ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Privacy Impact Assessment:

τεχνικές, θεσμικές και νομικές διαστάσεις.

Αλεξάνδρα Ι. Σπανού

Επιβλέπουσα Καθηγήτρια: Μήτρου Λίλιαν

Φεβρουάριος 2016

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγικά

Η επίδραση των Τεχνολογιών Πληροφοριών και Επικοινωνιών (ΠΙΕ) στην κοινωνική, οικονομική και προσωπική ζωή του ανθρώπου αποτελεί κεντρικό σημείο της σύγχρονης κοινωνικής προβληματικής και δημοφιλές αντικείμενο μελέτης. Όπως είναι φυσικό, οι απόψεις ποικίλλουν σημαντικά, καλύπτοντας ένα ευρύ φάσμα από την πλήρη δαιμονοποίηση της τεχνολογίας πληροφορικής μέχρι την προσδοκία της «κοινωνίας της αφθονίας», όπου οι νοήμονες μηχανές θα απαλλάξουν τον άνθρωπο από τη δουλεία της εργασίας.

Το ότι οι ΤΠΕ επιφέρουν σημαντικές αλλαγές στη ζωή του ανθρώπου που ξεπερνούν σε ένταση κάθε προηγούμενη τεχνολογική επανάσταση, αποτελεί κοινή και αναμφισβήτητη διαπίστωση σε επιστημονικές και μη αναλύσεις. Οι συντελούμενες αλλαγές έχουν ορισμένα ποιοτικά χαρακτηριστικά που δικαιολογούν τη σημασία που τους αποδίδεται (α) αφορούν όλες τις πτυχές της ζωής του ανθρώπου και (β) πραγματοποιούνται με πρωτόγνωρη, για την ανθρωπότητα ταχύτητα και διαχείριση προσωπικών πληροφοριών. Η γέννηση του σύγχρονου νομικού πλαισίου σε αυτή την περιοχή συσχετίζεται με τον πρώτο, σε παγκόσμιο επίπεδο, νόμο προστασίας δεδομένων που ενεργοποιήθηκε στα 1970 στο κρατίδιο της Έσσης της Γερμανίας. Από τότε πολλά κράτη ή μεγαλύτερα κοινωνικά σύνολα που ξεπερνούν τα στενά όρια ενός κράτους (π.χ. η Ευρωπαϊκή Κοινότητα) έχουν θεσπίσει νόμους για την προστασία από την επεξεργασία δεδομένων, που αντανακλούν την κουλτούρα τους και εκφράζουν την φροντίδα για την αύξηση του αισθήματος ασφάλειας των πολιτών τους.

Το αίσθημα ανασφάλειας των ανθρώπων, οδήγησε, εκτός από την θέσπιση των γενικών νομών, στην αλλαγή των διαδικασιών, πρακτικών και λειτουργιών που απαιτούνται για τη συλλογή και επεξεργασία των προσωπικών δεδομένων. Οι νέες αυτές διαδικασίες πήραν την μορφή θεμελιωμένων αρχών προστασίας δεδομένων (data protection principles), οι οποίες, με τη σειρά τους, αποτυπώθηκαν στους νόμους περί προστασίας δεδομένων του κάθε κράτους. Παρά τις διαφοροποιήσεις, υπάρχουν κάποιες βασικές αρχές που διέπουν τη συλλογή και επεξεργασία των προσωπικών δεδομένων που απαντώνται σε όλα τα μοντέλα προστασίας δεδομένων και είναι γνωστές ως βασικές αρχές προστασίας δεδομένων.

Η παρούσα εργασία πραγματεύεται το θέμα της ιδιωτικότητας από την σκοπιά της αξιολόγησής της. Πιο συγκεκριμένα αναλύεται η έννοια της ιδιωτικότητας καθώς και αξιολόγηση των επιπτώσεων που μπορεί να προκληθούν σε περίπτωση μη προστασίας της υπό συγκεκριμένες συνθήκες. Η μη προστασία της ιδιωτικότητας, δεν οφείλεται απαραιτήτως σε κακόβουλες ενέργειες από το εξωτερικό περιβάλλον ενός συστήματος, αλλά μπορεί να προκληθούν και εξαιτίας κατασκευαστικών παραλείψεων στο πληροφοριακό σύστημα ή σχεδιαστικών λαθών.

Η διάρθρωση της εργασίας αναπτύσσεται σε εφτά κεφάλαια. Στο πρώτο κεφάλαιο γίνεται εννοιολογικός προσδιορισμός βασικών εννοιών που πραγματεύεται η παρούσα εργασία και που έχουν να κάνουν με τους όρους της ιδιωτικότητας, της προστασίας προσωπικών δεδομένων και της εν γένει εξέλιξης της ιδιωτικότητας τα τελευταία χρόνια. Ακόμη, γίνεται λόγος για την σύνδεση των δύο αυτών εννοιών και πως τελικά η διασφάλιση των προσωπικών δεδομένων, μπορεί να υποστηρίξει και να προστατεύσει την ιδιωτικότητα.

Στη συνέχεια, στο δεύτερο κεφάλαιο αποσαφηνίζεται η έννοια των προσωπικών δεδομένων, και πως αυτά σχετίζονται με την ιδιωτικότητα. Ακόμη, παρουσιάζεται το κανονιστικό πλαίσιο προστασίας της ιδιωτικότητας καθώς και κάποιες κατευθυντήριες γραμμές που την διέπουν.

Στο τρίτο κεφάλαιο γίνεται μια ανάλυση των τεχνολογιών ενίσχυσης της ιδιωτικότητας, των μεθόδων που χρησιμοποιούνται, καθώς και τι παρέχουν στον ενδιαφερόμενο.

Στο τέταρτο κεφάλαιο γίνεται μια ανάλυση των δυνητικών απειλών και επιπτώσεων της ιδιωτικότητας, καθώς και οργανώνεται μία κατηγοριοποίηση των απειλών αυτών. Στη συνέχεια αναφέρονται οι πιθανές επιπτώσεις των κινδύνων που υπάρχουν, αλλά και παρουσιάζονται τρόποι αντιμετώπισης και ελαχιστοποίησης αυτών των απειλών.

Στο πέμπτο κεφάλαιο, αναλύεται η αξιολόγηση των επιπτώσεων ιδιωτικότητας, όπου διασαφηνίζεται το αντικείμενο της διαδικασίας της αξιολόγησης καθώς και ο τρόπος που αντιμετωπίζει τα πορίσματα της σε συνδυασμό με άλλες τεχνολογίες ενίσχυσης. Ακόμη, γίνεται αναφορά στα οφέλη που προκύπτουν από την αξιολόγηση της ιδιωτικότητας, αλλά και μειονεκτήματα που προκύπτουν από την διαδικασία αυτή.

Στο έκτο κεφάλαιο της παρούσης εργασίας, παρουσιάζεται η περίπτωση των RFID υπό το ισχύον Ευρωπαϊκό καθεστώς ως μια τεχνολογία η οποία ενδεχομένως να χρήζει επαναπροσδιορισμού των εφαρμογών της λόγω των ενδεχόμενων κινδύνων όσον αφορά την προστασία της ιδιωτικής ζωής, την ασφάλεια και την προστασία των προσωπικών δεδομένων των τελικών χρηστών.

Τέλος, στο έβδομο κεφάλαιο αναφέρεται και αξιολογείται ο νέος κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της ΕΕ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

1. Ιδιωτικότητα

1.1 Ορισμοί και έννοιες

Το 1890 γίνεται για πρώτη φορά μια προσπάθεια να οριστεί η αξία της ιδιωτικότητας (Brandeis & Warren, 1980) όπου συνδέεται με το δικαίωμα να μένει κανείς μόνος του ("the right to be left alone"). Παράλληλα τονίζεται η ανάγκη να υπάρξει συνταγματική κατοχύρωση ως έννοια. Το 1948, το Γενικό Συμβούλιο των Ηνωμένων Εθνών στην «*Παγκόσμια Δήλωση των Ανθρωπίνων Δικαιωμάτων*» κάνει μια γενικότερη αναφορά του συγκεκριμένου όρου ενώ το 1950 η Ευρωπαϊκή Επιτροπή των Ανθρωπίνων Δικαιωμάτων κατοχυρώνει θεσμικά το δικαίωμα σεβασμού της ιδιωτικής ζωής των πολιτών της. Η έννοια της ιδιωτικότητας, ανάλογα το είδος και πλαίσιο (Context) των πληροφοριών, μπορεί να διαχωριστεί στις κάτωθι εκφάνσεις (Rosenberg, 2013):

- *Ιδιωτικότητα Πληροφοριών (Informational Privacy): αφορά στον έλεγχο του αν και πώς τα προσωπικά δεδομένα ενός προσώπου μπορούν να συγκεντρωθούν, να αποθηκευτούν, να υποστούν επεξεργασία ή να διαδοθούν επιλεκτικά.*
- *Εδαφική (Μη προσπελασιμότητα του Χώρου) Ιδιωτικότητα (Territorial Privacy): αφορά στην προστασία της στενής φυσικής περιοχής που περιβάλλει ένα πρόσωπο. δηλαδή οικιακά και άλλα περιβάλλοντα, όπως ο εργασιακός ή ο δημόσιος χώρος.*

- *Σωματική Ιδιωτικότητα (Bodily Privacy): αφορά στην προστασία ενός προσώπου από αδικαιολόγητη παρέμβαση, όπως ο σωματικός έλεγχος, η υποχρεωτική υποβολή σε εξέταση/επέμβαση, η δοκιμή φαρμάκων, πληροφορίες που παραβιάζουν την ηθική αίσθηση του ατόμου.*
- *Ιδιωτικότητα Επικοινωνίας (Communication Privacy): αφορά στην προστασία της επικοινωνίας ενός προσώπου από μη εξουσιοδοτημένη παρακολούθηση.*

Από τότε είναι αξιοσημείωτο το γεγονός ότι έχουν γίνει και άλλες προσπάθειες κατηγοριοποίησης και διαχωρισμού του όρου της ιδιωτικότητας ως προς το πλαίσιο πληροφοριών (Solove, 2006).

