων που φέρουν την τεχνολογία RFID με ένα παγκοσμίως αποδεκτό σύμβολο, εκτός και εάν αφαιρείται ή απενεργοποιείται η ετικέτα RFID από το προϊόν και το H.B. 1011[389] το οποίο ρυθμίζει τη χρήση συσκευών ταυτοποίησης γενικότερα, ορίζει απαραίτητη τη ρητή συγκατάθεση των υποκειμένων, την οποία ανά πάσα στιγμή θα μπορούν να ανακαλέσουν. Έτσι θα μπορεί μία κυβερνητική υπηρεσία ή μία επιχείρηση να συλλέγει, χρησιμοποιεί ή αποθηκεύει σχετικά με το υποκείμενο δεδομένα με σκοπό να ολοκληρώσει μία συναλλαγή πώλησης ή να του παρέχει μία υπηρεσία.

---

[386] Βλ A. 274 (2009) «An act to amend the general business law, in relation to requiring the labeling of retail products or packages containing a radio frequency identification tag», διαθέσιμο στο https://assembly.state.ny.us/leg/?default_fld=&leg_video=&bn=AB274&term=2009&Summary=Y&Actions=Y&Text=Y

[387] Βλ. S. 08196 (2010) «An act to amend the general business law, in relation to regulating the use of radio frequency identification tags by retail mercantile establishments», διαθέσιμο στο https://assembly.state.ny.us/leg/?default_fld=&leg_video=&bn=S08196&term=2009&Summary=Y&Actions=Y&Text=Y

[388] Βλ. H.B. 1006 (2009) «An act relating to labeling identification devices», διαθέσιμο στο http://lawfilesext.leg.wa.gov/biennium/2009-10/Pdf/Bills/House%20Bills/1006.pdf

[389] Βλ. H.B. 1011 (2009) «An act relating to regulating the use of identification devices», διαθέσιμο στο http://lawfilesext.leg.wa.gov/biennium/2009-10/Pdf/Bills/House%20Bills/1011.pdf

Τέλος, το πιο πρόσφατο προτεινόμενο νομοσχέδιο προτάθηκε στο Τεννεσί το Μάρτιο του 2013. Ειδικότερα, με το S.B. 929[390] προτείνεται η εισαγωγή ρύθμισης στο νόμο για την προστασία των καταναλωτών η οποία θα ορίζει ότι η τεχνολογία RFID θα μπορεί να χρησιμοποιηθεί μόνο ως αντικλεπτικό σύστημα σε καταναλωτικά προϊόντα και θα πρέπει να αφαιρείται στο σημείο αγοράς. Ενώ σε περίπτωση παραβίασης, οι παραβάτες θα κριθούν ένοχοι για πλημμέλημα δεύτερου βαθμού[391], δηλαδή μέχρι 6 μήνες φυλάκιση ή/και χρηματική ποινή 500 δολάρια.

Συνοψίζοντας, λαμβάνοντας υπόψη όλες τις παραπάνω περιπτώσεις σε ομοσπονδιακό επίπεδο και ανά πολιτεία, προτάθηκαν τα εξής:

- η επίσημη αξιολόγηση της τεχνολογίας με τη συμμετοχή όλων των ενδιαφερομένων μερών,
- η εξασφάλιση των απαραίτητων μέτρων ασφαλείας για τη διασφάλιση της ακεραιότητας των δεδομένων κατά τη μετάδοση, τη διατήρησή τους στις βάσεις δεδομένων και κατά την πρόσβαση στο σύστημα,
- ο προσδιορισμός του σκοπού για τον οποίο χρησιμοποιούν τις ετικέτες RFID και τους αναγνώστες,
- ο περιορισμός της συλλογής των δεδομένων μονάχα στα αναγκαία για το συγκεκριμένο σκοπό,
- η θέσπιση μηχανισμών λογοδοσίας
    - οι φορείς εκμετάλλευσης της τεχνολογίας είναι νομικά υπεύθυνοι για τη συμμόρφωση με τις νομικές ρυθμίσεις
    - πρέπει να υπάρχουν και φορείς, τόσο στη βιομηχανία όσο και στη κυβέρνηση, στους οποίους οι καταναλωτές θα μπορούν να υποβάλλουν τα παράπονά τους σε περιπτώσεις παραβιάσεων

[390] Βλ. S.B. 929 (2013), διαθέσιμο στο http://www.capitol.tn.gov/bills/108/Bill/HB1176.PDF

[391] Βλ. Fiscal Note S.B. 929 – H.B. 1176, διαθέσιμο στο http://www.capitol.tn.gov/bills/108/Fiscal/SB0929.PDF. Σχετικά με τις ποινές σε περιπτώσεις πλημμελημάτων βλ. https://www.davis-hoss.com/State-Cases/Misdemeanors.aspx

- η εξασφάλιση πρόσβασης στους ενδιαφερομένους στα αποθηκευμένα δεδομένα που τους αφορούν αλλά και δυνατότητας διόρθωσης αυτών,
- η εξασφάλιση διαφάνειας με τους παρακάτω μηχανισμούς, καθώς οι καταναλωτές έχουν το δικαίωμα να γνωρίζουν πότε τα προϊόντα φέρουν ετικέτες RFID και τις τεχνικές προδιαγραφές αυτών:
    - να υπάρχει ειδική σήμανση-ένδειξη (π.χ. μία ετικέτα), ένα παγκοσμίως αποδεκτό σύμβολο, το οποίο να δηλώνει ότι η ετικέτα RFID που φέρει το συγκεκριμένο προϊόν μπορεί να μεταβιβάσει πληροφορίες ταυτοποίησης σε οποιοδήποτε ανεξάρτητο αναγνώστη, πριν και μετά την αγορά του προϊόντος, να έχει τέτοιο μέγεθος και τύπο, να είναι τοποθετημένη σε τέτοιο σημείο και να έχει τέτοιο χρώμα ώστε να έρχεται σε αντίθεση με το φόντο του προϊόντος και να είναι εμφανής,
    - οι φορείς εκμετάλλευσης της τεχνολογίας RFID να κοινοποιούν τις πολιτικές και τις πρακτικές που χρησιμοποιούν και αφορούν τη χρήση και τη συντήρηση των συστημάτων RFID
- η υποχρέωση αφαίρεσης ή καταστροφής της ετικέτας πριν ο καταναλωτής φύγει από το κατάστημα με κόστος της επιχείρησης,
- η τοποθέτηση προειδοποιητικής πινακίδας σε κάθε είσοδο της επιχείρησης σε απόσταση όχι μεγαλύτερη από 10 πόδια (περίπου 3 μέτρα), στο ύψος των ματιών ώστε να είναι αναγνώσιμη από έναν μέσο αναγνώστη σε απόσταση 10 ποδιών (περίπου 3 μέτρων) και η οποία, εκτός άλλων, θα δηλώνει πως η επιχείρηση διαθέτει προϊόντα με RFID ετικέτες και υποχρεούται να τις αφαιρέσει ή να τις απενεργοποιήσει,
- ο περιορισμός της χρήσης της τεχνολογίας RFID και η απαγόρευση ορισμένων πρακτικών από τις επιχειρήσεις, όπως:
    - να μην επιτρέπεται οι επιχειρήσεις να συνδέουν ή να συνδυάζουν τα δεδομένα μιας ετικέτας RFID για άλλους

σκοπούς πέρα από τη διευκόλυνση της διαχείρισης των αποθεμάτων,

- να μη γίνεται ανάγνωση εν αγνοία των υποκειμένων,
- να μη διατηρούν μυστικές βάσεις δεδομένων,
- να μη μεταβιβάζουν τα δεδομένα αυτά σε τρίτους χωρίς τη γραπτή συγκατάθεση των υποκειμένων ,
- να μη χρησιμοποιούν την τεχνολογία RFID για την ταυτοποίηση προσώπων,
- να μη χρησιμοποιούν την τεχνολογία RFID για τον εντοπισμό των ατόμων είτε άμεσα, είτε έμμεσα μέσω καταναλωτικών αγαθών και άλλων αντικειμένων εφόσον τα υποκείμενα δεν έχουν ενημερωθεί και δεν έχουν δώσει γραπτή συγκατάθεση,
- να μην εξαναγκάζουν τους πελάτες τους να δέχονται είτε ενεργές, είτε ανενεργές τις ετικέτες RFID να παραμένουν προσκολλημένες στο προϊόντα αφού τα αγοράσουν φέροντας ως δικαιολογία ότι είναι απαραίτητες για την εγγύηση του προϊόντος,
- να δίνουν τη δυνατότητα στους καταναλωτές να εντοπίζουν τους αναγνώστες και τις ετικέτες RFID και να τις αφαιρούν από μόνοι τους από τα προϊόντα που αγοράζουν,

- η ορθή ενημέρωση των καταναλωτών και των επιχειρήσεων με τους εξής τρόπους:
  - δημιουργία και δημοσίευση εγγράφων με σκοπό την ενημέρωση των καταναλωτών, τα οποία θα περιγράφουν την τεχνολογία RFID και πώς μπορεί να χρησιμοποιηθεί από τις επιχειρήσεις, τους εμπόρους και τις κυβερνητικές υπηρεσίες για τη συλλογή προσωπικών δεδομένων και
  - δημιουργία και δημοσίευση εγγράφων με σκοπό την ενημέρωση των επιχειρήσεων, τα οποία θα υποστηρίζουν την προστασία της ιδιωτικότητας και θα εξηγούν στις επιχειρήσεις τι πρέπει να κάνουν για να συμμορφώνονται με τις διατάξεις του νόμου

- η μη εφαρμογή της τεχνολογίας RFID με τέτοιο τρόπο ώστε να εξαλείφει την ανωνυμία, όπως για παράδειγμα να μην ενσωματωθεί ποτέ στα νομίσματα
- ο καθορισμός προστίμων

Ολοκληρώνοντας, από όλα τα παραπάνω είναι φανερό πως στις Ηνωμένες Πολιτείες της Αμερικής απασχολούν έντονα τα ενδιαφερόμενα μέρη οι επιπτώσεις στην ιδιωτικότητα από τη χρήση της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου και γι' αυτό έχουν προταθεί πολλά μέτρα αντιμετώπισης, κανένα όμως από τα οποία δεν έχει νομοθετηθεί μέχρι σήμερα. Επίσης αξίζει να αναφερθεί πως παρατηρήθηκε ότι υπάρχουν και αρκετά γραφεία δικηγόρων τα οποία εξειδικεύονται επί του θέματος, γεγονός που αποδεικνύει πως οι πολίτες αντιδρούν και προσφεύγουν στη δικαιοσύνη για την προστασία τους.

3.3. Συμπεράσματα σχετικά με την υπάρχουσα νομοθεσία για τη χρήση της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου

Η εφαρμογή της τεχνολογίας RFID ανά τεμάχιο είναι ένα ζήτημα το οποίο έχει ήδη αρχίσει και απασχολεί έντονα το νομοθέτη στον ευρωπαϊκό χώρο αλλά και στις Ηνωμένες Πολιτείες της Αμερικής. Είναι ένα φαινόμενο το οποίο έχει λάβει μεγάλη έκταση, πλέον πολλά προϊόντα φέρουν την τεχνολογία RFID σε επίπεδο τεμαχίου καθώς αυτό φέρει ισχυρά οικονομικά οφέλη στη βιομηχανία. Το ζήτημα που εγείρεται είναι πώς μπορεί να προστατευτεί ο καταναλωτής στη περίπτωση που με τη χρήση της τεχνολογίας RFID συνδέεται ο ίδιος με το προϊόν.

Ήδη από το 2002 είχε προταθεί[392] μία κωδικοποίηση των δικαιωμάτων των καταναλωτών σχετικά με τη χρήση της τεχνολογίας RFID, η οποία είχε τη μορφή κατευθυντήριων οδηγιών προς τις επιχειρήσεις. Σύμφωνα με αυτή, οι

[392] Βλ. Garfinkel S. (2002). An RFID Bill of Rights, MIT Technology Review, διαθέσιμο στο https://www.technologyreview.com/s/401660/an-rfid-bill-of-rights/ και Αλεξανδροπούλου–Αιγυπτιάδου, Ε., Μαυρίδης, Ι. (2007). Η Προστασία των Προσωπικών Δεδομένων.., ό.π. σελ: 499.

καταναλωτές έχουν το δικαίωμα να γνωρίζουν εάν τα προϊόντα φέρουν ετικέτες RFID, να αφαιρούν ή να απενεργοποιούν τις ετικέτες όταν προβούν στην αγορά του προϊόντος, να χρησιμοποιούν υπηρεσίες RFID χωρίς ετικέτες RFID, να έχουν πρόσβαση στα δεδομένα που έχουν αποθηκευτεί σε μία ετικέτα RFID καθώς και να γνωρίζουν πότε, που και γιατί διαβάζεται το περιεχόμενο μίας ετικέτας. Πρότεινε δηλαδή τα παραπάνω δικαιώματα να μην είναι υποχρεωτικά βάσει νόμου, αλλά να αποτελέσουν νομικό πλαίσιο αυτορρύθμισης για τους φορείς εκμετάλλευσης της τεχνολογίας και σε οποιαδήποτε αντίθετη περίπτωση μη εφαρμογής αυτών οι καταναλωτές θα μπορούν να μποϋκοτάρουν τις συγκεκριμένες επιχειρήσεις.

Μελετώντας χρονολογικά τις αντιδράσεις των πολιτών, τις κινητοποιήσεις των οργανισμών πολιτικής ελευθερίας (Civil Liberty Organizations) και τις νομοθετικές προτάσεις, παρατηρείται ότι για μία ακόμη φορά οι αντιδράσεις στις Ηνωμένες Πολιτείες της Αμερικής ξεκίνησαν νωρίτερα απ' ότι στην Ευρωπαϊκή Ένωση. Έτσι, από το 2003 οι οργανισμοί πολιτικής ελευθερίας στις Ηνωμένες Πολιτείες της Αμερικής δημοσίευσαν μία εργασία αναφορικά με τη στάση τους απέναντι στη χρήση της τεχνολογίας και την ίδια χρονιά η «Οργάνωση των Καταναλωτών κατά της προσβολής της ιδιωτικότητας και της αριθμητικής σήμανσης» (Consumer Against Supermarket Privacy Invasion and Numbering, CASPIAN) κατέθεσε πρόταση ομοσπονδιακού νόμου γνωστή ως «RFID Right to Know Act of 2003». Αυτές οι δύο δράσεις αποτέλεσαν τη βάση για την πρόταση νομοσχεδίων μετέπειτα και σε πολιτειακό επίπεδο.

Στην Ευρωπαϊκή Ένωση οι κινητοποιήσεις για τη δημιουργία ενός αποδεκτού πλαισίου για την ορθή χρήση της τεχνολογίας RFID ξεκίνησαν από το 2005 και με κομβικό σημείο τη Σύσταση της Επιτροπής της 12ης Μαΐου το 2009, κατέληξαν το 2011 σε ένα προτεινόμενο πλαίσιο εκτίμησης των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID, το οποίο εγκρίθηκε από την Ομάδα εργασίας του άρθρου 29. Μάλιστα, οι επιχειρήσεις που θα βασιστούν σε αυτό το πλαίσιο θα συμμορφώνονται και με το άρθρο 35 του νέου Κανονισμού 2016/679. Παράλληλα, με απόφαση της Επιτροπής συστάθηκε και ομάδα

εμπειρογνωμόνων για τη ραδιοσυχνική αναγνώριση η οποία συνδράμει στην ανάπτυξη του διαλόγου μεταξύ οργανώσεων των καταναλωτών, φορέων της αγοράς και εθνικών και ευρωπαϊκών αρχών, συμπεριλαμβανομένων των αρχών προστασίας δεδομένων.

Και στις δύο περιπτώσεις, τα προτεινόμενα πλαίσια αφορούν κατευθυντήριες οδηγίες προς τους φορείς εκμετάλλευσης της τεχνολογίας RFID με στόχο την προστασία της ιδιωτικότητας και την αποτελεσματική διαχείριση των κινδύνων. Στην περίπτωση της Ευρωπαϊκής Ένωσης το προτεινόμενο μέτρο είναι ένα εργαλείο εκτίμησης των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων για τις εφαρμογές RFID. Με άλλα λόγια, είναι ένα εργαλείο για τις επιχειρήσεις, το οποίο βοηθάει στον εντοπισμό των κινδύνων προσβολής της ιδιωτικότητας εξαιτίας της χρήσης της τεχνολογίας RFID και την εκτίμηση της πιθανότητας εμφάνισής τους, στην αξιολόγηση των επιπτώσεων και τελικά στην εύρεση μέτρων για την εξάλειψη ή ελαχιστοποίηση αυτών ώστε να μην αποτελούν πλέον απειλή. Με αυτό τον τρόπο, εξασφαλίζεται η συμμόρφωσή τους με την υπάρχουσα νομοθεσία της ΕΕ για την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων. Ενώ στις Ηνωμένες Πολιτείες της Αμερικής έχει παρατηρηθεί πως έχουν προταθεί πιο αυστηρά και πιο δραστικά μέτρα για την προστασία συγκεκριμένα του καταναλωτή, διότι η υπάρχουσα νομοθεσία για την προστασία των προσωπικών δεδομένων είναι ελλιπής[393].

Παρατηρώντας λοιπόν τις νομοθετικές προτάσεις που έχουν γίνει στις Ηνωμένες Πολιτείες της Αμερικής, εξατομικεύοντας αυτές στο δίκαιο της Ευρωπαϊκής Ένωσης και λαμβάνοντας υπόψη και τις οδηγίες που εξέδωσε η Επιτροπή το Μάιο του 2009 σε σύστασή της για την εφαρμογή των αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων σε εφαρμογές όπου χρησιμοποιείται η τεχνολογία RFID (ΕΕ L 122/47), κρίνεται εύλογο να προταθούν και οι παρακάτω ρυθμίσεις για την αποτελεσματικότερη προστασία της ιδιωτικότητας των καταναλωτών από τη χρήση της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου.

[393] Βλ. Αλεξανδροπούλου–Αιγυπτιάδου, Ε., Μαυρίδης, Ι. (2007). Η Προστασία των Προσωπικών Δεδομένων.., ό.π. σελ. 499.

Καταρχήν, επειδή η ενημέρωση των καταναλωτών είναι ένα από τα δικαιώματα των υποκειμένων το οποίο βαρύνει τον υπεύθυνο επεξεργασίας, προτείνονται τα παρακάτω μέτρα, εξατομικευμένα στην περίπτωση της χρήσης της τεχνολογίας RFID, για την αποτελεσματικότερη εξασφάλιση της ενημέρωσής τους.

Ένα αποτελεσματικό μέτρο θα ήταν η χρήση ενός παγκοσμίως αποδεκτού συμβόλου το οποίο θα προσκολλάται στα προϊόντα και θα δηλώνει ότι το προϊόν φέρει ετικέτα RFID, όπως αυτό που πρότεινε η Επιτροπή σε δελτίο τύπου το 2014 (βλ. Εικόνα 14). Αντίστοιχα, θα μπορούσε να υπάρχει και ένα παγκοσμίως αποδεκτό σύμβολο το οποίο θα αναρτάται στα σημεία όπου υπάρχουν οι αναγνώστες και θα δηλώνει την ύπαρξή τους.

Εικόνα 14 EU-wide logo RFID

Πηγή: Press release "Digital privacy: EU-wide logo and "data protection impact assessments" aim to boost the use of RFID systems" Brussels, 30 July 2014, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-14-889_en.htm

Εκτός από τη χρήση προειδοποιητικής ετικέτας πάνω σε κάθε προϊόν, ένα ακόμη προτεινόμενο μέτρο θα μπορούσε να είναι και η τοποθέτηση προειδοποιητικής πινακίδας σε κάθε είσοδο της επιχείρησης στο ύψος των ματιών ώστε να είναι αναγνώσιμη από έναν μέσο αναγνώστη και να δηλώνει πως η επιχείρηση διαθέτει προϊόντα με ετικέτες RFID και υποχρεούται να τις αφαιρέσει ή να τις απενεργοποιήσει. Βέβαια επειδή είναι κατανοητό πως ορισμένες επιχειρήσεις μπορεί να χρησιμοποιούν την τεχνολογία μόνο σε μερικά από τα προϊόντα τους, όπως για παράδειγμα στα πολύ ακριβά ως αντικλεπτικό σύστημα, αυτές δεν θα είναι υποχρεωμένες να τοποθετήσουν προειδοποιητική πινακίδα, παρά μόνο προειδοποιητική ετικέτα πάνω σε κάθε

από αυτά τα προϊόντα. Είναι σαφές λοιπόν να υπολογίζεται πόσα είναι τα προϊόντα μίας επιχείρησης που φέρουν την τεχνολογία RFID και να οριστεί ένα νούμερο ή ένα ποσοστό συγκριτικά με τον συνολικό αριθμό των προϊόντων της επιχείρησης, πάνω από το οποίο θα υποχρεώνονται οι επιχειρήσεις να τοποθετούν και την προειδοποιητική πινακίδα. Ταυτόχρονα καλό θα ήταν να λαμβάνεται υπόψη και το είδος των προϊόντων, δηλαδή εάν η τεχνολογία χρησιμοποιείται σε προϊόντα καθημερινής ανάγκης τότε τα μέτρα θα πρέπει να είναι πιο αυστηρά.

Παράλληλα, απαραίτητες είναι και οι δράσεις ευαισθητοποίησης και ορθής ενημέρωσης όλων των ενδιαφερομένων μερών. Δηλαδή λήψη κατάλληλων μέτρων από τη μία πλευρά για την αύξηση της ευαισθητοποίησης των καταναλωτών σχετικά με την τεχνολογία RFID, τα οφέλη της αλλά και τους κινδύνους που μπορεί να κρύβει όταν χρησιμοποιηθεί από τις επιχειρήσεις, τους εμπόρους και τις κυβερνητικές υπηρεσίες για τη συλλογή προσωπικών δεδομένων. Και από την άλλη πλευρά, ενημέρωση των φορέων εκμετάλλευσης της τεχνολογίας σχετικά με ζητήματα ασφαλείας των δεδομένων και την προστασία της ιδιωτικότητας και τι πρέπει να κάνουν για να συμμορφώνονται με τις διατάξεις του νόμου (όπως για παράδειγμα, να εφαρμόσουν το πλαίσιο PIA, βλ. παραπάνω Μέρος δεύτερο, Κεφάλαιο 5).

Η αφαίρεση ή η απενεργοποίηση των ετικετών RFID στο σημείο αγοράς, πριν φύγει ο καταναλωτής από το κατάστημα, με χρέωση του φορέα εκμετάλλευσης της τεχνολογίας θα πρέπει να γίνεται από προεπιλογή και οι καταναλωτές να μπορούν να διαπιστώνουν ότι η απενεργοποίηση ή η αφαίρεση συνέβη πραγματικά, εκτός και εάν οι καταναλωτές, αφού έχουν προηγουμένως ενημερωθεί με ακριβή και εύκολα κατανοητό τρόπο σχετικά με τη χρήση τους, έχουν επιλέξει να τις διατηρήσουν ενεργές. Πρέπει όμως να τους δίνεται η δυνατότητα ανά πάσα στιγμή για μεταγενέστερη αφαίρεση ή απενεργοποίηση και πάλι δωρεάν και με εύκολο τρόπο. Σε αυτή την περίπτωση πρέπει επίσης να απαγορευτεί οι επιχειρήσεις να εξαναγκάζουν τους πελάτες τους να διατηρούν τις ετικέτες RFID προσκολλημένες ή ενσωματωμένες στα προϊόντα αφού τα αγοράσουν, για παράδειγμα για λόγους εγγύησης.

Ταυτόχρονα, ως αποτέλεσμα της αρχής της διαφάνειας[394,395], οι καταναλωτές έχουν το δικαίωμα να γνωρίζουν τις πολιτικές και τις πρακτικές που χρησιμοποιούν οι φορείς εκμετάλλευσης και αφορούν τη χρήση και τη συντήρηση των συστημάτων RFID και τη δυνατότητα πρόσβασης στα συλλεγέντα δεδομένα που τους αφορούν και διόρθωσης αυτών όταν κρίνεται απαραίτητο. Σύμφωνα με την αρχή της διαφάνειας όπως αναφέρεται και στον ΓΚΠΔ, στο Κεφάλαιο ΙΙΙ σχετικά με τα δικαιώματα του υποκειμένου, ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να παρέχει κάθε πληροφορία σχετικά με την επεξεργασία, δωρεάν, γραπτώς ή με άλλα μέσα, σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση (άρθρο 12, παρ. 1).

[394] Σχετικά με την αρχή της διαφάνειας βλ. Αργυρός Α., Η Αρχή της διαφάνειας και τα προσωπικά δεδομένα ή οι ελεγκτικοί μηχανισμοί του κράτους και η περίπτωση των προσωπικών δεδομένων, ΕλλΔνη 49 (2008): 961, βλ. Εισήγηση στη διημερίδα του Εθνικού Κέντρου δημόσιας διοίκησης και του Σώματος Επιθεωρητών–Ελεγκτών δημόσιας διοίκησης (Καλαμάτα-Ξάνθη-2007), διαθέσιμη στο https://bit.ly/2AISH9q, βλ. Γιαννακάκης Ι. Ε., Η επισήμανση απορρήτου (Privacy Notice) ως βέλτιστη πρακτική για την ενημέρωση των υποκειμένων προσωπικών δεδομένων (GDPR), ΣΥΝήΓΟΡΟΣ, 124/2017, 54-56, βλ. Article 29 Data Protection Working Party (WP 260, rev.01), Guidelines on Transparency under Regulation 2016/679, as last Revised and Adopted on 11 April 2018, διαθέσιμο στο http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

[395] Η ενδέκατη από τις δεκατέσσερις κατευθυντήριες αρχές άσκησης πολιτικής σχετικά με την ανάπτυξη και την εφαρμογή της τεχνολογίας RFID αναδεικνύοντας τα πλεονεκτήματά της και ταυτόχρονα λαμβάνοντας υπόψη και τα πιθανά προβλήματα που μπορεί να προκύψουν, που πρότεινε ο Ο.Ο.Σ.Α. σε κείμενό του, αφορά τις επισημάνσεις απορρήτου ως μέτρο προς αντιμετώπιση του αδιαφανή τρόπου με τον οποίο η τεχνολογία RFID συλλέγει τα δεδομένα, βλ. OECD, (2008) OECD Policy Guidance on Radio Frequency Identification (RFID), ό.π., σελ. 9.