Επιπλέον, με τη βοήθεια της αυτοματοποιημένης επεξεργασίας δεδομένων , τα δεδομένα (Data) αναδείχθηκαν και καθιερώθηκαν ως «ξεχωριστός» όρος σε σχέση με την επεξεργασία τους. Ο συσχετισμός αυτός μπορεί πλέον να χαρακτηρίσει το «δεδομένο» ως τεχνικό όρο και μέρος ενός συστήματος που προσδιορίζει τα δεδομένα ως επεξεργασμένες πληροφορίες έπειτα από αυτοματοποιημένη επεξεργασία. Ο όρος πλέον ως προς τον σκοπό παρουσιάζει μια ουδετερότητα ενώ η έννοια της πληροφορίας συσχετίζεται με την χρησιμότητα της. Οι δύο αυτές έννοιες παρά τους διαφοροποιημένους ορισμούς τους θεωρούνται σχεδόν συνώνυμες (Μήτρου, 2006). Στο χώρο της πληροφορικής και του διαδικτύου η ιδιωτικότητα και η προάσπιση της σχετίζεται με την ιδιωτικότητα των πληροφοριών και της επικοινωνίας καθώς δεν υπάρχει άμεση επίδραση στην εδαφική και σωματική ακεραιότητα του ατόμου (Auerbach, 2004).

Η επιτυχής παροχή πληροφοριών μέσω διαδικτύου έχει τονιστεί ότι εξαρτάται σε μεγάλο βαθμό από την πολιτική διασφάλισης των προσωπικών δεδομένων και πληροφοριών που χρησιμοποιούνται σε αυτό. Έτσι, η επεξεργασία των προσωπικών δεδομένων θεωρείται πολύ σημαντικός παράγοντας στα πλαίσια του κρατικού μηχανισμού και τη λειτουργία του Δημόσιου τομέα (Μήτρου, 2006). Πολλές φορές για λόγους όμως αναγνώρισης κάποιων χρηστών του διαδικτύου ή για τον συσχετισμό δεδομένων και πληροφοριών για ειδικά ζητήματα, τα προσωπικά αυτά δεδομένα μπορούν να χρησιμοποιηθούν από τις δημόσιες Αρχές (Ιγγλεζάκης, 2007).

Ο ορισμός της ιδιωτικότητας των πληροφοριών που έχει ευρέως αποδεχτεί προτάθηκε το 1967 (Westin, 1967) και αναφέρει «*Η ιδιωτικότητα είναι η αξίωση των ατόμων, των ομάδων και των ιδρυμάτων, να αποφασίζουν από μόνοι τους για το πότε, πώς και μέχρι ποιο σημείο οι πληροφορίες που αφορούν αυτούς, θα διαβιβάζονται σε άλλους*». Το πιο σημαντικό σε αυτόν τον ορισμό είναι ότι διαχωρίζει τις πληροφορίες σε δημόσια διαθέσιμες και σε ιδιωτικές οι οποίες χρίζουν προστασίας. Οι παράγοντες που καθορίζουν αν κάποια πληροφορία είναι ιδιωτική ή δημόσια συνήθως σχετίζονται με το εκάστοτε ισχύον νομικό και κανονιστικό πλαίσιο. Παράλληλα η ραγδαία εξάπλωση των Πληροφοριακών Συστημάτων δίνει το δικαίωμα σε κάθε άτομο να ορίζει το ίδιο ποιες προσωπικές πληροφορίες μπορεί να τις χαρακτηρίσει ως δημόσιες ή ως ιδιωτικές και άρα απόρρητες.

Η ιδιωτικότητα των Πληροφοριών (πληροφοριακή ιδιωτικότητα) θεωρείται πολύ σημαντική στο χώρο του διαδικτύου δεδομένου του χαρακτήρα αλλά και του όγκου των πληροφοριών που υπάρχουν και αξιοποιούνται μέσα σε αυτό (Vrakas et al., 2010). Ένα χαρακτηριστικό παράδειγμα τέτοιου είδους δεδομένων - πληροφοριών είναι τα διάφορα στοιχεία που μπορεί να χρησιμοποιήσει ο κάθε χρήστης όπως: οικονομικά - φορολογικά στοιχεία, δημογραφικά στοιχεία, ποινικό μητρώο, ιατρικά αρχεία και δεδομένα που σχετίζονται με θρησκευτικές και πολιτικές πεποιθήσεις. Παράλληλα παρατηρείται ότι οι υπηρεσίες που παρέχονται από Δημόσιες Αρχές υποχρεούνται να έχουν όλες αυτές τις παραπάνω πληροφορίες που θεωρούνται ιδιωτικές, σε αντίθεση με τις διάφορες ηλεκτρονικές υπηρεσίες του διαδικτύου όπως το εμπόριο, η μάθηση όπου ο χρήστης επιλέγει κάθε φορά ποια δεδομένα θα γνωστοποιήσει προκειμένου να καταστεί δυνατή η χρήση της συγκεκριμένης υπηρεσίας.

Αναμφίβολα, υπάρχει ένας διαχωρισμός μεταξύ ιδιωτικής και δημόσιας σφαίρας. Ωστόσο δεν υπάρχει γενική συναίνεση για το ποια είναι η διαχωριστική γραμμή μεταξύ των δυο, ενώ υπάρχουν πολλές διαφορετικές θεωρίες σχετικά με τους ορισμούς των δυο σφαιρών. Υπάρχει όμως γενική αποδοχή του γεγονότος ότι υπάρχουν αν και οι δυο αυτές σφαίρες αντιμετωπίζονται διαφορετικά από διάφορες πολιτικές ιδεολογίες ως προς την αξία και τη σπουδαιότητά τους. Υπάρχει πλήθος ορισμών για την ιδιωτικότητα. Ενδεικτικά αναφέρουμε τη θεωρία του Robert Holms κατά τον οποίο η ιδιωτικότητα

είναι η ελευθερία από την παρέμβαση σε τομείς της ζωής ενός ατόμου οι οποίοι δεν είναι ανοιχτοί ρητά ή μη σε τρίτους. Παράλληλα, ο Robert Ellis Smith ορίζει την ιδιωτικότητα ως την επιθυμία καθενός από εμάς για φυσικό χώρο ο οποίος θα είναι ελεύθερος από παρεμβάσεις, παρεμβολές, ντροπιαστικές πράξεις, ή απόδοση ελέγχου και την προσπάθεια ελέγχου του χρόνου και του τρόπου των αποκαλύψεων προσωπικών πληροφοριών σχετικά με εμάς. Επίσης, κατά τον Miller (1971) η ιδιωτικότητα είναι «η ικανότητα ταυ ατόμου να ελέγχει τη ροή των πληροφοριών γύρω από το άτομό του», ενώ η Gavison θεωρώντας ότι είναι δύσκολο να τεθεί στον ορισμό της ιδιωτικής ζωής η ικανότητα ελέγχου από το ίδιο το υποκείμενο, με μια περισσότερο ουδέτερη προσέγγιση χωρίζει την έννοια της ιδιωτικής ζωής σε τρία μέρη: τη μυστικότητα, την ανωνυμία και την απομόνωση.

1.2 Ιδιωτική ζωή και τηλεπικοινωνίες

Σημαντικό ρόλο στην μείωση της προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων έπαιξε και η τρομοκρατική ενέργεια στη Νέα Υόρκη την 11^{η} Σεπτεμβρίου 2001, στη Μαδρίτη το 2004 και στο Λονδίνο το 2005. Όλες οι παραπάνω ενέργειες έδωσαν την αφορμή για μεγαλύτερη πρόσβαση των κρατικών υπηρεσιών στα προσωπικά δεδομένα. Την τάση αυτή υπογραμμίζει και η συζήτηση σε ευρωπαϊκό επίπεδο που επιτρέπει σε διαχειριστές τηλεπικοινωνιών, σε εταιρίες κινητής τηλεφωνίας και internet service providers να κρατούν στα αρχεία τους τα δεδομένα ευρωπαίων πολιτών από όλα τα δεδομένα κυκλοφορίας.