V. Προτάσεις για ειδική ρύθμιση της χρήσης της τεχνολογίας RFID στην ελληνική έννομη τάξη

Η τεχνολογία RFID είναι μία σύγχρονη και επαναστατική τεχνολογία με την οποία επιτυγχάνεται ταυτόχρονη αναγνώριση πολλών αντικειμένων και προσώπων από απόσταση. Με τη χρήση της είναι δυνατόν να δημιουργηθεί ένα περιβάλλον όπου όλα τα αντικείμενα θα μπορούν να αναγνωριστούν, να ταυτοποιηθούν και να εντοπιστούν από απόσταση και ασύρματα, χωρίς την προϋπόθεση της φυσικής ή οπτικής επαφής. Αυτό όμως έχει ως αποτέλεσμα να πραγματοποιείται η μετάδοση και συλλογή δεδομένων εν αγνοία του υποκειμένου και στις περιπτώσεις όπου η τεχνολογία συνδέεται είτε άμεσα, είτε έμμεσα με προσωπικά δεδομένα να προκύπτουν σημαντικά ζητήματα ιδιωτικότητας. Επειδή η χρήση της έχει γίνει ιδιαίτερα ελκυστική και πλέον πληθώρα εφαρμογών τη χρησιμοποιούν, αποτελεί επιτακτική ανάγκη η υιοθέτηση της τεχνολογίας να διενεργείται με τη λήψη των κατάλληλων μέτρων προστασίας των δεδομένων που υφίστανται επεξεργασία.

Έχει παρατηρηθεί πως σε διεθνές επίπεδο έχουν αναληφθεί σχετικές νομοθετικές πρωτοβουλίες για την προστασία της ιδιωτικότητας από την εφαρμογή της τεχνολογίας RFID, όχι όμως και στον ελληνικό χώρο. Μετά από συγκριτική επισκόπηση των νομοθετικών πρωτοβουλιών σε ΕΕ και ΗΠΑ σχετικά με τρεις χαρακτηριστικούς τομείς εφαρμογής της τεχνολογίας RFID που αφορούν α) την εμφύτευση RFID ετικέτας στο ανθρώπινο σώμα, β) τη χρήση της τεχνολογίας RFID στα ηλεκτρονικά διαβατήρια και γ) τη χρήση της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου, προέκυψαν τα παρακάτω συμπεράσματα τα οποία κρίνεται απαραίτητο να ληφθούν υπόψη από το νομοθέτη για τη δημιουργία ενός ελληνικού νομοθετικού πλαισίου ρυθμιστικού της χρήσης της τεχνολογίας RFID το οποίο θα σέβεται τα οφέλη της τεχνολογίας, δε θα επιβραδύνει την εξέλιξή της και ταυτόχρονα δε θα προκύπτουν κίνδυνοι προσβολής της ιδιωτικότητας.

Καταρχήν αποτελεί επιτακτική ανάγκη η προστασία του υποκειμένου από τα ζητήματα ιδιωτικότητας που προκύπτουν με την εμφύτευση RFID ετικέτας στο ανθρώπινο σώμα. Τα οφέλη της εμφύτευσης μικροτσίπ

ταυτοποίησης, όπως η ετικέτα RFID, κυρίως σε εργαζομένους είναι ισχυρά για τις επιχειρήσεις αλλά και οι επιπτώσεις στην ιδιωτικότητα των εργαζομένων είναι πολύ σοβαρές. Στις Ηνωμένες Πολιτείες της Αμερικής είχαν αρχίσει να δραστηριοποιούνται για πρώτη φορά το 2006 όπου σε πολιτειακό επίπεδο δημοσιεύτηκε νόμος ο οποίος απαγορεύει την υποχρεωτική εμφύτευση μικροτσίπ σε άνθρωπο και από τότε μέχρι και σήμερα έχει δημοσιευτεί σχετικός νόμος σε 6 πολιτείες και σχετικό νομοσχέδιο σε άλλες 6 πολιτείες. Αντίθετα, στην Ευρωπαϊκή Ένωση δεν έχει υπάρξει ούτε σχετική νομοθεσία, ούτε νομοσχέδιο, μόνο μία μελέτη που έγινε για την Επιτροπή του Ευρωπαϊκού Κοινοβουλίου Απασχόλησης και Κοινωνικών Υποθέσεων τον Ιανουάριο του 2018.

Στην περίπτωση που θα επιτρεπόταν η εμφύτευση RFID ετικέτας σε εργαζόμενο, τίθεται το ζήτημα τι θα ισχύει όταν θα λήξει η σύμβαση εργασίας[396], με ποιον τρόπο θα αφαιρεθεί το εμφύτευμα, σε ποιον θα ανήκει η ευθύνη για την αφαίρεση και μετά την αφαίρεση σε ποιον θα ανήκει η RFID ετικέτα, μήπως πρέπει να καταστραφεί και αν ναι με ποιο τρόπο, σε ποιον θα ανήκουν τα συλλεχθέντα δεδομένα και ποια θα είναι η επιτρεπόμενη χρονική διάρκεια τήρησης των δεδομένων. Επίσης, δεν εξασφαλίζεται η προστασία των υποκειμένων σε περίπτωση που έχουν δεχθεί ψυχολογικές πιέσεις προκειμένου να αποδεχθούν την εμφύτευση της RFID ετικέτας, καθώς η ανάγκη των ανθρώπων για την εύρεση και σύναψη σύμβασης εργασίας, σε συνδυασμό με την ελλιπή ενημέρωση για τις επιπτώσεις στην ιδιωτικότητά τους, μπορεί να τους οδηγήσει να δεχθούν παρά τη πραγματική θέλησή τους.

Επειδή λοιπόν με την εμφύτευση RFID ετικέτας στο ανθρώπινο σώμα οι επιπτώσεις στην ιδιωτικότητα είναι σοβαρές και πιθανόν μη αναστρέψιμες, ο νομοθέτης οφείλει να απαγορεύσει την υποχρεωτική εμφύτευση RFID ετικέτας και γενικότερα την εμφύτευση οποιουδήποτε μικροτσίπ ταυτοποίησης στον άνθρωπο για οποιοδήποτε λόγο, όχι μόνο στον εργασιακό χώρο, και να ορίσει αυστηρές ποινές σε περιπτώσεις παραβάσεων. Ενώ στις περιπτώσεις που είναι απαραίτητο ένας άνθρωπος να δεχθεί την εμφύτευση RFID ετικέτας

[396] Σχετικά με την ιδιοκτησία των δεδομένων μετά την αφαίρεση της RFID ετικέτας στον εργασιακό χώρο βλ. Graveling R., Winski Th., Dixon K. (2018). The use of chip implants for workers, ό.π. σελ. 24.

εφόσον δεν υπάρχει εναλλακτική λύση, όπως για παράδειγμα για ιατρικούς σκοπούς, θα πρέπει το υποκείμενο να ενημερώνεται με σαφή και κατανοητό τρόπο, να λαμβάνεται η γραπτή του συγκατάθεση και να διασφαλίζεται πως θα τηρούνται απόλυτα οι αρχές της επεξεργασίας, όπως ορίζονται στο άρθρο 5 στον Κανονισμό 2016/679. Σε αυτή την περίπτωση όμως, πέρα από τους παραπάνω προβληματισμούς, πρέπει να ληφθεί υπόψη από το νομοθέτη και ότι ενδέχεται να δημιουργηθούν σοβαρά προβλήματα κοινωνικής περιθωριοποίησης και στιγματισμού αυτών των ανθρώπων καθώς μπορεί να φοβούνται να παρευρίσκονται και να δραστηριοποιούνται μαζί τους άλλοι άνθρωποι φοβούμενοι μήπως έτσι εκτεθούν και οι ίδιοι στους πιθανούς κινδύνους, όπως την παρακολούθηση.

Δεύτερον, κρίνεται απαραίτητη η προστασία του υποκειμένου από τα ζητήματα ιδιωτικότητας που προκύπτουν με τη χρήση της τεχνολογίας RFID στα ηλεκτρονικά διαβατήρια. Η ανάγκη για ενίσχυση της ασφάλειας των συνόρων οδήγησε στη χρήση ηλεκτρονικών διαβατηρίων με την ενσωμάτωση βιομετρικών χαρακτηριστικών, όπως τα δακτυλικά αποτυπώματα, και στη χρήση μίας κοινής τεχνολογίας, όπως η RFID, για την επίτευξη της παγκόσμιας διαλειτουργικότητάς τους. Αρχικά, στις Ηνωμένες Πολιτείες της Αμερικής υπογράφηκε σχετική μεταρρύθμιση του ισχύοντος νόμου το Μάιο του 2002 η οποία απαιτεί όλα τα διαβατήρια και τα έγγραφα ταυτοποίησης που χρησιμοποιούνται για την είσοδο στις Ηνωμένες Πολιτείες της Αμερικής να είναι αναγνώσιμα από μηχανήματα, να μη μπορούν να αλλοιωθούν και να εμπεριέχουν βιομετρικά χαρακτηριστικά και έπειτα ακολούθησε η Ευρωπαϊκή Ένωση το 2004 με την έκδοση του Κανονισμού 2252/2004 σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών.

Η αποθήκευση βιομετρικών δεδομένων στα διαβατήρια δημιούργησε έντονους προβληματισμούς σε περίπτωση αποθήκευσης αυτών και σε μία κεντρική βάση δεδομένων, γεγονός που θέτει σε επικινδυνότητα την ιδιωτικότητα. Συγκεκριμένα στις Ηνωμένες Πολιτείες της Αμερικής τα στοιχεία των κατόχων διαβατηρίων των πολιτών και θεωρήσεων (visa) αποθηκεύονται

σε μία βάση δεδομένων η οποία έχει χαρακτηριστεί η μεγαλύτερη στον κόσμο. Αντίθετα, στον ευρωπαϊκό Κανονισμό 2252/2004 δεν απαγορεύεται πουθενά η αποθήκευσή τους σε μία κεντρική βάση δεδομένων, αλλά το θέμα υπάγεται αποκλειστικά στην εθνική νομοθεσία. Σε μία τέτοια περίπτωση όμως παραβιάζεται η αρχή του σκοπού και η αρχή της αναλογικότητας και αυξάνεται ο κίνδυνος κατάχρησης των δεδομένων και για άλλους σκοπούς μη προβλεπόμενους. Ο νομοθέτης λοιπόν οφείλει να απαγορεύσει ρητά τη δημιουργία κεντρικής βάσης δεδομένων για την αποθήκευση των βιομετρικών δεδομένων, όπως προβλέπεται και στον αντίστοιχο γερμανικό νόμο περί διαβατηρίων.

Από την επιλογή των δακτυλικών αποτυπωμάτων ως το βιομετρικό χαρακτηριστικό για την αλάνθαστη εξακρίβωση και ταυτοποίηση των κατόχων των διαβατηρίων προκύπτει το ζήτημα της ακρίβειά τους καθώς ενδέχεται είτε να αλλοιωθούν με την πάροδο των χρόνων λόγω διάφορων παραγόντων, είτε να συντελέσουν σε λανθασμένη ταυτοποίηση του υποκειμένου. Για τέτοιες περιπτώσεις, όπου τα δεδομένα μπορεί να μην είναι ακριβή, ο νομοθέτης οφείλει να προβλέπει την ύπαρξη εφεδρικών συστημάτων στα σημεία όπου πραγματοποιούνται οι έλεγχοι των διαβατηρίων[397]. Επίσης, επειδή η συλλογή των δακτυλικών αποτυπωμάτων χρησιμοποιείται μέχρι και σήμερα για σκοπούς επιβολής του δικαίου και για τη διαπίστωση εγκληματικής δραστηριότητας ενδέχεται οι κάτοχοι των ηλεκτρονικών διαβατηρίων να ενταχθούν στην κατηγορία των υπόπτων για διάπραξη εγκλημάτων[398], προβληματισμός τον οποίο δεν πρέπει να παραβλέψει ο νομοθέτης.

Τέλος, η χρήση της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου και συγκεκριμένα ανά τεμάχιο έχει ήδη αρχίσει και απασχολεί έντονα το νομοθέτη στον ευρωπαϊκό χώρο αλλά και στις Ηνωμένες Πολιτείες της Αμερικής. Λόγω των ισχυρών οικονομικών οφελών στη βιομηχανία ήδη πολλά προϊόντα φέρουν την τεχνολογία RFID σε επίπεδο τεμαχίου και το

[397] Βλ. Ιγγλεζάκης, Ι. (2010). Ο Κανονισμός 2252/2004 για τα βιομετρικά διαβατήρια.., ό.π. σελ. 83 και Hornung G. (2007). The European Regulation on Biometric Passports: Legislative Procedures.., ό.π. σελ. 258.

[398] Βλ. Παναγοπούλου-Κουτνατζή, Φ. (2013). Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας.., ό.π., σελ. 491.

ζήτημα που εγείρεται είναι πώς μπορεί να προστατευτεί ο καταναλωτής στην περίπτωση που με τη χρήση της τεχνολογίας RFID συνδέεται ο ίδιος με το προϊόν.