Στην εποχή μας, όπως έχει χαρακτηριστικά ειπωθεί, οι προσπάθειες που γίνονται για την προστασία της ιδιωτικότητας συνδέονται με τις ραγδαίες τεχνολογικές εξελίξεις και το γεγονός αυτό εγείρει σημαντικούς θεωρητικούς νομικούς προβληματισμούς με σκοπό την αντιμετώπιση των πρακτικών προβλημάτων. Οι τεχνολογίες ακριβούς εντόπισης έχουν οδηγήσει στην δυνατότητα εύρεσης μιας συσκευής οπουδήποτε κι αν αυτή βρίσκεται. Τα αποτελέσματα για το χρήστη μπορεί να είναι εξαιρετικά δυσάρεστα.

Για παράδειγμα κάποιος στρίβει σε μια γωνία και του έρχεται μήνυμα στο κινητό του τηλέφωνο με το εξής περιεχόμενο «πεινάτε; Στην επόμενη γωνία θα βρείτε μια Pizza Hut

η οποία δίνει δώρο αναψυκτικό για κάθε πίτσα. Ελάτε!» Παράλληλα, πλήθος υπηρεσιών εξεύρεσης συντρόφου ή ακόμη και παιχνιδιών βυθίζονται σε πληροφορίες δεδομένων εντοπισμού από κινητά τηλέφωνα. Χαρακτηριστικά αναφέρουμε το πρόγραμμα παρακολούθησης τρίτων μέσω διαδικτύου με την ονομασία «Spying» που διαφημίζεται στις σελίδες του yahoo mail με την εξής φράση «εντοπίστε φίλους δίνοντας απλώς τον αριθμό του κινητού τους, εντοπισμός μέσω GPS με €8 το μήνα».

1.3 Εξέλιξη της ιδιωτικότητας

Εάν η προστασία της ιδιωτικής ζωής αποτελεί ακρογωνιαίο λίθο της δημοκρατίας, τότε η δημοκρατία βρίσκεται σε κίνδυνο. Ειδικά μετά την έλευση του υπολογιστή, οι καταπατήσεις στην ιδιωτική ζωή έχουν πολλαπλασιαστεί. Επίσης, οι διάφορες τρομοκρατικές επιθέσεις στις αρχές του 21ου αιώνα έχουν δώσει στις κυβερνήσεις παγκοσμίως όλα εκείνα τα επιχειρήματα που χρειάζονται για να ενισχύσουν την εθνική ασφάλεια, υποχρεώνοντας τις εταιρείες τηλεπικοινωνιών να διατηρούν τηλεφωνικά αρχεία, για να δικαιολογήσουν την έκδοση εντάλματος υποκλοπών στις τηλεφωνικές κλήσεις όλων των πολιτών, για να εξετάζουν τραπεζικά αρχεία, να συγχωνεύονται προσωπικά αναγνωρίσιμες πληροφορίες από πολλαπλές πηγές, σκιαγραφώντας έτσι το προφίλ των πολιτών ώστε να καθορίζουν ποιος μπορεί να αποτελέσει κίνδυνο για την καθεστηκυία τάξη. Πολλές εταιρείες έχοντας με το μέρος τους και την συνενοχή των κυβερνητικών προσπαθειών, ασχολούνται με τις λεπτομέρειες της ζωής μας. Προσωπικά δεδομένα σε πραγματικό χρόνο αποτελούν «το καύσιμο» της σημερινής οικονομίας. Η ανάπτυξη των νέων τεχνολογιών, ενώ αναμφισβήτητα προσφέρει πολλά οφέλη, αποτελεί και ένα δίκοπο μαχαίρι: αν ο χρήστης δεν είναι προσεκτικός στην διαχείριση των νέων μέσων, μπορεί να υποφέρει πολύ.

Οι νέες τεχνολογίες μπορούν να χρησιμοποιηθούν και χρησιμοποιούνται για να ανακαλυφθούν ολοένα και περισσότερα σχετικά με το πού είμαστε, πού πάμε, τι κάνουμε, ποια είναι τα συμφέροντα και οι ροπές μας, να χειραγωγηθεί η συμπεριφορά μας και οι επιλογές μας με τρόπους τους οποίους οι περισσότεροι άνθρωποι δεν γνωρίζουν.

Αλλά η προστασία της ιδιωτικής ζωής δεν είναι μια τελειωμένη υπόθεση. Οι έρευνες κοινής γνώμης που έχουν γίνει και γίνονται σχετικά με το θέμα αυτό, δείχνουν ότι επικρατεί σταθερά μια ανησυχία και δυσπιστία των πολιτικών ηγετών μας και των εταιρικών πολεμάρχων σε θέματα προστασίας της ιδιωτικής ζωής. Οι πολίτες μπορούν να επιλέξουν είτε να παραιτηθούν από τα προσωπικά στοιχεία, στην αμείλικτη παρότρυνση των μεγάλων επιχειρήσεων, ή να εξακολουθούν να εκτιμούν ότι έχει απομείνει.

Ένα από τα μέσα για την προστασία της ιδιωτικής ζωής είναι η αξιολόγηση των επιπτώσεων στην ιδιωτική ζωή (ΑΕΙ[1]). Υπάρχει αυξανόμενο ενδιαφέρον για την ΑΕΙ διεθνώς, και αποτελεί και το βασικό θέμα που πραγματεύεται η παρούσα εργασία.

Στην Ευρώπη, το ενδιαφέρον για την ΑΕΙ πυροδοτήθηκε από δύο βασικά γεγονότα. Πρώτα ήταν η ανάπτυξη και η δημοσίευση εγχειριδίου της ΑΕΙ στο Ηνωμένο Βασίλειο, του πρώτου στην Ευρώπη, το Δεκέμβριο του 2007 (Wright & Hert, 2012).

Η δεύτερη ήταν από την συζήτηση που εντάθηκε από την δημοσίευση της σύστασης της Ευρωπαϊκής Επιτροπής σχετικά με την τεχνολογία RFID τον Μάιο του 2009 με την οποία η Επιτροπή κάλεσε τα κράτη μέλη να παρέχουν ενημέρωση στην σχετική ομάδα εργασίας για την προστασία προσωπικών δεδομένων του άρθρου 29, για την ανάπτυξη ενός πλαισίου αξιολόγησης των επιπτώσεων της ιδιωτικής ζωής σε σχέση με την ανάπτυξη της τεχνολογίας ταυτοποίησης ραδιοσυχνοτήτων (RFID).

1.4 Η Ιδιωτικότητα ως ανθρώπινο δικαίωμα

Η ιδιωτικότητα είναι ένα από τα βασικά ανθρώπινα δικαιώματα το οποίο μπορεί πολύ εύκολα να προσβληθεί στην σύγχρονη εποχή. Υποστηρίζει την ανθρώπινη αξιοπρέπεια και άλλες αξίες όπως η ελευθερία συναναστροφής και η ελευθερία του λόγου. Αναγνωρίζεται διεθνώς σε διαφορετικές κουλτούρες και καθεστώτα και προστατεύεται από την Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου, την Διεθνή Συνθήκη Πολιτικών Δικαιωμάτων και σε πολλές άλλες διεθνείς συνθήκες και συμβάσεις. Σχεδόν

[1]ΑΕΙ : Αξιολόγηση Επιπτώσεων στην Ιδιωτικότητα

όλες οι χώρες του κόσμου έχουν ενσωματώσει στο Σύνταγμά τους διατάξεις που σχετίζονται με την ιδιωτικότητα. Αυτές οι διατάξεις περιλαμβάνουν, κατ' ελάχιστον, το απαραβίαστο της οικογενειακής στέγης και το απόρρητο των επικοινωνιών. Τα νεότερα Συντάγματα περιλαμβάνουν συγκεκριμένα δικαιώματα του ατόμου που αφορούν την πρόσβαση και τον έλεγχο των προσωπικών του πληροφοριών.

Στις ΗΠΑ, η έννοια της ιδιωτικότητας εμφανίστηκε πρώτη φορά το 1890 στο άρθρο του Harvard Law Review από τους καθηγητές Samuel Warren και Louis Brandeis, οι οποίοι όρισαν την ιδιωτικότητα ως το «δικαίωμα του να αφήνεται κανείς μόνος» (the right to be let alone). Αυτός ο ορισμός της ιδιωτικότητας τον τελευταίο αιώνα περιλαμβάνει τουλάχιστον δυο εκδοχές, το δικαίωμα των ατόμων να ελέγχουν το φυσικό τους χώρο αλλά και των προσωπικών τους πληροφοριών. Η τελευταία εκδοχή ονομάζεται επίσης πληροφοριακή ιδιωτικότητα» ή «πληροφοριακός αυτοκαθορισμός».

Κατά συνέπεια, η ιδιωτικότητα περιλαμβάνει το δικαίωμα του ατόμου να ελέγχει τη συλλογή, χρήση και αποκάλυψη των προσωπικών του δεδομένων. Όπως μαρτυρεί η ετυμολογική προσέγγιση του όρου «προσωπικά δεδομένα», η προέλευσή του είναι απευθείας από την ορολογία της πληροφορικής, στην οποία γίνεται ευρύτατη χρήση του όρου «δεδομένα». Οι προσωπικές πληροφορίες θα πρέπει να είναι γενικά πληροφορίες που ταυτίζονται με ένα συγκεκριμένο άτομο. Με άλλα λόγια, είναι πληροφορίες που χρησιμοποιούνται για να αναγνωριστεί ένα πρόσωπο και μπορούν να περιλαμβάνουν το όνομα, τη διεύθυνση, το τηλέφωνο, την ημερομηνία γέννησης, τη φυλή και την οικογενειακή κατάσταση ή ακόμη την ηλεκτρονική διεύθυνση, το ιατρικό ιστορικό, την οικογενειακή κατάσταση. Ορισμένες εταιρίες που χρησιμοποιούν τεχνολογικά μέτρα προστασίας της πνευματικής ιδιοκτησίας χρησιμοποιούν τα συγκεκριμένα μέτρα για να συλλέξουν προσωπικές πληροφορίες για τους καταναλωτές τους, ενώ οι πληροφορίες αυτές τους βοηθούν στη συνέχεια στην καλύτερη προώθηση των προϊόντων τους (Cavoukian, 2002).

Η ιδιωτικότητα (privacy) είναι ίσως το λιγότερο σαφώς προσδιορισμένο από τα ανθρώπινα δικαιώματα που περιλαμβάνονται στον αντίστοιχο διεθνή κατάλογο. Υπάρχουν πολλοί ορισμοί της ιδιωτικότητας, οι οποίοι ποικίλουν ανάλογα με το περιβάλλον, την κουλτούρα και το πλαίσιο εφαρμογής της. Σε πολλές χώρες, συγχέεται η

έννοια της ιδιωτικότητας με την έννοια της προστασίας προσωπικών δεδομένων. Η τελευταία ερμηνεύει την ιδιωτικότητα ως την ελευθερία του ατόμου να διαχειρίζεται αυτοβούλως τις προσωπικές του πληροφορίες.

Εκτός της στενής αυτής ερμηνείας, η προστασία της ιδιωτικότητας αποτελεί το όριο πέραν του οποίου η κοινωνία δεν μπορεί να εισβάλλει στα προσωπικά ενός ατόμου. Η απουσία ενός συγκεκριμένου ορισμού δεν υπονοεί σε καμία περίπτωση ότι το ζήτημα της ιδιωτικότητας δεν είναι σημαντικό. Όπως ένας συγγραφέας έχει παρατηρήσει, «κατά κάποια έννοια, όλα τα ανθρώπινα δικαιώματα άπτονται του δικαιώματος της ιδιωτικότητας». Μερικοί ορισμοί της ιδιωτικότητας δίνονται παρακάτω: Στα 1890, ο μελλοντικός δικαστής του Ανώτατου Δικαστηρίου των ΗΠΑ, Louis Brandeis, διευκρίνισε την έννοια της ιδιωτικότητας που έγκειται στο «δικαίωμα της απομόνωσης» (right to be left alone) του ατόμου. Ο Alan Westin, συγγραφέας μιας πρωτοποριακής εργασίας με τίτλο «Privacy and Freedom» το 1967, όρισε την ιδιωτικότητα ως την επιθυμία του ανθρώπου να επιλέγει ελεύθερα τις συνθήκες και την έκταση στην οποία θα εκθέτει τον εαυτό του. τις απόψεις του και την συμπεριφορά του προς τους άλλους.

Σύμφωνα με τον Bloustein (2002) η ιδιωτικότητα σχετίζεται με την ανθρώπινη προσωπικότητα. Προστατεύει το απαραβίαστο της προσωπικότητας, την ανεξαρτησία του ατόμου, την αξιοπρέπεια και την ακεραιότητα. Η επιτροπή Calcutt στο Ηνωμένο Βασίλειο υποστήριξε ότι δεν μπόρεσε να βρει πουθενά έναν θεσπισμένο ικανοποιητικό ορισμό της ιδιωτικότητας. Παρόλα αυτά η επιτροπή αισθάνθηκε ικανοποίηση όταν μπόρεσε να την ορίσει νομικά και να ενσωματώσει τον ορισμό αυτό στην πρώτη της αναφορά σχετικά με την ιδιωτικότητα: «Το δικαίωμα του ατόμου να προφυλάσσει τόσο την προσωπική του ζωή ή τα προσωπικά του ζητήματα όσο και της οικογένειας του από εισβολή που επιχειρείται είτε με φυσικά μέσα είτε με την δημοσίευση πληροφοριών».

1.5 Ιδιωτικότητα και προσωπικά δεδομένα

Η Προστασία Προσωπικών Δεδομένων είναι μια πολυδιάστατη έννοια, η οποία πολλές φορές περιέχει ασαφείς ερμηνείες, και αμφισβητείται ανάλογα με το περιεχόμενο της, αλλά και το πολιτισμικό πλαίσιο της κοινωνίας στην οποία αναφέρεται. Η αξιολόγηση

των επιπτώσεων της ιδιωτικότητας θα πρέπει να είναι σαφής σχετικά με το τι σημαίνει προστασία της ιδιωτικής ζωής για το πλαίσιο το οποίο αναφέρεται (και συχνά θα ισχύουν περισσότερες από μία έννοιες).

Υπάρχουν διάφοροι λόγοι για τους οποίους οι οργανώσεις, τόσο σε κυβερνητικό επίπεδο όσο και σε επίπεδο των επιχειρήσεων, διεξάγουν αξιολογήσεις επιπτώσεων της ιδιωτικότητας. Σε ορισμένες περιπτώσεις, όπως στον Καναδά, τις ΗΠΑ και ίσως και το Ηνωμένο Βασίλειο, αυτές οι αξιολογήσεις είναι υποχρεωτικές για δημόσιες υπηρεσίες και οργανισμούς. Σε άλλες περιπτώσεις, οι οργανισμοί πραγματοποιούν αξιολόγηση των επιπτώσεων της ιδιωτικότητας, επειδή θέλουν να αποφύγουν πιθανούς μελλοντικούς κινδύνους που απορρέουν από σφάλματα στην διαχείριση των προσωπικών δεδομένων, ή να αποκτήσουν ορισμένα πλεονεκτήματα.

Η αξιολόγηση των επιπτώσεων Προστασίας Προσωπικών Δεδομένων θα πρέπει να βασίζεται μεθοδολογικά στην εκτίμηση των κινδύνων και της διαδικασίας διοίκησης του οργανισμού στον οποίο αναφέρεται. Αν μια κυβερνητική υπηρεσία ή μια εταιρεία ή οποιοδήποτε νομικό πρόσωπο που ασχολείται με τα προσωπικά δεδομένα μπορεί να αποφύγει την εφαρμογή ενός συστήματος που σχετίζεται με προσωπικά δεδομένα, άμεσα θα ελαχιστοποιήσει τους πιθανούς κινδύνους. Οι υποστηρικτές της αξιολόγησης των επιπτώσεων της ιδιωτικότητας έχουν προσδιορίσει διάφορους κινδύνους που παρουσιάζονται σε έναν οργανισμό ο οποίος συλλέγει προσωπικά δεδομένα και αναγνωρίσιμες πληροφορίες, αλλά έχουν αναδείξει και τα διάφορα οφέλη που απορρέουν από τη διεξαγωγή της αξιολόγησης των επιπτώσεων της ιδιωτικότητας για τον εντοπισμό, την αποφυγή ή τον περιορισμό αυτών των κινδύνων. Πράγματι, πολλοί είναι εκείνοι οι οποίοι θέτουν την ΑΕΙ ως μια επιμέρους οργανωσιακή πρακτική της συνολικής στρατηγικής διαχείρισης κινδύνων του οργανισμού.

Παρατηρείται λοιπόν ότι η προστασία της ιδιωτικότητας κρίνεται απαραίτητη, καθώς η συλλογή και επεξεργασία πληροφοριών ενεργοποιεί την πολυλειτουργική χρήση και την αποξένωση της πληροφορίας από τον φορέα της και τους αρχικούς στόχους της συλλογής και επεξεργασίας της. Η σύζευξη ανάμεσα στην πληροφορική και τον τομέα της επικοινωνίας, καθώς και η αποκέντρωση της επεξεργασίας προξενούν μεγάλες αλλαγές στο περιβάλλον χρήσης και προστασίας των προσωπικών δεδομένων. Μέσα σε

αυτό το περιβάλλον προβάλλει η ανάγκη για την προστασία των δεδομένων και συνδέεται άρρηκτα με την εξέλιξη της τεχνολογίας και λειτουργεί ως ασπίδα προστασίας απέναντι στους διάφορους κινδύνους.