Στον ευρωπαϊκό χώρο το 2011 μία ομάδα εργασίας RFID με εκπροσώπους του κλάδου της βιομηχανίας πρότεινε ένα πλαίσιο εκτίμησης των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων για τις εφαρμογές RFID (PIA) το οποίο οι φορείς εκμετάλλευσης εφαρμογών RFID οφείλουν να εφαρμόζουν πριν την εγκατάσταση της τεχνολογίας. Αφορά κυρίως τον ευρωπαϊκό χώρο, αλλά έχει επηρεαστεί πολύ και από τους υπεύθυνους χάραξης πολιτικής (policy makers) στις ΗΠΑ. Το PIA βοηθάει στον εντοπισμό των κινδύνων από τη χρήση της εφαρμογής RFID και στην εύρεση μεθόδων αντιμετώπισής τους ή τουλάχιστον ελαχιστοποίησής τους ώστε να μην αποτελούν πλέον κίνδυνο για την ιδιωτικότητα και ταυτοχρόνως να συμμορφώνονται με τους νομικούς κανόνες για την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων[399]. Αποτελεί ένα αποτελεσματικό μέτρο διότι η δημιουργία αυτού αποτέλεσε μία διεθνή προσπάθεια[400]. Επίσης 3 χρόνια αργότερα και η Ομάδα εργασίας του άρθρου 29 εξέδωσε γνώμη για τις πρόσφατες εξελίξεις στο ΔτΠ[401] και ορισμένες από τις συστάσεις που έκανε σχετίζονται με την εφαρμογή της τεχνολογίας RFID.

Είναι γεγονός ότι οι νομικές ρυθμίσεις που προκύπτουν κατά την πάροδο των χρόνων για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι πάντοτε επηρεασμένες από τις εξελίξεις στο χώρο των νέων τεχνολογιών. Έτσι συνέβη και με τον νέο Κανονισμό 2016/679 ο οποίος στο άρθρο 25 αναφέρεται στην προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ

[399] Βλ. Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID (2011), σελ. 3. Σημειώνεται ότι η ελληνική εκδοχή δεν είναι πλέον διαθέσιμη, ενώ ήταν μέχρι 16/10/2014. Βλ. την αγγλική εκδοχή σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf, σελ. 3.

[400] Spiekerman S. (2012). The RFID PIA – Developed by Industry, Endorsed by Regulators, Series: Law, Governance and Technology Series, Privacy Impact Assessment, Part IV, Vol. 6, σελ: 345.

[401] Βλ. Γνώμη 8/2014 σχετικά με τις πρόσφατες εξελίξεις στο διαδίκτυο των πραγμάτων, 1471/14/EL, WP 223, 6 Σεπτεμβρίου, σελ. 26-30, διαθέσιμη στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_el.pdf

ορισμού η οποία θα διευκολύνει σημαντικά την προστασία της ιδιωτικότητας και στο άρθρο 35 παρ.1 καθορίζει ότι ο υπεύθυνος επεξεργασίας οφείλει να διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Το εργαλείο που μπορεί να χρησιμοποιήσει ο υπεύθυνος επεξεργασίας για την εκτίμηση των επιπτώσεων είναι το προτεινόμενο από την ομάδα εργασίας RFID πλαίσιο PIA[402] εξασφαλίζοντας έτσι και τη συμμόρφωση της επιχείρησης με το άρθρο 35 του νέου Κανονισμού 2016/679.

Ένα αποτελεσματικό μέτρο το οποίο οφείλει να λάβει υπόψη του ο νομοθέτης για την προστασία της ιδιωτικότητας των καταναλωτών από τη χρήση της τεχνολογίας RFID στον τομέα του λιανικού εμπορίου και βαρύνει τον υπεύθυνο επεξεργασίας, είναι η σωστή ενημέρωση των καταναλωτών. Η ενημέρωση μπορεί να επιτευχθεί με τη χρήση ενός παγκοσμίως αποδεκτού συμβόλου το οποίο θα προσκολλάται στα προϊόντα και θα δηλώνει ότι το προϊόν φέρει ετικέτα RFID και ενός παγκοσμίως αποδεκτού συμβόλου το οποίο θα αναρτάται στα σημεία όπου υπάρχουν οι αναγνώστες και θα δηλώνει την ύπαρξή τους. Επίσης, η ενημέρωση μπορεί να πραγματοποιηθεί και με τη τοποθέτηση προειδοποιητικής πινακίδας σε κάθε είσοδο της επιχείρησης στο ύψος των ματιών ώστε να είναι αναγνώσιμη από έναν μέσο αναγνώστη η οποία θα δηλώνει πως η επιχείρηση διαθέτει προϊόντα με ετικέτες RFID και υποχρεούται να τις αφαιρέσει ή να τις απενεργοποιήσει. Βέβαια επειδή μπορεί μόνο ορισμένα προϊόντα της επιχείρησης να φέρουν την τεχνολογία RFID, πρέπει να οριστεί ένα ποσοστό συγκριτικά με τον συνολικό αριθμό των προϊόντων της επιχείρησης πάνω από το οποίο θα υποχρεώνονται οι επιχειρήσεις να τοποθετούν την προειδοποιητική πινακίδα. Ταυτόχρονα είναι απαραίτητο να πραγματοποιείται ορθή ενημέρωση σχετικά με την τεχνολογία RFID όχι μόνο για τους καταναλωτές, αλλά και για τους φορείς εκμετάλλευσης της τεχνολογίας σχετικά με ζητήματα ασφαλείας των

[402] Βλ. "Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του Κανονισμού 2016/679", WP 248 αναθ. 01, σελ. 26, διαθέσιμο στο https://www.lawspot.gr/sites/default/files/images/nea/misc/wp29-dpia.pdf στα ελληνικά και στο http://ec.europa.eu/newsroom/document.cfm?doc_id=47711 στα αγγλικά.

δεδομένων και την προστασία της ιδιωτικότητας και τι πρέπει να κάνουν για να συμμορφώνονται με τις διατάξεις του νόμου.

Επιπρόσθετα, η αφαίρεση ή η απενεργοποίηση των ετικετών RFID στο σημείο αγοράς είναι απαραίτητο να οριστεί από το νομοθέτη ότι θα γίνεται από προεπιλογή και οι καταναλωτές θα μπορούν να διαπιστώνουν ότι η απενεργοποίηση ή η αφαίρεση συνέβη πραγματικά. Είναι απαραίτητο να απαγορευτεί στις επιχειρήσεις να εξαναγκάζουν τους πελάτες τους να διατηρούν τις ετικέτες RFID προσκολλημένες ή ενσωματωμένες στα προϊόντα αφού τα αγοράσουν, για παράδειγμα για λόγους εγγύησης, και σε περιπτώσεις που οι ίδιοι οι καταναλωτές επέλεξαν να μην τις απενεργοποιήσουν, θα πρέπει να τους δίνεται η δυνατότητα ανά πάσα στιγμή για μεταγενέστερη αφαίρεση ή απενεργοποίηση δωρεάν και με εύκολο τρόπο.

Ολοκληρώνοντας, αξίζει να γίνει αναφορά στις ποινικές κυρώσεις που θέτει ο νέος νόμος 4624/2019. Στην παρ.1 του άρθρου 38 του νόμου ορίζεται ότι «*Όποιος, χωρίς δικαίωμα α) επεμβαίνει με οποιονδήποτε τρόπο σε σύστημα αρχειοθέτησης*[403] *δεδομένων προσωπικού χαρακτήρα, και με την πράξη του αυτή λαμβάνει γνώση των δεδομένων αυτών β) τα αντιγράφει, αφαιρεί, αλλοιώνει, βλάπτει, συλλέγει, καταχωρεί, οργανώνει, διαρθρώνει, αποθηκεύει, προσαρμόζει, μεταβάλλει, ανακτά, αναζητεί πληροφορίες, συσχετίζει, συνδυάζει, περιορίζει, διαγράφει, καταστρέφει, τιμωρείται με φυλάκιση μέχρι ενός (1) έτους, εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη*.». Σε αυτή την περίπτωση θα μπορούσαν να υπαχθούν οι επανεγγράψιμες ετικέτες RFID στις οποίες μπορούν να αποθηκευτούν περισσότερα δεδομένα και όχι μόνο το μοναδικό αναγνωριστικό της ετικέτας. Εάν λοιπόν σε μία επανεγγράψιμη ετικέτα RFID είναι αποθηκευμένα δεδομένα προσωπικού χαρακτήρα, τότε η παράνομη πρόσβαση σε αυτές εμπίπτει στις διατάξεις του εν λόγω άρθρου.

Από όλα τα παραπάνω, είναι ξεκάθαρο πως είναι απαραίτητη η θέσπιση ειδικών ρυθμίσεων ιδανικά σε κάθε τομέα εφαρμογής της

[403] Σύμφωνα με άρθρο 4 αρ. 6 του ΓΚΠΔ σύστημα αρχειοθέτησης ορίζεται «*κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο, είτε αποκεντρωμένο, είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση*».

τεχνολογίας ξεχωριστά για την αποτελεσματικότερη προστασία των πολιτών. Ο Έλληνας νομοθέτης λαμβάνοντας υπόψη τις σχετικές νομοθετικές πρωτοβουλίες για την προστασία της ιδιωτικότητας από την εφαρμογή της τεχνολογίας RFID που έχουν αναληφθεί ήδη σε διεθνές επίπεδο και τους ερευνητικούς προβληματισμούς που έχουν τεθεί οφείλει να δημιουργήσει ένα νομοθετικό πλαίσιο ρυθμιστικό της χρήσης της τεχνολογίας RFID με βασικές αρχές οι οποίες θα αποβλέπουν στο σεβασμό και στην προστασία των δεδομένων που συγκεντρώνονται και χρησιμοποιούνται στα συστήματα που χρησιμοποιούν την εν λόγω τεχνολογία, αλλά δεν θα παρεμποδίζουν την εκμετάλλευση των πλεονεκτημάτων της και την περαιτέρω εξέλιξή της.

Βιβλιογραφία και Αρθρογραφία

Αλεξανδροπούλου–Αιγυπτιάδου, Ε. (2002). Ζητήματα από το δίκαιο πληροφορικής, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή

Αλεξανδροπούλου–Αιγυπτιάδου, Ε. (2005). Ηλεκτρονική επεξεργασία προσωπικών δεδομένων και το δικαίωμα αντίρρησης του υποκειμένου τους, Αρμ ΝΘ΄, σελ: 137-142

Αλεξανδροπούλου–Αιγυπτιάδου, Ε. (2007). Προσωπικά δεδομένα: Η νομική ρύθμιση της ηλεκτρονικής επεξεργασίας τους, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα- Κομοτηνή

Αλεξανδροπούλου–Αιγυπτιάδου, Ε., Μαυρίδης, Ι. (2007). Η Προστασία των Προσωπικών Δεδομένων Ενόψει της Εφαρμογής της Νέας Τεχνολογίας της Ταυτοποίησης με Ραδιοσυχνότητες (RFID): Νομική και Τεχνολογική Προσέγγιση, Αρμ ΞΑ΄, σελ: 493-504

Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2007). Η Πλοήγηση των Ανηλίκων στο Διαδίκτυο και η Νομική Προστασία των Προσωπικών Δεδομένων, Αρμ ΞΑ΄, σελ: 848-854

Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2008). Κοινωνία της Πληροφορίας και Νομική Προστασία των Προσωπικών Δεδομένων της Οικογένειας και των Μελών της, Ελληνική Δικαιοσύνη 49, σελ: 691-99

Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2010). Νομική Διασφάλιση του Απορρήτου των Κινητών Επικοινωνιών (Η ελληνική νομική ρύθμιση ενόψει και του πρόσφατου ν. 3674/2008), σε Λαμπρινουδάκη, Κ.-Μήτρου, Λ.-Γκρίτζαλη, Σ.-Κάτσικα,Σ., Προστασία της ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, εκδ. Παπασωτηρίου, Αθήνα 2010, σελ: 655-678

Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2013). Η προστασία των προσωπικών δεδομένων των ανηλίκων στην Πρόταση Κανονισμού για την προστασία των προσωπικών δεδομένων της 25.1.2012, σε Πρακτικά 4ου Πανελλήνιου Συνέδριου της Ένωσης Ελλήνων Νομικών «e-Θέμις» και του Πανεπιστημίου Μακεδονίας, με τίτλο «LegalTech & Data Protection

(Θεσσαλονίκη 22-24 Μαρτίου 2013), εκδ. Νομική Βιβλιοθήκη, Αθήνα, σελ: 47-56

Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). *Προσωπικά Δεδομένα,* Νομική Βιβλιοθήκη, Αθήνα

Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2018). Η προστασία των προσωπικών δεδομένων ανηλίκων στο Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679, ΔiΜΕΕ 1/2018, σελ: 5-19

Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2018). Ο Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679/ΕΕ - Προκλήσεις εφαρμογής, Πρακτικά 1ου διεπιστημονικού συνεδρίου «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ» Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής, Νομική Σχολή ΔΠΘ, Κομοτηνή 25-26 Μαΐου, σελ. 17-30

Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2018). Η προστασία των προσωπικών δεδομένων πριν και μετά τον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679/ΕΕ, Πρακτικά 9ου Συνεδρίου ΕΕΝ e-Θέμις: Προσωπικά δεδομένα και δικηγορία (Ιωάννινα 11-12/5/2018), εκδ. Νομική Βιβλιοθήκη, Αθήνα

Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2018). Επεξεργασία προσωπικών δεδομένων στον τραπεζικό χώρο με έμφαση στην Τειρεσίας Α.Ε., Πρακτικά 7ου Συνεδρίου ΕΕΝ e-Θέμις, Πιστωτικά Ιδρύματα: Νομικές & Θεσμικές Όψεις, Θεσσαλονίκη, εκδ. Νομική Βιβλιοθήκη, Αθήνα, σελ. 35-52

Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2019). Διασυνοριακή ροή δεδομένων υγείας, Βιοηθικοί προβληματισμοί IV: Δεδομένα υγείας και γενετικά δεδομένα, Εκδ. Παπαζήση

Αραβαντινός, Β. (1997). Η προστασία των στοιχείων προσωπικού χαρακτήρα από την αθέμιτη επεξεργασία τους με ηλεκτρονικό υπολογιστή. (Συμβολή στη δικαιοκυβερνητική), Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή

Αργυρός, Α. (2008). Η Αρχή της διαφάνειας και τα προσωπικά δεδομένα ή οι ελεγκτικοί μηχανισμοί του κράτους και η περίπτωση των προσωπικών δεδομένων, ΕλλΔνη 49, σελ: 961

Αρμαμέντος, Π., Σωτηρόπουλος, Β., Προσωπικά δεδομένα Ερμηνείας Ν. 2472/1997, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2005

Γεραρής, Χ. (2010). Τα προσωπικά δεδομένα και οι νέες προκλήσεις, ΔiΜΕΕ 1/2010, σελ: 42-44

Γιαννακάκης, Ι. Ε. (2017). Η επισήμανση απορρήτου (Privacy Notice) ως βέλτιστη πρακτική για την ενημέρωση των υποκειμένων προσωπικών δεδομένων (GDPR), ΣΥΝήΓΟΡΟΣ, 124/2017, 54-56

Γιαννακούλα, Α., Μηλαπίδου, Μ., (επιμ.). (2017). Προσωπικά δεδομένα. (Σειρά: Ειδικοί Ποινικοί Νόμοι), Αθήνα : Νομική Βιβλιοθήκη, ISBN: 978-960-562-682-2

Δαγτόγλου, Π. (2012). Συνταγματικό Δίκαιο, Ατομικά Δικαιώματα, Τέταρτη Ενημερωμένη Έκδοση, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη.

Ζωγραφόπουλος, Δ. Γ. (2017). Η υποχρέωση διενέργειας εκτίμησης αντικτύπου (Data protection impact assessment-DPIA) στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR), ΣΥΝήΓΟΡΟΣ, 120/2017, σελ: 41-43.

Ιγγλεζάκης, Ι. (2003). Ευαίσθητα Προσωπικά Δεδομένα. Η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και οι συνέπειές της, εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη, ISBN 960-301-736-1, ISBN-13 978-960-301-736-3

Ιγγλεζάκης Ι. (2005). Κοινωνικό Κράτος Δικαίου. Υπό το πρίσμα της συνταγματικής αναθεώρησης του 2001 (άρθρο 25§1 Σ) και του Ευρωπαϊκού Κοινοτικού Δικαίου, εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη

Ιγγλεζάκης, Ι. (2006). Εισαγωγή στο Δίκαιο της Πληροφορικής, εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη

Ιγγλεζάκης, Ι. (2006). Προστασία προσωπικών δεδομένων στο σύστημα πληροφοριών ‘‘Τειρεσίας’’, εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη, ISBN: 9789604450725

Ιγγλεζάκης, Ι. (2008). Το Δίκαιο της πληροφορικής (β΄ εκδ.), εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη, ISBN/ISSN: 978-960-445-356-6

Ιγγλεζάκης, Ι. (2009). Οι εφαρμογές της βιομετρικής τεχνολογίας και η συμβατότητά τους με την προστασία των προσωπικών δεδομένων, ΣΥΝήΓΟΡΟΣ 76/2009, σελ: 77-79

Ιγγλεζάκης, Ι. (2010). Ο Κανονισμός 2252/2004 για τα βιομετρικά διαβατήρια και οι ρήτρες διασφάλισης της προστασίας προσωπικών δεδομένων. ΣΥΝήΓΟΡΟΣ 78/2010, σελ: 81-83

Ιγγλεζάκης Ι. (2012). Το δικαίωμα στην ψηφιακή λήθη και οι περιορισμοί του, εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη, ISBN: 978-960-568-078-7

Ιγγλεζάκης, Ι. (2012). Η μεταρρύθμιση των κανόνων προστασίας προσωπικών δεδομένων στην ΕΕ. Η Πρόταση Κανονισμού για την αντικατάσταση της Οδηγίας 95/46/ΕΚ, ΣΥΝήΓΟΡΟΣ 92/2012, σελ: 72-75

Ιγγλεζάκης, Ι. (2012). Ζητήματα εναρμόνισης της νομοθεσίας για την προστασία προσωπικών δεδομένων στην ΕΕ, ΔiΜΕΕ 4/2012, σελ: 477-481

Ιγγλεζάκης Ι. (2012). Το δικαίωμα στην ψηφιακή λήθη σύμφωνα με την πρόταση Κανονισμού της ΕΕ για την προστασία δεδομένων, ΣΥΝήΓΟΡΟΣ 94/2012, σελ:76-79

Ιγγλεζάκης, Ι. (2013). Προστασία δεδομένων προσωπικού χαρακτήρα από τον σχεδιασμό και εξ ορισμού, ΣΥΝήΓΟΡΟΣ 96/2013, σελ: 79-95

Ιγγλεζάκης, Ι. (2013). Διαβατήρια με βιομετρικά στοιχεία και προστασία προσωπικών δεδομένων στη νομολογία του ΔΕΕ (Με αφορμή την απόφαση ΔΕΕ στην υπόθεση C-291/12), ΣΥΝήΓΟΡΟΣ 100/2013, σελ: 71-73

Ιγγλεζάκης, Ι. (2013). Προστασία προσωπικών δεδομένων στις υπηρεσίες κοινωνικής δικτύωσης με βάση την Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της ΕΕ για την προστασία των δεδομένων, σε Πρακτικά 4ου Πανελλήνιου Συνέδριου της Ένωσης Ελλήνων Νομικών «e-Θέμις» και του Πανεπιστημίου Μακεδονίας, με τίτλο «LegalTech & Data Protection (Θεσσαλονίκη 22-24 Μαρτίου 2013), εκδ. Νομική Βιβλιοθήκη, Αθήνα 2013, σελ: 113-125

Ιγγλεζάκης, Ι. (2018). Δίκαιο της πληροφορικής (3η΄ εκδ.), εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη, ISBN/ISSN: 978-960-568-828-8

Ιγγλεζάκης, Ι. (2018). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679) - Εισαγωγή στο νέο νομικό πλαίσιο προστασίας προσωπικών δεδομένων, εκδ. Interactive.

Κανελλοπούλου-Μπότη, Μ. (2010). Η προστασία του απορρήτου και των προσωπικών δεδομένων σε ηλεκτρονικά ιατρικά αρχεία, σε Λαμπρινουδάκη, Κ.-Μήτρου, Λ.-Γκρίτζαλη, Σ.-Κάτσικα,Σ., Προστασία της ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, εκδ. Παπασωτηρίου, Αθήνα, σελ: 567-582.

Κίτσος, Π. (2011). Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών, Διδακτορική Διατριβή, Πανεπιστήμιο Μακεδονίας, Θεσσαλονίκη

Κίτσος, Π., Γιαννουκάκου, Αικ., Αλεξανδροπούλου, Ε. (2014). Η ηλεκτρονική υγεία την εποχή των Big και Open Data (ενόψει και των ρυθμίσεων της Πρότασης Κανονισμού της ΕΕ για την προστασία των προσωπικών δεδομένων), ΔiΜΕΕ 11/2014, σελ: 2-12

Κίτσος, Π., Παππά, Π. (2012). Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στις υπηρεσίες του υπολογιστικού νέφους, ΔiΜΕΕ 2/2012, σελ: 166-176

Κουσουνή-Πανταζοπούλου, Α. (2012). Νομικές Διαστάσεις του Cloud Computing, ΔiΜΕΕ 2/2012, σελ: 177-185

Κώστα, Ε. (2010). Ζητήματα ιδιωτικότητας και νέες τεχνολογίες: το παράδειγμα της τεχνολογίας RFID, σε Λαμπρινουδάκη, Κ.-Μήτρου, Λ.-Γκρίτζαλη, Σ.-Κάτσικα,Σ., Προστασία της ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, εκδ. Παπασωτηρίου, Αθήνα 2010, σελ: 583-602.

Μαντζούφας, Π. (2007). Η Διακινδύνευση στην Κοινωνίας της Πληροφορίας και η Προστασία των Προσωπικών Δεδομένων, Αρμ Ζ΄, σελ: 1088-1109

Μαντζούφας, Π. (2010). Βιοπολιτική και βιομετρία, διαθέσιμο στο https://www.constitutionalism.gr/1828-biopolitiki-kai-biometria/

Μήτρου, Λ. (1999). Η Αρχή Προστασίας Προσωπικών δεδομένων, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή

Μήτρου, Λ. (2010). Η προστασία της ιδιωτικότητας στην Πληροφορική και στις Επικοινωνίες. Η νομική διάσταση, σε Λαμπρινουδάκη, Κ.-Μήτρου, Λ.-Γκρίτζαλη, Σ.-Κάτσικα,Σ., Προστασία της ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, εκδ. Παπασωτηρίου, Αθήνα 2010, σελ: 505-551

Μήτρου, Λ. (2013). Privacy by Design. Η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων, ΔiΜΕΕ 1/2013, σελ:14-25

Μήτρου, Λ. (2015). Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος, ΔiΜΕΕ 4/2015, σελ: 534-549

Μήτρου, Λ. (2017). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, Νέο δίκαιο - νέες υποχρεώσεις - νέα δικαιώματα. Ιδρυτής Σειράς: Γ. Παπαδημητρίου. Διεύθυνση σειράς: Θ. Κ. Παπαχρίστου, Λ. Μήτρου, Τ. Βιδάλης, Θ. Ξηρός. [Σειρά: Δίκαιο και Κοινωνία στον 21ο Αιώνα - τ. 29, 1η έκδ.], ISBN/ISSN: 978-960-568-723-6, Εκδόσεις Σάκκουλα Α.Ε.

Μυλώση, Μ. (2014). Η έννομη προστασία των δεδομένων οικονομικής συμπεριφοράς από την αθέμιτη ηλεκτρονική επεξεργασία τους-Συγκριτική μελέτη της νομικής ρύθμισης σε Ελλάδα και Γαλλία, Διδακτορική Διατριβή, Πανεπιστήμιο Μακεδονίας, Θεσσαλονίκη.

Μυλώση, Μ., Αλεξανδροπούλου, Ε. (2015). Προσωπικά δεδομένα οικονομικής συμπεριφοράς και ηλεκτρονική επεξεργασία τους από την ΤΕΙΡΕΣΙΑΣ ΑΕ, ΔΙΜΕΕ 1/2015, σελ. 25-37.

Μυλώση, Μ., Γιαννουκάκου, Α., Νικήτα, Μ. (2013). Ιδιωτικότητα και Διαφάνεια στη Δημόσια Διοίκηση: προσωπικά δεδομένα και διάχυση", Νομικές και Κοινωνικές Προεκτάσεις του Διαδικτύου σήμερα, Πανελλήνιο Συνέδριο, Νομική Βιβλιοθήκη, Θεσσαλονίκη, Ιούνιος 2013, σελ: 175-194

Ορφανουδάκης, Σ. (2003). Η αρχή της αναλογικότητας, σειρά: μελέτες συνταγματικού δικαίου και Πολιτειολογίας, Αθήνα-Θεσσαλονίκη

Παναγοπούλου-Κουτνατζή, Φ. (2010). Οι ιστότοποι κοινωνικής δικτυώσεως ως εθνική, ευρωπαϊκή και διεθνής πρόκληση της προστασίας της ιδιωτικότητας, εκδ. Σάκκουλα, Αθήνα-Θεσσαλονίκη

Παναγοπούλου-Κουτνατζή, Φ. (2012). Το δικαίωμα στη λήθη στην εποχή της αβάσταχτης μνήμης: Σκέψεις αναφορικά με την Πρόταση Κανονισμού Προστασίας Δεδομένων, Εφημερίδα Διοικητικού Δικαίου, 2/2012, σελ. 264-278

Παναγοπούλου-Κουτνατζή, Φ. (2013). Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας: Σκέψεις με αφορμή την απόφαση ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012), ΔiΜΕΕ 4/2013, σελ. 482-492

Παναγοπούλου-Κουτνατζή, Φ. (2014). Διαδίκτυο των πραγμάτων (Internet of Things-IoT): Αποικισμός της καθημερινής ζωής ή νέα τεχνολογική πρόκληση;, ΔiΜΕΕ 3/2014, σελ: 346-358

Παναγοπούλου-Κουτνατζή, Φ. (2016). Η εξέλιξη του δικαιώματος στη λήθη (περί λήθης της λήθης;), Εφημερίδα Διοικητικού Δικαίου, 6/2016, σελ. 714-728

Παναγοπούλου-Κουτνατζή, Φ. (2017). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 679/2016/ΕΕ. Εισαγωγή και Προστασία Δικαιωμάτων, ISBN/ISSN: 978-960-568-740-3, Εκδόσεις Σάκκουλα Α.Ε.