Επιπρόσθετα, η εν λόγω προστασία δεν αφορά μόνο τη ρύθμιση της πληροφορίας που κρίνεται προσωπικό και ευαίσθητο δεδομένο, αλλά στοχεύει και στον περιορισμό της συλλογής και διάδοσής της. Τέτοια πληροφορία μπορεί να αποτελεί κάθε είδους πληροφορία η οποία μπορεί να αφορά ένα φυσικό πρόσωπο, ενώ ακόμη και εάν αυτή θεωρείται αρχικά αβλαβής θα κριθεί από την επεξεργασία στην οποία υπόκειται και το περιβάλλον μέσα στο οποίο χρησιμοποιείται. Αυτό συνεπάγεται ότι η προστασία των προσωπικών δεδομένων δεν αποτελεί συνάρτηση της ιδιωτικής ή δημόσιας σφαίρας ή της απόρρητης ή απλής πληροφορίας, αλλά πρόκειται για μια ευρύτερη έννοια που αφενός δεν εμπίπτει στη διάκριση αυτή αφετέρου σέβεται το δικαίωμα στην απομόνωση (Hustinx, 2005). Εάν κανείς αναλογιστεί ότι πάντοτε υπάρχουν πληροφορίες που δεν επιθυμεί να αποκαλυφθούν ή να διαδοθούν, καθίσταται σαφές ότι η προστασία των προσωπικών δεδομένων συνδέεται άμεσα με την προστασία της ιδιωτικότητας. Ιδιαίτερα τα τελευταία χρόνια που συντελείται ευρεία και εύκολη χρήση του διαδικτύου σχεδόν από όλες τις πληθυσμιακές ομάδες, η προστασία των προσωπικών δεδομένων των χρηστών καθίσταται επιτακτική ανάγκη. Κάθε χρήστης που πλοηγείται στο διαδίκτυο, συνδέεται από έναν υπολογιστή, ο οποίος ανήκει σε μια συγκεκριμένη διεύθυνση πρωτοκόλλου διαδικτύου (IP) που επίσης θεωρείται προσωπικό δεδομένο, καθώς μπορεί να πιστοποιήσει την ταυτότητα του χρήστη του υπολογιστή.

Όσον αφορά τη σχετική νομοθεσία, στη χώρα μας, όπως και στις υπόλοιπες ευρωπαϊκές χώρες, τα άτομα προστατεύονται δια του νόμου από την ανεξέλεγκτη χρήση των προσωπικών δεδομένων τους. Ο Αρμόδιος φορέας που υφίσταται για την εφαρμογή του σχετικού νόμου είναι η Αρχή Προστασίας Δεδομένων (Ν. 2472/1997 και 3471/2006). Σύμφωνα με τους εν λόγω νόμους, ισχύει ο κανόνας ότι προκειμένου κανείς να χρησιμοποιήσει προσωπικά δεδομένα απαιτείται να λάβει τη σχετική συγκατάθεση από την Αρχή Προστασίας Δεδομένων. Θα πρέπει, συγκεκριμένα, να υπάρχει συναίνεση για την επεξεργασία και σαφής ενημέρωση για τον επίδοξο χρήστη των δεδομένων, τους λόγους χρήσης τους και τον τρόπο και τον τόπο που αυτά θα χρησιμοποιηθούν. Σε

ειδικές περιπτώσεις, ενδέχεται να επιβληθεί από το νόμο η επεξεργασία κάποιων δεδομένων χωρίς συγκατάθεση, βάσει των σχετικών νόμων που αναφέρουν ρητά τις εν λόγω εξαιρέσεις.

2. Προσωπικά δεδομένα

Από νομικής πλευράς, προσωπικά δεδομένα είναι κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί (αρ. 2 95/46/ΕΚ) Στις χώρες της Βόρειας Αμερικής χρησιμοποιείται ευρύτερα ο όρος Προσωπικής Ταυτοποίησης Προσώπων (Personal Identifiable Information, P.I.I.). Σε όλους τους ορισμούς των προσωπικών δεδομένων χρησιμοποιείται ο όρος ταυτοποίηση. Σύμφωνα με το αρ. 2 της 95/46/F.K, ένα φυσικό πρόσωπο μπορεί να τύχει είτε άμεσης είτε έμμεσης ταυτοποίησης. Η άμεση ταυτοποίηση απαιτεί βασικές πληροφορίες που ανήκουν στο σύνολο των προσωπικών δεδομένων: ονοματεπώνυμο, διεύθυνση, βιομετρικά χαρακτηριστικά κ.λπ. Η έμμεση ταυτοποίηση απαιτεί τον συσχετισμό διάφορων συμπληρωματικών στοιχείων του ατόμου που αφορά ο αριθμός αυτοκινήτου είναι ένα παράδειγμα δεδομένου έμμεσης ταυτοποίησης διότι απαιτείται ο συνδυασμός του με την χρονική στιγμή ταυτοποίησης.

Η Ευρωπαϊκή νομοθεσία έχει προχωρήσει και σε άλλη μια επιπλέον διαβάθμιση των προσωπικών δεδομένων, ως απόρροια της "αμυντικής" θεώρησης του δικαιώματος του πληροφοριακού προσδιορισμού του ατόμου. Διαχωρίζει τα δεδομένα σε απλά προσωπικά και ευαίσθητα. Ευαίσθητα είναι τα δεδομένα που σχετίζονται με την φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές και φιλοσοφικές πεποιθήσεις, την συνδικαλιστική δράση, την υγεία, την κοινωνική πρόνοια, την ερωτική ζωή και τις ποινικές διώξεις και καταδίκες ενός φυσικού προσώπου. Δεδομένα που δεν ανήκουν στις παραπάνω κατηγορίες και μπορούν να χρησιμοποιηθούν για την ταυτοποίηση προσώπων χαρακτηρίζονται απλά προσωπικά δεδομένα. Η διαβάθμιση των δεδομένων έγινε διότι θεωρήθηκε ότι οι κατηγορίες που ανήκουν στα ευαίσθητα, συγκροτούν τον σκληρό πυρήνα της ιδιωτικής σφαίρας και για το λόγο αυτό θα πρέπει να τυγχάνουν διακριτικής προστασίας.

2.1 Τα προσωπικά δεδομένα στο διαδίκτυο

Είναι γεγονός ότι για να έχει πρόσβαση ένας χρήστης του διαδικτύου σε κάποιες σελίδες θα πρέπει να δώσει τα προσωπικά του στοιχεία. Αυτή η πρακτική είναι εντελώς διαφορετική από την κατάσταση κατά την οποία οι πληροφορίες στέλνονται ταχυδρομικώς παρόλο που πάλι είναι γνωστά σε τρίτους, συνήθως εταιρίες, το όνομα και η διεύθυνση του υποκειμένου. Ωστόσο, στην σύγχρονη οικονομία η παρουσία ή απουσία ανταγωνισμού παίζει τεράστιο ρόλο. Πολλές εταιρίες μπορούν να δώσουν πρόσβαση στη σελίδα τους χωρίς να ζητήσουν περεταίρω στοιχεία, ενώ άλλες μπορούν να ζητήσουν πρώτα την παροχή προσωπικών στοιχείων. Παρόμοια, κάποιες εταιρίες μπορούν να στέλνουν spam (διαφημιστικά μηνύματα χωρίς την άδεια του χρήστη να λαμβάνει τέτοιου είδους αλληλογραφία), ενώ άλλες το αποφεύγουν. Για τους καταναλωτές είναι λοιπόν σκόπιμο να χρησιμοποιούν τεχνολογικά μέσα κατά αυτών των μηνυμάτων.

2.2 Ιδιωτικότητα, Απόρρητο και Ασφάλεια

Η έννοια της ιδιωτικότητας συχνά ορίζει τον απόρρητο χαρακτήρα ορισμένων ζητημάτων και με αυτόν τον τρόπο προσβάλλεται η αποκάλυψη απόρρητης πληροφορίας. Πολλές φορές βέβαια παρατηρείται σύγχυση ή και ταύτιση της έννοιας όταν χρησιμοποιείται με τον προσδιορισμό του καταφύγιου (Refugium) και του απορρήτου (Secrecy) και της εμπιστευτικότητας (Confidentiality). Οι συγκεκριμένοι όροι αν και παρουσιάζουν πολλά όμοια χαρακτηριστικά και αναλύσουν παρεμφερείς αξιώσεις προστασίας ωστόσο δεν πρέπει να ταυτίζονται.

Η έννοια του απορρήτου (Secrecy) αναφέρεται είτε στη μη πρόσβαση ορισμένων πληροφοριών που εμπίπτουν στη σφαίρα επιρροής ενός ατόμου είτε στο καθήκον ή την υποχρέωση προσώπων ή οργανισμών να διαφυλάσσουν πληροφορίες, που είτε ένα άτομο έχει εμπιστευτεί σε αυτά, στο πλαίσιο μιας γενικότερης σχέσης εμπιστοσύνης (όπως το ιατρικό απόρρητο ή το τραπεζικό απόρρητο), είτε τις κατέχουν λόγω θέσης και αρμοδιότητας (όπως το υπηρεσιακό απόρρητο). Αυτό σημαίνει πως κάποια πληροφορία σχετική με το δημόσιο χώρο δεν θεωρείται ότι προστατεύεται από το απόρρητο. Για να είναι απόρρητη/εμπιστευτική η πληροφορία θα πρέπει να είναι σε μία κατάσταση όπου

θα υπάρχει περιορισμός στην πρόσβαση τόσο από πρόσωπα όσο και από ομάδες κ.α. (Μήτρου, 2010). Με βάση αυτά, γίνεται για πρώτη φορά μια προσπάθεια να καταγραφούν οι βασικοί παράμετροι για την αποτίμηση της επικινδυνότητας (Risk Assessment) μέσω της ανάλυσης τόσο των δυνητικών απειλών (Threats) που υφίστανται οι συναλλαγές των πολιτών και των επιχειρήσεων σε περιβάλλον υπηρεσιών ηλεκτρονικής διακυβέρνησης, όσο και των αρνητικών επιπτώσεων (Impact) που μπορούν να προκληθούν στον πάροχο της υπηρεσίας ή και στο χρήστη.

2.3 Νομικό-Κανονιστικό Πλαίσιο Προστασίας της Ιδιωτικότητας

Ως προς το νομικό πλαίσιο προστασίας της ιδιωτικότητας παρατηρείται πως δεν προστατεύει τα προσωπικά δεδομένα με βάση το δικαίωμα στην ιδιωτική ζωή, αλλά καθορίζει την προστασία στα πλαίσια της αξίας της ιδιωτικότητας του κάθε ατόμου. Έτσι, με αυτό τον τρόπο παρέχει προστασία στο άτομο σε περιπτώσεις εισβολής και παρέμβασης στον ιδιωτικό του χώρο, καθώς και σε περιπτώσεις καταπίεσης, χειραγώγησης, ελεγκτικής και πατερναλιστικής συμπεριφοράς που έχει σκοπό τον περιορισμό της ελευθερίας του προσώπου στο να αναπτύσσει την προσωπικότητα του, να απολαμβάνει και να διαμορφώνει τις σχέσεις του με τους συνανθρώπους του και γενικότερα να αυτοπροσδιορίζεται (Ακριβοπούλου, 2009). Πάνω σε αυτά τα δεδομένα εξασφαλίζεται και η προστασία ως προς την ταυτότητα και τη δυνατότητα το κάθε άτομο να επιλέγει εναλλακτικές μορφές ζωής (όσον αφορά την σεξουαλικότητα ή τις σχέσεις οικειότητάς του) χωρίς να υπάρχουν κρούσματα κριτικής, χειραγώγησης ή εξευτελιστικής συμπεριφοράς.

2.3.1 Κατευθυντήριες Αρχές που διέπουν την Προστασία της Ιδιωτικότητας

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης έχει ορίσει στις Κατευθυντήριες Οδηγίες για την Προστασία της Ιδιωτικότητας και τη Διασυνοριακή Ροή των Προσωπικών Δεδομένων (Clarke, 2009) βασικές αρχές που προστατεύουν τα

προσωπικά δεδομένα και υπάρχουν σε όλους σχεδόν τους σύγχρονους νόμους των δημοκρατικών χωρών σε παγκόσμιο επίπεδο. Οι αρχές αυτές είναι οι εξής:

Αρχή περιορισμού της συλλογής (Collection Limitation Principle): Θα πρέπει να υπάρχουν όρια στη συλλογή προσωπικών δεδομένων, η συλλογή τους θα πρέπει να πραγματοποιείται με χρήση θεμιτών και σύννομων μέσων και - όπου είναι δυνατό - με τη συναίνεση ή την ενημέρωση του χρήστη.

Αρχή ποιότητας των δεδομένων (Data Quality Principle): Τα προσωπικά δεδομένα θα πρέπει να είναι σχετικά με το σκοπό για τον οποίο πρόκειται να χρησιμοποιηθούν ενώ - στο βαθμό που είναι απαραίτητο για το σκοπό αυτό - θα πρέπει να είναι πλήρη, ακριβή και ενημερωμένα.

Αρχή προσδιορισμού του σκοπού (Purpose Specification Principle): Ο σκοπός για τον οποίο συλλέγονται προσωπικά δεδομένα θα πρέπει να προσδιορίζεται το αργότερο κατά τη χρονική στιγμή της συλλογής τους, ενώ η συνακόλουθη χρήση τους θα πρέπει να περιορίζεται στην εκπλήρωση του σκοπού αυτού ή κάποιου πλήρως συμβατού σκοπού.

Αρχή περιορισμού της χρήσης (Use Limitation Principle)**:** Τα προσωπικά δεδομένα δε θα πρέπει να κοινοποιούνται σε τρίτες οντότητες ή να χρησιμοποιούνται για άλλο σκοπό εκτός από τον προσδιορισμένο, σύμφωνα με την αρχή προσδιορισμού του σκοπού, εκτός εάν υπάρχει η σχετική συναίνεση του χρήστη ή η εξουσιοδότηση από το νόμο.

Αρχή προστασίας της ασφάλειας (Security Safeguards Principle)**:** Τα προσωπικά δεδομένα θα πρέπει να προστατεύονται με χρήση των κατάλληλων μηχανισμών απέναντι σε κινδύνους, όπως η μη εξουσιοδοτημένη πρόσβαση, καταστροφή, χρήση, τροποποίηση ή κοινοποίηση σε τρίτες οντότητες.

Αρχή της διαφάνειας (Openness Principle): Θα πρέπει να υπάρχει γενική διαφάνεια αναφορικά με τις πολιτικές και τις πρακτικές που σχετίζονται με τη συλλογή και επεξεργασία των προσωπικών δεδομένων, καθώς και με την ταυτότητα του φορέα που διενεργεί τη συλλογή και επεξεργασία.

Αρχή της συμμετοχής του ατόμου (Individual Participation Principle): Το κάθε άτομο θα πρέπει να έχει το δικαίωμα:

- *Να αποκτά είτε απ' ευθείας από τον υπεύθυνο της επεξεργασίας είτε μέσω κάποιου άλλου τρόπου, επιβεβαίωση αναφορικά με το αν ο υπεύθυνος της επεξεργασίας διαθέτει δεδομένα που σχετίζονται με το εν λόγω άτομο.*
- *Να του ανακοινώνονται δεδομένα που σχετίζονται με αυτό, μέσα σε εύλογο χρονικό διάστημα, με εύλογο τρόπο, σε μορφή εύκολα κατανοητή και εφόσον η ανακοίνωση προϋποθέτει κόστος, αυτό να μην είναι υπερβολικό.*
- *Να του παρέχονται οι λόγοι για τους οποίους απορρίπτονται αιτήσεις του που αναφέρονται στις δύο παραπάνω παραγράφους και να διατηρεί στην περίπτωση αυτή τη δυνατότητα της αμφισβήτησης, της απόρριψης και της περαιτέρω διεκδίκησης.*
- *Να αμφισβητεί προσωπικά δεδομένα που σχετίζονται με αυτό, και, σε περίπτωση επιτυχημένης αμφισβήτησης, να μπορεί να προχωρεί σε εξάλειψη, διόρθωση ή ολοκλήρωση των δεδομένων αυτών.*

Αρχή της ευθύνης και λογοδοσίας (Accountability Principle): Κάθε υπεύθυνος της επεξεργασίας δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι υπόλογος, αναφορικά με την εφαρμογή των μέτρων εκείνων που προάγουν τις παραπάνω αρχές, που πρέπει να διέπουν την προστασία των προσωπικών δεδομένων.

Η χώρα μας είναι από τις πρώτες χώρες που ενσωμάτωσαν την κοινοτική οδηγία 95/46/ΕΚ στο εσωτερικό δίκαιο. Πολλές προτάσεις νόμου που κατατέθηκαν στο Κοινοβούλιο αλλά και προσχέδια νόμου εκποιήθηκαν από το 1985 που όμως πολλά από αυτά δεν απέδωσαν στην πράξη (Μήτρου, 2010). Παράλληλα, στα πλαίσια της ελληνικής νομοθεσίας, το άρθρο 9 Α του Συντάγματος είναι αυτό που ορίζει την προστασία των προσωπικών δεδομένων ως συνταγματικό δικαίωμα καθώς επίσης και ο νόμος 2472/97 (ΦΕΚ Α' 50/10.04.1997) που ορίζει την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Επιπλέον, υπάρχει και ο νόμος 3471/06 (ΦΕΚ Α' 133/28.06.2006) που - εκτός των τροποποιήσεων που επέφερε στον Ν. 2472/97 – σχετίζεται με την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Μήτρου, 2010). Ο σχετικός νόμος μετέφερε τις ρυθμίσεις της Οδηγίας 95/46/ΕΚ για την προστασία δεδομένων στην ελληνική έννομη τάξη. Σκοπός του είναι η θεσμοθέτηση προϋποθέσεων για την επεξεργασία δεδομένων

με προσωπικό χαρακτήρα, με στόχο την προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και της ιδιωτικής ζωής. Έτσι, βάσει νόμου, ορίζονται οργανωτικοί, διαδικαστικοί και κυρωτικοί κανόνες για την επεξεργασία προσωπικών δεδομένων με σκοπό την ορθή ροή τους στο πλαίσιο του κράτους, της οικονομίας και της κοινωνίας καθώς επίσης οργανώνονται και οι πληροφοριακές σχέσεις μεταξύ των προσώπων (Μήτρου, 2010).

Με τον όρο επεξεργασία προσωπικών δεδομένων εννοείται η κάθε εργασία ή σειρά εργασιών που πραγματοποιείται από το δημόσιο ή από νομικό πρόσωπο δημοσίου ή ιδιωτικού δικαίου ή από ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα. Υπεύθυνος επεξεργασίας θεωρείται οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός.