Παπαδόπουλος, Μ., Ευγενίδης, Π. (2016). Νεφοϋπολογιστική (cloud computing) και προστασία προσωπικών δεδομένων, ΔiΜΕΕ 2/2016, 182-195

Ρεκλείδης, Ε., Ριζομυλιώτης Π., Γκρίτζαλης, Στ. (2010). RFID: Απειλές κατά της Ιδιωτικότητας και Μέτρα Προστασίας, σε Λαμπρινουδάκη, Κ.-Μήτρου, Λ.-Γκρίτζαλη, Σ.-Κάτσικα,Σ., Προστασία της ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, εκδ. Παπασωτηρίου, Αθήνα, σελ: 193-220

Σαατζίδου-Παντελιάδου, Ε. (2007). Νέοι κανόνες δικαίου στο πλαίσιο της Νέας Οικονομίας – Ηλεκτρονική επεξεργασία δεδομένων οικονομικής συμπεριφοράς, Θεσσαλονίκη

Συνοδινού, Τ.-Ε. (2005). Η ανίχνευση της ιδιωτικότητας μέσα από τις ραδιοσυχνότητες: Προστασία προσωπικών δεδομένων και τεχνολογιών αναγνώρισης μέσω ραδιοσυχνοτήτων (RFID), Αρμ ΝΘ', σελ: 1363-1374

Σωτηρόπουλος, Β. (2006). Η συνταγματική προστασία των προσωπικών δεδομένων, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Θεσσαλονίκη

Τάσσης, Σπ. (2012). Συνοπτική παρουσίαση του νέου νόμου για τις ηλεκτρονικές επικοινωνίες (Ν 4070/2012), ΔiΜΕΕ 2/2012), σελ: 54-60, διαθέσιμο στο http://www.tassis.com/images/publications/DiMEE_TASSHS%20%CE%BD%CE%B5%CE%BF%CF%82%20%CE%BD%CE%BF%CE%BC%CE%BF%CF%82%202012.pdf

Τάσσης, Σπ. (2014). Η ιδιωτικότητα ως αντάλλαγμα για την ανάπτυξη τεχνολογικών καινοτομιών, ΔiΜΕΕ 2/2014, 179-185

Τζέμος, Β.-Γ. (2015). Ο Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ. Ερμηνεία κατ' άρθρο, Νομική Βιβλιοθήκη.

Aguirre, J. I. (2007). EPCglobal: a universal standard (Doctoral dissertation, Massachusetts Institute of Technology).

Ahsan, K., Shah, H., Kingston, P. (2010). RFID applications: An introductory and exploratory study, International Journal of Computer Science Issues, 7 (1), No. 3, διαθέσιμο στο https://arxiv.org/ftp/arxiv/papers/1002/1002.1179.pdf

Alexandropoulou-Egyptiadou, E. (2011). The Greek Regulatory Framework on confidentiality and its waiver in mobile communications (after the implementation of the Directives 1995/46, 2002/58 & 2006/24/E.C.), Hellenic Review of International Law 64 (2011), pp. 425-35

Alexandropoulou-Egyptiadou, E. (2014). Minors' internet navigation and personal data protection, in International Organizations and the Protection

of Human Rights, Essays in honor of Prof. Paroula Naskou-Perraki (eds.Th. Skouteris- M. Vagias), ed. Themis, N.A.Sakkoulas and Co, Athens

Alexandropoulou,E., Nikita, M. (2017). The Greek Regulatory Framework On Personal Data Protection (Following the implementation of the relative E.U. Directives), Proceedings of the 7th International Conference of Information Law and Ethics, University of Pretoria, South Africa 22-23 February 2016, ed. The University of Macedonia Press, Thessaloniki, pp. 193-201

Al Malkawi, M., H., Abussaud, A., M. (2005). CPE542 Project, Security over the RFID, Appendix A, pp. 17-21, διαθέσιμο στο http://www.just.edu.jo/~tawalbeh/cpe542/project/r10.pdf

Betzel, M. (2005). Privacy Year in Review: Recent Changes in the Law of Biometrics. ISJLP, Vol. 1, pp. 517-541.

Bolan, C. (2008). A Review of the Electronic Product Code Standards for RFID Technology. In INC, pp. 171-178.

Bottis, M. (2013). Not a Scalpel: RFID Implants for Patients and Personnel in Hospitals, in Bottis M. (ed.), Privacy and Surveillance-current aspects and future perspectives, Nomiki Bibliothiki, pp. 113-124

Bouchagiar G., Botti M. (2018). THE RIGHT TO BE FORGOTTEN: Memory holes as the default?, Amsterdam Privacy Conference, Amsterdam, The Netherlands, 2018, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3226404

Bustard, J. (2015). The Impact of EU Privacy Legislation on Biometric System Deployment: Protecting citizens but constraining applications. IEEE Signal Processing Magazine, Vol. 32(5), pp. 101-108. DOI: 10.1109/MSP.2015.2426682

Cap Gemini (2005). RFID and Consumers: What European Consumers Think About Radio Frequency Identification and the Implications for Business, Cap Gemini, Paris.

Clarke, R. (2009). Privacy Impact Assessment: Its Origins and Development, Computer Law & Security Review, Vol. 25 (2), pp. 123-135.

Coustasse, A., Kimble, C. A., Stanton, R. B., Naylor, M. (2016). Could the Pharmaceutical Industry Benefit from Full-Scale Adoption of Radio-Frequency Identification (RFID) Technology with New Regulations?, Perspectives in health information management, Vol. 13 (Fall), διαθέσιμο στο https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5075230/.

Coyle, K. (2005). Management of RFID in Libraries, The Journal of Academic Librarianship, Vol. 31(5), pp. 486-489, διαθέσιμο στο http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.454.9531&rep=rep1&type=pdf

Dixit, V., Verma, H., K., Singh, A., K. (2011). Comparison of various Security Protocols in RFID, International Journal of Computer Applications, Vol. 24(7), pp. 17-21.

Dressen, D. (2004). Considerations for RFID technology selection. Atmel Applications Journal, Vol. 3, pp. 45-47, διαθέσιμο στο http://application-notes.digchip.com/015/15-16260.pdf

Domdouzis, K., Kumar, B., Anumba, C. (2007). Radio-Frequency Identification (RFID) applications: A brief introduction. Advanced Engineering Informatics, Vol. 21(4), pp. 350-355, doi: 10.1016/j.aei.2006.09.001.

Engels, D. W., & Sarma, S. E. (2005). Standardization requirements within the RFID class structure framework, MIT Auto-ID Labs Technical Report, διαθέσιμο στο https://www.researchgate.net/publication/267835808_Standardization_Requirements_within_the_RFID_Class_Structure_Framework

Ferguson, R. B. (2007). DHS confirms Real ID Act regulations coming; States rebel, διαθέσιμο στο http://www.eweek.com/c/a/Mobile-and-Wireless/DHS-Confirms-Real-ID-Act-Regulations-Coming-States-Rebel

Fishkin, K. P., Roy, S., Jiang, B. (2004). Some methods for privacy in RFID communication, in European Workshop on Security in Ad-hoc and Sensor Networks, Springer, Berlin, Heidelberg, pp. 42-53.

Friggieri, A., Michael, K., Michael, M. G. (2009). The legal ramifications of microchipping people in the United States of America- a state legislative comparison, In IEEE International Symposium on Technology and Society, pp. 1-8. Los Alamitos.

Garfinkel, S. (2002). Adopting fair information practices to low cost RFID systems. In Privacy in Ubiquitous Computing Workshop.

Garfinkel, S. (2002). An RFID Bill of Rights, MIT Technology Review, διαθέσιμο στο https://www.technologyreview.com/s/401660/an-rfid-bill-of-rights/

Gaukler, G., Seifert, R.W. (2007). Applications of RFID in supply chains, chapter 2 in Trends in supply chain Design and Management: Technologies and Methodologies, Edited by Hosang Jung, Frank Chen, Bongju Jeong, Springer London Ltd., online at http://ise.tamu.edu/people/faculty/gaukler/Applications%20of%20RFID%20in%20Supply%20Chains%20-%20Gaukler%20and%20Seifert.pdf

Glasser, D. J., Goodman, K. W., Einspruch, N. G. (2007). Chips, tags and scanners: Ethical challenges for radio frequency identification. Ethics and Information Technology, Vol. 9(2), pp. 101-109.

Graveling, R., Winski Th., Dixon, K. (2018). The use of chip implants for workers, PE 614.209, IP/A/EMPL/2017-12, διαθέσιμο στο http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)614209

Harris, D. B. (1960). Radio transmission systems with modulatable passive responder, U.S. Patent No. 2,927,321. Washington, DC: U.S. Patent and Trademark Office.

Hert, De P., Kloza, D., Wright, D. (2012). Recommendations for a privacy impact assessment framework for the European Union, Παραδοτέο D3 του

έργου PIAF (A Privacy Impact Assessment Framework for data protection and privacy rights), διαθέσιμο στο http://piafproject.eu/ref/PIAF_D3_final.pdf

Hopper, N. J., Blum, M. (2000). A Secure Human-Computer Authentication Scheme, Tech. Rep. CMU-CS-00-139, Carnegie Mellon University, διαθέσιμο στο https://apps.dtic.mil/dtic/tr/fulltext/u2/a382135.pdf

Hopper, N. J., Blum, M. (2001). Secure Human Identification Protocols, In: Boyd C. (eds) Advances in Cryptology – ASIACRYPT, Vol. 2248, pp. 52–66.

Hornung, G. (2007). The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards, SCRIPTed, Vol. 4 (3), pp. 246-262, διαθέσιμο στο http://newton.ee.auth.gr/biometrics/images/docs/hornung.pdf

Iglezakis, I. (2011). Regulation models addressing data protection issues in the EU concerning RFID technology, 4th Conference on Information Law and Ethics, Thessaloniki, May 20-21, available at SSRN: https://ssrn.com/abstract=2279433.

Iglezakis, I. (2013). EU Data Protection Legislation and Case-Law with Regard to Biometric Applications, in Bottis, M. (edit.), Proceedings of the 3rd ISIL 2010 - An Information Law for the 21st century, ed. Nomiki Bibliothiki, pp. 40-53, available at SSRN: https://ssrn.com/abstract=2281108 or http://dx.doi.org/10.2139/ssrn.2281108

Iglezakis, I. (2014). The Right to Be Forgotten in the Google Spain Case (Case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet?, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472323

Ilie-Zudor, E., Kemény, Z., Van Blommestein, F., Monostori, L., Van Der Meulen, A. (2011). A survey of applications and requirements of unique

identification systems and RFID techniques, Computers in Industry, Vol. 62 (3), pp. 227-252.

Juels, A. (2006). R.F.I.D. Security and Privacy: A Research Survey, IEEE Journal on Selected Areas in Communications, Vol. 24 (2), pp. 381-394.

Juels, A., Rivest, R. L., Szydlo, M. (2003). The blocker tag: Selective blocking of RFID tags for consumer privacy. In Proceedings of the 10th ACM conference on Computer and communications security, ACM, pp. pp. 103-111.

Juels, A., Weis, A., St. (2005). Authenticating pervasive devices with human protocols, In: Shoup V. (eds) Advances in Cryptology – CRYPTO 2005. CRYPTO 2005. Lecture Notes in Computer Science, Vol. 3621. Springer, Berlin, Heidelberg, pp. 293-308.

Katina, M., McCathie, L. (2005). The pros and cons of RFID in Supply Chain Management. Proceedings of the International Conference on Mobile Business (ICMB'05), IEEE Computer Society, pp. 623-629, διαθέσιμο στο at http://ro.uow.edu.au/infopapers/105

Kindt, E. (2007). Biometric applications and the data protection legislation, Datenschutz and Datensicherheit, Vol. 31 (3), pp. 166-170.

Kitsos, P., Yiannoukakou, Aik., Nikita, M., Milossi, M. (2013). Big and Open Data Privacy Risks in Health Sector. Developing a Trend or Establishing the Future?, 5th Conference on E-Democracy, Security, Privacy and Trust in a Digital World, Athens, December 2013.

Kosta, E. (2006). The use of RFID chips on Identification Documents, Proceedings of the 2nd Greek National Conference with International Participation: Electronic democracy - challenges of the digital era, Athens, pp. 471-480.

Kosta, E. (2012). The application of the ePrivacy Directive on RFID systems, Informatiebeveiliging, Vol. (1), pp. 4-7.

Kosta, E., Meints, M., Hansen, M., Gasson, M. (2007). An analysis of security and privacy issues relating to RFID enabled ePassports. In IFIP

International Information Security Conference, pp. 467-472, Springer, Boston, MA.

Landt, J. (2005). The history of RFID. IEEE potentials, Vol. 24(4), pp. 8-11.

Levary, R. R., Thompson, D., Kot, K., & Brothers, J. (2005). Radio frequency identification: Legal aspects. Rich. JL & Tech., Vol. 12, p. 1-18.

Michael, K., Michael, M. G. (2010, June). The diffusion of RFID implants for access control and epayments: A case study on Baja Beach Club in Barcelona. In Technology and Society (ISTAS). In IEEE International Symposium on Technology and Society, IEEE, pp. 242-252.

Michalopoulos, D., Mavridis, I. (2010). Surveying privacy leaks through online social network, 14th Panhellenic Conference on Informatics, IEEE, pp. 184-187, ISBN: 978-1-4244-7838-5, DOI: 10.1109/PCI.2010.31

Millosi, M. (2012). Privacy protection in e-Health environment, in Bottis,M., (edit.). Privacy and Surveillance-current aspects and future perspectives, Proceedings of the Liss-Cost seminar in Athens, Greece “Surveillance in Academia”, 2012 plus selected papers from ICIL 2011 and 2012 in Corfu, Greece, ed. Nomiki Bibliothiki Group, pp. 164-186

Nikita, M., Alexandropoulou, E. (2012). The Greek Regulatory Framework on the Personal Data Protection with Emphasis on the Use of Surveillance Systems, Proceedings of LiSS Conference 3: The State of Surveillance (edit. C. William, R. Webster, G. Galdon Calaveli et al.), University of Stirling, pp. 210-219.

Nikita, M. (2012a). RFID in the Supply Chain and the Privacy Concerns, in Bottis, M., Alexandropoulou,E., Iglezakis,I., (edit.). Values and Freedoms in Modern Information Law & Ethics, Proceedings of the 4th International Conference of Information Law and Ethics, University of Macedonia, 20-22 May 2011, ed. Nomiki Bibliothiki Group, Athens 2012, pp. 1212-1233.

Nikita, M., (2012b). RFID chips and EU e-passports: the end of privacy?, in Bottis,M., (edit.). Privacy and Surveillance-current aspects and future perspectives, Proceedings of the Liss-Cost seminar in Athens, Greece

"Surveillance in Academia", 2012 plus selected papers from ICIL 2011 and 2012 in Corfu, Greece, ed. Nomiki Bibliothiki Group, pp. 199-211.

Nikita, M. (2015). The recommended RFID privacy and data protection impact assessment framework in the EU, in Bottis, M., Alexandropoulou, E., Iglezakis, I., (edit.). Lifting the barriers to empower the future of Information Law and Ethics, Proceedings of the 6th International Conference of Information Law and Ethics, University of Macedonia, 30-31 May 2014, ed. The University of Macedonia Press, Thessaloniki 2015, pp. 197-210.

Nogueira, M., Greis, N. (2009). Uses of RFID Technology in US Identification Documents, Institute for Homeland Security Solutions.

O' Connor, M. C. (2006). RFID Brings Order to a Chaotic Office, RFID Journal, RFID Journal LLC, διαθέσιμο στο http://www.rfidjournal.com/articles/view?2374

Oertel, B., Wölk, M., Hilty, L. M., Köhler, A., Kelter, A., Ullmann, M., Wittmann, S. (2005). Security aspects and prospective applications of RFID systems. Bundesamt für Sicherheit in der Informationstechnik, Bonn, διαθέσιμο στο https://www.researchgate.net/publication/258275664_Security_Aspects_and_Prospective_Applications_of_RFID_Systems/comments

Oertel, B., Wölk, M., Hilty, L. (2010). Security aspects and prospective applications of RFID systems. Federal Office for Information Security, διαθέσιμο στο https://www.bsi.bund.de/EN/Publications/RFID/RIKCHA_en_htm.html

Office of the Victorian Privacy Commissioner, Privacy Impact Assessments - A guide for the Victorian Public Sector, Edition 2, Melbourne, April 2009, διαθέσιμο στο https://www.privacy.vic.gov.au/privacy/web2.nsf/files/privacy-impact-assessments-guide/$file/guideline_05_09_no1.pdf.

O' Donoghue, P., Rutz, C. (2016). Real-time anti-poaching tags could help prevent imminent species extinctions, Journal of Applied Ecology, Vol.

53(1), pp. 5-10, διαθέσιμο στο https://besjournals.onlinelibrary.wiley.com/doi/pdf/10.1111/1365-2664.12452

Porter, L. (2005). The Gen 2 Standard: What Is It, and What Does It Mean?. Paxar Corporation, διαθέσιμο στο http://www.hegrobelgium.be/images/pdf/RFID_gen2.pdf (τελευταία πρόσβαση 8/8/2018)

Prasad, N. S. R. K., Rajesh, A. (2012). RFID-based hospital real time patient management system, International Journal of Computer Trends and Technology, Vol. 3 (3), pp. 1011-1016, διαθέσιμο στο http://ijcttjournal.org/Volume3/issue-3/IJCTT-V3I3P134.pdf

Psion Teklogix (2004) “Understanding RFID and Associated Applications”, online at http://barcodingworks.com//?module=file&act=procFileDownload&file_srl=834&sid=f4c018c2525553c93e3b669d3ddd518d

Roberts, C. M. (2006). Radio frequency identification (RFID). Computers & security, Vol. 25(1), pp. 18-26.

Ruiz-Garcia, L., Lunadei, L. (2011). The role of RFID in agriculture: Applications, limitations and challenges. Computers and Electronics in Agriculture, Vol. 79(1), pp. 42-50.

Sardroud, J. M. (2012). Influence of RFID technology on automated management of construction materials and components. Scientia Iranica, Vol. 19(3), pp. 381-392.

Sarma, S., Engels, D. W. (2003). On the future of RFID tags and protocols. White paper, Auto-ID Center, Massachusetts Institute of Technology.

Singh, I., Patil, H. (2010). RFID: Dynamic Surveillance Approach, International Journal of Computer Science Issues (IJCSI), Vol. 7(3), pp. 24-28, διαθέσιμο στο https://www.researchgate.net/profile/Mustafa_Al-Fayoumi/publication/46093584_Practical_E-Payment_Scheme/links/00b49525be8ab3cc11000000.pdf#page=38

Spiekerman, S. (2012). The RFID PIA – Developed by Industry, Endorsed by Regulators, Series: Law, Governance and Technology Series, Privacy Impact Assessment, Part IV, Vol. 6, pp. 323-346.

Stein, S. G. (2007). Where Will Consumers Find Privacy Protection from RFIDS: A Case for Federal Legislation. Duke Law & Technology Review, Vol. 1, διαθέσιμο στο https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1169&context=dltr

Stewart, Bl. (2002). Privacy Impact Assessment Handbook, Office of the Privacy Commissioner, Auckland, March 2002, revised June 2007, διαθέσιμο στο http://www.privacy.org.nz/assets/Uploads/Privacy-Impact-Assessment-Handbook-June2007.pdf

Stockman, H. (1948). Communication by means of reflected power. Proceedings of the IRE, Vol. 36(10), pp. 1196-1204.

US Department of Commerce (2005), Radio Frequency Identification. Opportunities and Challenges in Implementation, Department of Commerce, Washington D.C., April 2005, διαθέσιμο στο http://all-experts.com/assets/roadmaps/437__RFID_April.pdf

Vernon, F. (1952). Application of the microwave homodyne. Transactions of the IRE professional Group on Antennas and Propagation, Vol. 4(1), pp. 110-116.

Warwick, K., I, Cyborg. UK: Century, 2002.

White, G., Gardiner, G., Prabhakar, G. P., & Abd Razak, A. (2007). A comparison of barcoding and RFID technologies in practice. Journal of information, information technology and organizations, Vol. 2, pp. 119-132, ISSN 1557-131, διαθέσιμο στο http://eprints.uwe.ac.uk/13460/

Woellik, H., Mueller, A., & Herriger, J. (2014). Permanent RFID timing system in a track and field athletic stadium for training and analysing purposes. Procedia Engineering, Vol. 72, pp. 202-207

Wright, D. (2011). Should Privacy Impact Assessments Be Mandatory?, Communications of the ACM, Vol. 54 (8), pp. 121-131.

Wright, D., Hert, De P. (2012) “Introduction to Privacy Impact Assessment”, Series: Law, Governance and Technology Series, Privacy Impact Assessment, Part I, Vol. 6, pp. 3-32.

Άλλα έγγραφα

Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των περιφερειών – Η ραδιοσυχνική αναγνώριση (RFID) στην Ευρώπη: βήματα προς την κατεύθυνση χάραξης πλαισίου πολιτικής», {SEC(2007) 312}, COM (2007) 96 τελικό, διαθέσιμη στο http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:EL:PDF

Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των περιφερειών, Το Ίντερνετ των πραγμάτων-Ένα σχέδιο δράσης για την Ευρώπη, COM(2009) 278 τελικό, διαθέσιμη στο http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2009)0278_/com_com(2009)0278_el.pdf

Απόφαση της Επιτροπής της 23ης Νοεμβρίου 2006 σχετικά με την εναρμόνιση του ραδιοφάσματος για συσκευές ταυτοποίησης ραδιοσυχνοτήτων (RFID) που λειτουργούν στη ζώνη υπερυψηλών συχνοτήτων (UHF) [κοινοποιηθείσα υπό τον αριθμό Ε (2006) 5599] (2006/804/ΕΚ), Επίσημη Εφημερίδα της ΕΕ αριθ. L 329/64 της 25.11.2006, διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32006D0804&from=EN

Απόφαση της Επιτροπής της 28ης Ιουνίου 2007 για τη σύσταση της ομάδας εμπειρογνωμόνων για τη ραδιοσυχνική αναγνώριση (2007/467/ΕΚ), Επίσημη Εφημερίδα της ΕΕ αριθ. L 176/25 της 6.7.2007, διαθέσιμη στο

http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32007D0467&from=EN

Απόφαση του Δικαστηρίου (τέταρτο τμήμα) της 17ης Οκτωβρίου 2013 Michael Schwarz κατά Stadt Bochum, «Προδικαστική παραπομπή – Χώρος ελευθερίας, ασφάλειας και δικαιοσύνης – Διαβατήριο με βιομετρικά στοιχεία – Ψηφιακά δακτυλικά αποτυπώματα – Κανονισμός (ΕΚ) 2252/2004 – Άρθρο 1, παράγραφος 2 – Κύρος – Νομική βάση – Διαδικασία έκδοσης – Άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης – Δικαίωμα στην ιδιωτική ζωή – Δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα – Αναλογικότητα», διαθέσιμο στο http://curia.europa.eu/juris/liste.jsf?language=el&num=C-291/12

Γνώμη 8/2014 σχετικά με τις πρόσφατες εξελίξεις στο διαδίκτυο των πραγμάτων, 1471/14/EL, WP 223, 6 Σεπτεμβρίου, διαθέσιμη στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_el.pdf

Γνώμη 5/2010 σχετικά με την πρόταση του κλάδου για ένα πλαίσιο εκπόνησης εκτιμήσεων των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID, 00066/10/EL, WP 175, 13 Ιουλίου 2010, διαθέσιμη στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp175_annex_en.pdf

Γνώμη 4/2007 σχετικά με την έννοια του όρου ‘δεδομένα προσωπικού χαρακτήρα’, 01248/07/EL WP 136, 20 Ιουνίου, διαθέσιμη στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_el.pdf

Γνωμοδότηση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων όσον αφορά την ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, η ραδιοσυχνική αναγνώριση (RFID) στην Ευρώπη: βήματα προς την κατεύθυνση χάραξης πλαισίου πολιτικής

COM(2007) 96, (2008/C 101/01), Επίσημη Εφημερίδα της ΕΕ αριθ. C 101/1 της 23.4.2008, διαθέσιμη στο https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EL.pdf

Γνωμοδότηση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων όσον αφορά την πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την τροποποίηση, μεταξύ άλλων, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγίας σχετικά με την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες), Επίσημη Εφημερίδα της ΕΕ αριθ. C 181, 18.7.2008, σελ: 1–13, διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=uriserv:OJ.C_.2008.181.01.0001.01.ELL&toc=OJ:C:2008:181:FULL

Δελτίο τύπου IP/09/571, Η προστασία της ιδιωτικής ζωής των πολιτών πρέπει να καταστεί προτεραιότητα στην ψηφιακή εποχή τονίζει η Ευρωπαία Επίτροπος κα Reding, Βρυξέλλες, 14 Απριλίου 2009, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-09-571_el.htm

Δελτίο τύπου IP/09/ 952, Όταν το δοχείο γιαουρτιού αρχίζει να σας μιλάει: η Ευρώπη προετοιμάζεται για την επανάσταση του Διαδικτύου, Βρυξέλλες, 18 Ιουνίου 2009, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-09-952_el.htm?locale=en

Δελτίο τύπου IP/09/740, Μικροκυκλώματα με μεγάλες δυνατότητες: Νέες συστάσεις της Ευρωπαϊκής Ένωσης εξασφαλίζουν ότι οι ραβδωτοί κωδικοί του 21ου αιώνα σέβονται την προσωπική ζωή, Βρυξέλλες, 12 Μαΐου 2009, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-09-740_el.htm

Δελτίο τύπου IP/11/742, Προστασία δεδομένων: σύμφωνα με νέα μελέτη, οι Ευρωπαίοι αποκαλύπτουν προσωπικά δεδομένα τους στο Διαδίκτυο, όμως εξακολουθούν να ανησυχούν για την προστασία της ιδιωτικής τους ζωής, Βρυξέλλες, 16 Ιουνίου 2011, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-11-742_el.htm

Δελτίο τύπου IP/12/46, Η Επιτροπή προτείνει τη σφαιρική μεταρρύθμιση των κανόνων περί προστασίας δεδομένων με σκοπό την αύξηση του ελέγχου που οι χρήστες ασκούν επί των δεδομένων τους και τη μείωση των εξόδων για τις επιχειρήσεις, Βρυξέλλες, 25 Ιανουαρίου 2012, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-12-46_el.htm