Ο Ν. 2472/97 ενσωματώνει τις ρυθμίσεις της Οδηγίας 95/46/ΕΚ επιτρέποντας την επεξεργασία δεδομένων προσωπικού χαρακτήρα στις περιπτώσεις όπου:

- *Το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του,*
- *Εντάσσεται στο πλαίσιο της εκπλήρωσης μίας συμβατικής σχέσης στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος. Είναι αναγκαία για την εκπλήρωση υποχρέωσης από το νόμο,*
- *Αποσκοπεί στη διαφύλαξη ζωτικού συμφέροντος του προσώπου στο οποίο αναφέρονται τα δεδομένα,*
- *Είναι απαραίτητη για την εκπλήρωση έργου δημοσίου συμφέροντος και*
- *Κρίνεται αναγκαία για την ικανοποίηση του έννομου συμφέροντος του υπεύθυνου επεξεργασίας, εφόσον δεν προέχει το συμφέρον του υποκειμένου των δεδομένων.*

Η προστασία των προσωπικών δεδομένων είναι κάτι που μπορεί να δεχτεί σταδιακές διαμορφώσεις παράλληλα με την εξέλιξη της Πληροφορίας (Information Age) και αποτελεί στοιχείο της νέας πληροφοριακής έννομης τάξης. Η παγκοσμιοποίηση της επεξεργασίας και της τεχνολογίας, οι αλλαγές των αντιλήψεων σχετικά με το περιεχόμενο της ιδιωτικότητας σχετικά με τη σχέση της με άλλα ιδιωτικά και δημόσια

αγαθά, τόσο σε ατομικό όσο και σε κρατικό-κοινωνικό επίπεδο αλλά και άλλοι τεχνολογικοί παράγοντες, είναι στοιχεία που καθορίζουν τα όρια της ιδιωτικότητας και της προστασίας. Στο χώρο της ιδιωτικότητας της πληροφόρησης παρατηρείται μια σχετική κρίση καθώς επηρεάζεται τόσο από την παρούσα κατάσταση όσο και από τα βασικά χαρακτηριστικά των ΤΠΕ , τον τρόπο δηλαδή εξέλιξης και λειτουργίας τους. Από τη μία πλευρά οι νέες τεχνολογίες είναι αυτές που αποτελούν προϊόν της κοινωνίας και προσδιορίζονται από αυτή, από την άλλη πλευρά οι ίδιες καθορίζουν και επηρεάζουν σε πολλές περιπτώσεις την εξέλιξη της κοινωνίας και τους θεσμούς της.

Έτσι, με τη ραγδαία ανάπτυξη των τεχνολογιών της πληροφορίας και επικοινωνίας έχουν παρατηρηθεί σημαντικές αλλαγές τόσο στις πληροφορίες και τις υπηρεσίες όσο και στον καθορισμό των κοινωνικών και οικονομικών δομών και σχέσεων (Μήτρου, 2010).

3. Οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας και η προστασία της

Η ανεπάρκεια του μέχρι προσφάτου κανονιστικού πλαισίου δημιουργεί κινδύνους στην ιδιωτικότητα. Ήδη από τη δεκαετία του ΄90 ήταν κατανοητό ότι η ιδιωτικότητα δεν είναι αντιμέτωπη με την τεχνολογία. Η τεχνολογία πάντα θα εξελίσσεται και η ιδιωτικότητα θα πρέπει αντίστοιχα να προστατεύεται με τέτοιο τρόπο που να συμβαδίζει με τις τεχνολογικές εξελίξεις Με τον τρόπο αυτό η τεχνολογία γίνεται σύμμαχος της ιδιωτικότητας μέχρι την στιγμή που τα νομοθετικά πλαίσια θα μπορούν να δημιουργήσουν μια επαρκή προστασία.

Η πρώτη προσπάθεια για την ενίσχυση της ιδιωτικότητας στην νέα ψηφιακή εποχή έγινε με τις «Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας» (Privacy-Enhancing Technologies ή PETS) που βασίζονταν στην ιδέα ότι η τεχνολογία μπορεί να ενισχύσει την ιδιωτικότητα και όχι να την καταπατήσει. Οι PETs είναι τεχνολογίες Πληροφορικής που

προστατεύουν την ιδιωτικότητα στα πληροφοριακά συστήματα αποτρέποντας την περιττή ή παράνομη συλλογή, χρήση και αποκάλυψη προσωπικών δεδομένων. Οι συγκεκριμένες τεχνολογίες δίνουν παράλληλα τα κατάλληλα εργαλεία σε κάθε άτομο προκειμένου να μπορούν μόνα τους να ελέγχουν τα προσωπικά τους δεδομένα. Η κρυπτογραφία είναι ένα παράδειγμα όπου μπορούν τα άτομα και οι οργανισμοί να προστατέψουν τα προσωπικά τους δεδομένα στη σημερινή εποχή όπου το διαδίκτυο αποτελεί το σημαντικότερο μέσω επικοινωνίας και συναλλαγών. Για την ανάπτυξη των PETs, έγινε ενσωμάτωση καθολικών αρχών για την διαχείριση προσωπικών δεδομένων, στον κώδικα λειτουργίας των τεχνολογιών και των συστημάτων επεξεργασίας πληροφοριών. Οι αρχές αυτές είναι οι εξής:

1. Καθορισμός σκοπού και περιορισμών χρήσης –*Είναι σημαντικό να καθορίζονται οι λόγοι για την συλλογή, την χρήση, την αποκάλυψη και την διατήρηση προσωπικών πληροφοριών πριν την συλλογή. Οι προσωπικές πληροφορίες δεν θα πρέπει να χρησιμοποιηθούν ή να γνωστοποιηθούν σε τρίτους για σκοπούς διαφορετικούς από αυτούς που αρχικά συλλέχθηκαν εκτός και αν υπάρχει συγκατάθεση του προσώπου το οποίο αφορούν.*

2. Συμμετοχή του ατόμου – *Κάθε άτομο θα πρέπει να έχει την δυνατότητα να ασκεί έλεγχο στα προσωπικά του δεδομένα κατά την διάρκεια της ζωής τους.*

3. Υψηλή προστασία - *Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων προσωπικού χαρακτήρα θα πρέπει να διαφυλαχθεί, ανάλογα με την ευαισθησία των πληροφοριών.*

Παράλληλα οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας και η προστασία της ιδιωτικότητας αυξάνουν τις δυνατότητες του ατόμου στον έλεγχο της επεξεργασίας των προσωπικών του πληροφοριών και παράλληλα παρέχουν τις εξής λειτουργίες (Cavoukian, 2011):

- *Αποτροπή της μη εξουσιοδοτημένης πρόσβασης σε προσωπικές επικοινωνίες και αποθηκευμένα αρχεία.*

- *Αυτοματοποίηση της ανάκτησης πληροφοριών που σχετίζονται με τις πρακτικές προστασίας της ιδιωτικότητας που χρησιμοποιεί ο συλλέκτης των δεδομένων, καθώς και αυτοματοποίηση των αποφάσεων του ατόμου με βάση αυτές τις πρακτικές.*
- *Αποτροπή της αυτοματοποιημένης συλλογής δεδομένων μέσω cookies, HTTP επικεφαλίδων, σφαλμάτων ιστού(web bugs) και spyware.*
- *Αποτροπή σύνδεσης επικοινωνιών με συγκριμένα άτομα.*
- *Διευκόλυνση συναλλαγών που αποκαλύπτουν ελάχιστες προσωπικές πληροφορίες.*
- *Φιλτράρισμα ανεπιθύμητων μηνυμάτων.*

Οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας (TEI) μπορούν να χωριστούν σε δύο γενικές κατηγορίες: Τις TEI που δρουν ως υποκατάστατα (substitute PETs – οι οποίες υποκαθιστούν τους κανονισμούς που αφορούν την ιδιωτικότητα θωρακίζοντας την ψηφιακή ταυτότητα του υποκειμένου και αποτρέποντας την συλλογή των προσωπικών δεδομένων ή των προσωπικά αναγνωρίσιμων δεδομένων (Personal Identifiable Information)) και τις TEI που δρουν συμπληρωματικά (complementary PETs – Οι οποίες βοηθούν στην επίτευξη των κανονιστικών στόχων χρησιμοποιώντας τεχνικά μέτρα).

4. Επιπτώσεις Ιδιωτικότητας

Μία σημαντική παραβίαση ιδιωτικότητας σε έναν οργανισμό ή σε μία διαδικασία οργανισμού μπορεί να εγκυμονεί κινδύνους και απειλές, όπου θα έχουν επιπτώσεις σε αυτόν, στα μέλη του και στο περιβάλλον που τον απαρτίζει. Στην κοινωνία της πληροφορίας, υπάρχουν σοβαροί κίνδυνοι για την ιδιωτικότητα. Στο παρόν κεφάλαιο, θα προσδιοριστεί ο όρος της απειλής και θα κατηγοριοποιηθεί σύμφωνα με παραδείγματα που αναφέρονται.