Δελτίο τύπου IP/12/360, Ψηφιακό θεματολόγιο: Η Επιτροπή ανοίγει διαβούλευση σχετικά με τις έξυπνες, συνδεδεμένες συσκευές- το «διαδίκτυο των πραγμάτων», 12 Απριλίου 2012, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-12-360_el.htm

Δελτίο τύπου 171/16, Μεταρρύθμιση της προστασίας των δεδομένων: το Συμβούλιο εγκρίνει τη θέση του σε πρώτη ανάγνωση, 08/04/2016, διαθέσιμο στο http://www.consilium.europa.eu/el/press/press-releases/2016/04/08/data-protection-reform-first-reading/pdf

Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization, ISO) (2009), ISO 31000:2009, Risk management - Principles and guidelines, διαθέσιμο στο https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en

Ενοποιημένη απόδοση της Συνθήκης για την Ευρωπαϊκή Ένωση και της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, Επίσημη Εφημερίδα της ΕΕ αριθ. C 326, 26.10.2012, σελ: 47–390, διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A12012E%2FTXT

Κανονισμός (ΕΚ) αριθ. 2252/2004 ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 13ης Δεκεμβρίου 2004 σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών (ΕΕ L 385), διαθέσιμος στο http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=uriserv:OJ.L_.2004.385.01.0001.01.ELL&toc=OJ:L:2004:385:TOC

Κανονισμός (ΕΚ) αριθ. 444/2009 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 28 Μαΐου 2009 , για την τροποποίηση του κανονισμού (ΕΚ) αριθ. 2252/2004 του Συμβουλίου σχετικά με την καθιέρωση

προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών, διαθέσιμος στο http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=uriserv:OJ.L_.2009.142.01.0001.01.ELL&toc=OJ:L:2009:142:TOC

Κανονισμός Όρων Χρήσης Μεμονωμένων Ραδιοσυχνοτήτων ή Ζωνών Ραδιοσυχνοτήτων, ΦΕΚ 1713/Β/26-6-2014, διαθέσιμο στο https://www.eett.gr/opencms/export/sites/default/EETT/Electronic_Communications/Radio_Communications/Rigths_Of_Use/FEK1713_26-6-14.pdf.

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), διαθέσιμος στο http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL.

Νόμος 2472/1997, Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, διαθέσιμος στο http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/PROSOPIKA%20DEDOMENA/FILES/2472_97_JUNE2013.PDF

Νόμος 3471/2006, ΦΕΚ 133/Α'/28.6.2006 Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997, διαθέσιμος στο http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/PROSOPIKA%20DEDOMENA/FILES/%CE%9D3471_06.PDF

Νόμος 4070/2012, ΦΕΚ 82/Α΄/10-04-2012, Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις, διαθέσιμος στο http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/PROSOPIKA%20DEDOMENA/FILES/4070_2012.PDF

Νόμος 4039/2012, ΦΕΚ 15/Α΄/02.02.2012, Για τα δεσποζόμενα και τα αδέσποτα ζώα συντροφιάς και την προστασία των ζώων από την εκμετάλλευση ή τη χρησιμοποίηση με κερδοσκοπικό σκοπό, διαθέσιμος στο https://nomoi.info/%CE%A6%CE%95%CE%9A-%CE%91-15-2012-%CF%83%CE%B5%CE%BB-1.html

Νόμος 4205/2013, ΦΕΚ 242/Α΄/611.2013, Ηλεκτρονική επιτήρηση υπόδικων, κατάδικων και κρατούμενων σε άδεια και άλλες διατάξεις, διαθέσιμος στο http://www.ministryofjustice.gr/site/Portals/0/uploaded_files/uploaded_11/N_4205-2013.pdf

Νόμος 4411/2016, ΦΕΚ 142/Α/3-8-2016, Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών - Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις, διαθέσιμος στο https://www.kodiko.gr/nomologia/download_fek?f=fek/2016/a/fek_a_142_2016.pdf&t=d7e237a47706c669e18310c5becdcdac

Νόμος 4624/2019, ΦΕΚ Α' 137/29-08-2019, 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, διαθέσιμος στο https://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=66,121,83,229,125,127,247,242

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», Επίσημη Εφημερίδα της ΕΕ αριθ. L 281 της 23/11/1995, σελ: 31–50, διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:31995L0046.

Οδηγία 2009/136/ΕΚ της 25ης Νοεμβρίου 2009, για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ), Επίσημη Εφημερίδα της ΕΕ αριθ. L 337/11, διαθέσιμη στο http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:El:PDF

Πρόγραμμα εργασίας 2005 της Ομάδας εργασίας του άρθρου 29 (00863/05/EL - WP 109), εγκρίθηκε 14 Απριλίου 2005, διαθέσιμο στο http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp109_el.pdf

Πρόταση Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (γενικός κανονισμός για την προστασία δεδομένων)», COM/2012/011 final, 2012/0011 (COD), διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52012PC0011&from=EN

Σύσταση της Επιτροπής της 12ης Μαΐου 2009 για την εφαρμογή αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων στις εφαρμογές που

υποστηρίζονται από ραδιοσυχνική αναγνώριση [κοινοποιηθείσα υπό τον αριθμό Ε(2009) 3200] (2009/387/ΕΚ), Επίσημη Εφημερίδα της ΕΕ αριθ. L 122/47 της 16.5.2009, διαθέσιμη στο: http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009H0387&from=EN

Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (2012/C 326/02), διαθέσιμος στο: http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=uriserv:OJ.C_.2012.326.01.0391.01.ELL&toc=OJ:C:2012:326:TOC

Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology", 10107/05/EN, WP 105, January 19, 2005, διαθέσιμο στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf

Article 29 Data Protection Working Party, Guidelines on Transparency under Regulation 2016/679, 17 EN, WP 260 rev.01, as last Revised and Adopted on 11 April 2018, διαθέσιμο στο http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Article 29 Data Protection Working Party, The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 02356/09/EN, WP 168, διαθέσιμο στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

Commission Staff working document, Advancing the Internet of Things in Europe, accompanying the document "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Digitising European Industry - Reaping the full benefits of a Digital Single Market COM(2016) 180", Brussels, 19.4.2016, διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016SC0110

EDPS, Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012, διαθέσιμη στο

http://www.europarl.europa.eu/document/activities/cont/201205/20120524ATT45776/20120524ATT45776EN.pdf

ENISA Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications [of March 31, 2010]", Ιούλιος 2010, διαθέσιμη στο https://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia/view

Enhanced Border Security and Visa Entry Reform Act, 2002 (Public Law 107-173), Congressional and Administrative News, 2002-07, No. 5, pp. 543-565, νόμος διαθέσιμος στο https://www.congress.gov/107/plaws/publ173/PLAW-107publ173.pdf

Federal Trade Commission, RFID applications and implications for consumers. A Workshop Report, March 2005, διαθέσιμο στο www.ftc.gov/os/2005/03/050308rfidrpt.pdf

Guidelines on the Use of the Common European RFID Sign, Final version 12 January 2012, διαθέσιμο στο https://economie.fgov.be/sites/default/files/Files/Online/Guidelines-for-use-of-the-Common-European-RFID-Sign.pdf

ICAO Doc 9303 (2006), Machine readable travel documents. Specifications for electronically enabled passports with biometric identification capability, part 1, volume 2, 6th Edition.

ICAO Technical Report (2004a), Biometrics deployment of machine readable travel documents. Development and specification of globally interoperable biometric standards for machine assisted identity confirmation using machine readable travel documents, Version 2.0, ICAO TAG MRTD/NTWG.

ICAO (2004b), Annex I - Use of Contactless Integrated Circuits in Machine Readable Travel Document, Version 4.0.

ICAO Technical Report (2010), Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, ISO/IEC JTC1 SC17 WG3/TF5.

ICAO Working Paper (2011), Revision of the logical data structure technical report on optional expanded chip functionality, Technical advisory group on Machine Readable Travel Documents (tag/MRTD), TAG/MRTD/20-WP/3.

Industry Proposal, Privacy and Data Protection Impact Assessment Framework for RFID Applications. Appendix 1: The proposed Framework. March 31, 2010, διαθέσιμη στο http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_annex_en.pdf

Information Commissioner's Office (ICO), Privacy Impact Assessment Handbook. Version 2.0, Wilmslow, Cheshire, Δεκέμβριος 2007, Version 2.0, Ιούνιος 2009, διαθέσιμο στο http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf

International Organization for Standardization (2009), ISO Guide 73:2009. Risk Management – Vocabulary, διαθέσιμο στο https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en:term:3.8.1

OECD (2004). Emerging Technology Applications, in OECD, Information Technology Outlook 2004, OECD Publishing, Paris, pp. 261–284, doi: http://dx.doi.org/10.1787/it_outlook-2004-9-ens.

OECD (2006). Emerging Technology Applications, in OECD, OECD Information Technology Outlook 2006, OECD Publishing, Paris, pp. 245–282, doi: http://dx.doi.org/10.1787/it_outlook-2006-9-en .

OECD (2006). Radio-Frequency Identification: Drivers, Challenges and Public Policy Considerations, [DSTI/ICCP(2005)19/FINAL], διαθέσιμο σε http://www.oecd.org/internet/consumer/36323191.pdf.

OECD (2007). Radio Frequency Identification Implementation in Germany: Challenges and Benefits, [DSTI/ICCP/IE(2007)6/FINAL], διαθέσιμο σε https://www.oecd.org/germany/39693586.pdf.

OECD (2008a). ICT Policy Developments, in OECD, OECD Information Technology Outlook 2008, OECD Publishing, Paris, pp. 307–338, DOI: http://dx.doi.org/10.1787/it_outlook-2008-9-en.

OECD (2008b). RFID Applications, Impacts and Country Initiatives, OECD Digital Economy Papers, No. 144, OECD Publishing, doi: http://dx.doi.org/10.1787/230464075484.

OECD (2008c). OECD Policy Guidance on Radio Frequency Identification (RFID), Ministerial Meeting on the future of the meeting economy, Seoul, Korea, 17-18 June, διαθέσιμο σε http://www.oecd.org/sti/ieconomy/oecdpolicyguidanceonradiofrequencyidentificationrfid.htm

OECD (2013). The OECD Privacy Framework (2013), διαθέσιμο στο http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Position Statement on the Use of RFID on Consumer Products (2003), διαθέσιμο στο https://www.cdt.org/files/privacy/031114rfid.pdf

Press Release IP/06/289, Commission launches public consultation on radio frequency ID tags, Brussels, 9 March 2006, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-06-289_en.htm

Press Release IP/06/909, Commission opens online public consultation on radio frequency identification (RFID), Brussels, 3 July 2006, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-06-909_en.htm?locale=en.

Press Release IP/06/1808, From alarms to medical implants: Commission frees frequencies for short range wireless devices across the EU, Brussels, 14 December 2006, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-06-1808_en.htm.

Press Release EDPS/07/13, EDPS Opinion on RFID: major opportunities for Information Society but privacy issues need to be addressed with more ambition, 20 December 2007, διαθέσιμο στο http://europa.eu/rapid/press-release_EDPS-07-13_en.htm.

Press Release IP/09/740, Small chips with big potential: New EU recommendations make sure 21st century bar codes respect privacy, Brussels, 12 May 2009, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-09-740_en.htm?locale=en

Press Release IP/09/571, Citizens' privacy must become priority in digital age, says EU Commissioner Reding, Brussels, 14 April 2009, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-09-571_en.htm?locale=en

Press Release IP/14/889, Digital privacy: EU-wide logo and “data protection impact assessments” aim to boost the use of RFID systems, Brussels, 30 July 2014, διαθέσιμο στο http://europa.eu/rapid/press-release_IP-14-889_en.htm.

Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 Ιανουαρίου 2011, διαθέσιμο στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf

REAL ID Act – Title II, improved security for drivers' licenses and personal identification cards, H.R.1268, διαθέσιμο στο https://www.dhs.gov/xlibrary/assets/real-id-act-text.pdf

Reding V., SPEECH/12/26, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, 22 January 2012, διαθέσιμη στο http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm.

Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology (1670/05/EN, WP 111), adopted on 28 September 2005, διαθέσιμο σε https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp111_en.pdf

SPEECH/11/236, Neelie Kr., Smart tags - working together to protect privacy, διαθέσιμος στο http://europa.eu/rapid/press-release_SPEECH-11-236_en.htm?locale=en.

Ιστοσελίδες

Project Cyborg 1.0 διαθέσιμο στο http://www.kevinwarwick.com/project-cyborg-1-0/.

EPIC, “National ID and the REAL ID Act.” διαθέσιμο στο https://epic.org/privacy/id_cards/

Department of Homeland Security, “REAL ID and You: Rumor Control” διαθέσιμο στο https://www.dhs.gov/real-id-and-you-rumor-control

U.S. Mission to the International Civil Aviation Organization, https://icao.usmission.gov/mission/icao/

Eurostat Survey about the Enterprises using radio frequency identification (RFID) instrument, https://ec.europa.eu/eurostat/web/products-datasets/-/tin00126

Σημείωση: Οι ηλεκτρονικές πηγές επανελέγχθηκαν στις 18/09/2019.