4.1 Εννοιολογικός προσδιορισμός Απειλών - Επιπτώσεων

Ως απειλή ορίζεται οποιαδήποτε «*πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσότερων ιδιοτήτων των χαρακτηριστικών ασφαλείας ενός πληροφοριακού συστήματος»* (Vrakas et al., 2010). Οι απειλές που σχετίζονται με τα συστήματα πληροφόρησης, δεν θεωρούνται μόνο οι κακόβουλες ενέργειες που προκαλούνται από εξωτερικές ή εσωτερικές οντότητες, αλλά συμπεριλαμβάνουν και σχεδιαστικά λάθη ή μη ηθελημένες ενέργειες που μπορούν να οδηγήσουν το πληροφοριακό σύστημα στην αποτυχία υλοποίησης των στόχων του.

Με τον όρο ανάλυση επικινδυνότητας (Risk Analysis) εννοούμε τη διαδικασία αναγνώρισης κινδύνων καθώς και τον υπολογισμό επικινδυνότητας. Η εκτίμηση επικινδυνότητας (Risk Assessment) είναι η διαδικασία αξιολόγησης της υπολογισμένης επικινδυνότητας σε σχέση με κριτήρια αξιολόγησης της σημαντικότητάς της (Vrakas et al., 2010)

Η ανάλυση επικινδυνότητας είναι η διαδικασία αναγνώρισης κινδύνων και ο υπολογισμός επικινδυνότητας. Η εκτίμηση επικινδυνότητας (Risk Assessment) είναι η διαδικασία αξιολόγησης της υπολογισμένης επικινδυνότητας σε σχέση με κριτήρια αξιολόγησης της σημαντικότητάς της (Tsohou et al., 2011). Η συγκεκριμένη διαδικασία γενικά αποτελεί την αποτίμηση επικινδυνότητας καθώς αυτή (Risk Assessment and Management) στηρίζεται στην αρχή ότι απόλυτη ασφάλεια δεν είναι δυνατό να υπάρξει, άρα το καλύτερο που μπορεί να γίνει είναι να εξισορροπηθεί η

έκταση των πιθανών κινδύνων με το κόστος εφαρμογής των κατάλληλων αντιμέτρων (Countermeasures). Με τον τρόπο αυτό είναι ορθό να υπάρχουν μεθοδολογίες που να επιτρέπουν τη μέτρηση των κινδύνων και την έκφρασή τους σε κοινές μονάδες μέτρησης με την αποτελεσματικότητα των αντιμέτρων, ώστε να είναι δυνατή η σύγκρισή τους.

4.2 Κατηγορίες Απειλών

Όταν ένας πολίτης κάνει μια τυπική συναλλαγή με το Δημόσιο, απαιτείται συνήθως η φυσική παρουσία του σε έναν εξουσιοδοτημένο δημόσιο υπάλληλο. Με τον τρόπο αυτό η ταυτοποίηση των στοιχείων πραγματοποιείται με τη φυσική παρουσία του ατόμου ενώ η αυθεντικότητα αυτών των στοιχείων γίνεται με την προσκόμιση κατάλληλου εγγράφου το οποίο διαφέρει ανάλογα με το είδος της συναλλαγής και τη Δημόσια Αρχή. Για παράδειγμα, για την έκδοση Αποδεικτικού Φορολογικής Ενημερότητας (Α.Φ.Ε.) ή για την υποβολή Δήλωσης Φορολογίας Εισοδήματος απαιτείται η φυσική παρουσία του ενδιαφερομένου σε μία Δημόσια Οικονομική Υπηρεσία (Δ.Ο.Υ.), προκειμένου αυτός να ταυτοποιηθεί, και ακολουθεί επίδειξη εγγράφου από το οποίο προκύπτει ο Αριθμός Δελτίου Ταυτότητας (Α.Δ.Τ.) ή ο Αριθμός Διαβατηρίου (Α.Δ.) προκειμένου να αποδειχθεί η αυθεντικότητα τους. Συνεπώς, αρχικά ο πολίτης ταυτοποιείται και στη συνέχεια αυθεντικοποιείται με την αξιοποίηση του κατάλληλου εγγράφου. Με όλα τα παραπάνω θεωρείται απίθανη η περίπτωση μία οντότητα να υποδυθεί μία άλλη. Χωρίς αυτούς τους περιορισμούς είναι πολύ πιθανό να υπήρχαν κρούσματα χρήσης πλαστών στοιχείων από τον ενδιαφερόμενο είτε απουσία ουσιαστικού ελέγχου από την πλευρά του δημοσίου υπαλλήλου.

Ο τρόπος παράκαμψης αυτών των περιορισμών θα συμπεριλάμβανε είτε τη χρήση πλαστών στοιχείων από τον ενδιαφερόμενο είτε την απουσία ουσιαστικού ελέγχου από την πλευρά του δημοσίου υπαλλήλου.

Από την άλλη πλευρά, ο κίνδυνος που υπάρχει στις υπηρεσίες ηλεκτρονικής διακυβέρνησης είναι ότι ένας δυνητικά κακόβουλος χρήστης δεν θα προσπαθήσει μόνο να εκμεταλλευτεί γνωστές ευπάθειες (Vulnerabilities) του συστήματος, αντίστοιχες με αυτές που εμφανίζονται στις υπηρεσίες Διαδικτύου, αλλά και στις συγκεκριμένες

διαδικασίες εγγραφής, ταυτοποίησης και αυθεντικοποίησης, ανεξαρτήτως του τρόπου πραγματοποίησής τους, ηλεκτρονικά ή μη (Palanisamy & Mukerji, 2012).

4.3 Πιθανές Επιπτώσεις Απειλών - Κινδύνων

Υπάρχουν πολλές διαφορετικές επιπτώσεις των απειλών αυτών στους χρήστες και τους δημόσιους φορείς που σχετίζονται με τις υπηρεσίες ηλεκτρονικής διακυβέρνησης, όταν αυτές αξιοποιηθούν σε μία επίθεση. Στον παρακάτω πίνακα παρουσιάζονται ενδεικτικά κάποιες πιθανές επιπτώσεις που μπορεί να έχουν οι κίνδυνοι αυτοί, τόσο στους χρήστες όσο και στους δημόσιους φορείς, ως προς το επίπεδο εμπιστοσύνης που εντάσσεται η υπηρεσία. Ωστόσο ο πίνακας αυτός είναι ενδεικτικός και δεν μπορεί να αποτελέσει πηγή αποτύπωσης των επιπτώσεων καθώς υπάρχουν μεγάλες διαφοροποιήσεις ανάλογα με την υπηρεσία και τις ποικίλες επιπτώσεις (νομικές, οικονομικές κτλ) που θα μπορούσε να υποστεί ο φορέας.

5. Αξιολόγηση Επιπτώσεων Ιδιωτικότητας

5.1 Αντικείμενο της ΑΕΙ

Η Αξιολόγηση Επιπτώσεων στην Ιδιωτικότητα είναι ένα εργαλείο που χρησιμοποιούν οι οργανισμοί με σκοπό την εξασφάλιση ότι κατά τη διάρκεια σχεδιασμού ενός συστήματος, ή μίας διαδικασίας, καλύπτονται οι ανάγκες του συστήματος σχετικά με την ιδιωτικότητα. Οι εφαρμογές της ΑΕΙ εφαρμόζονται με κατευθυνόμενες ερωτήσεις που βασίζονται στις απαιτήσεις της ιδιωτικότητας και είναι εξαιρετικές για την εφαρμογή των αρχών της Ιδιωτικότητας δια του Σχεδιασμού στον οργανισμό (Cavoukian, 2013). Πολλές φορές , οι Αξιολογήσεις Επιπτώσεων στην Ιδιωτικότητα, διεξάγονται παράλληλα με τις αξιολογήσεις απειλών/επικινδυνότητας που είναι βασικές για την συνολική προστασία της ιδιωτικότητας.

Μία ΑΕΙ στοχεύει σε δύο κυρίως πράγματα: Αρχικά συντελεί στην συμμόρφωση του οργανισμού ως προς τις νομικές και ρυθμιστικές απαιτήσεις που αφορούν την ιδιωτικότητα και δεύτερον βοηθά στο χτίσιμο και στην εξωτερίκευση του προγράμματος διαχείρισης πληροφοριών και επικινδυνότητας του οργανισμού, που συμπεριλαμβάνει την γνωστοποίηση των αρχών της Ιδιωτικότητας δια του Σχεδιασμού. Ο δεύτερος στόχος έχει ιδιαίτερη σημασία για τα άτομα τα οποία δεν σχετίζονται άμεσα με τη διασφάλιση της ιδιωτικότητας του οργανισμού καθώς τα βοηθά να καταλάβουν καλύτερα την αξία της αξιολόγησης, την σημασία της στην διεκπεραίωση της εργασίας τους, καθώς και τον ρόλο που παίζει στο να αυξάνει το κύρος του οργανισμού.

Οι κίνδυνοι της ιδιωτικότητας μπορεί να προκύψουν από οποιαδήποτε πηγή, όπως για παράδειγμα από τα τρωτά σημεία στην οργάνωση ή το σχεδιασμό και την υλοποίηση ενός έργου, από εξωτερικές απειλές, π.χ., από κακόβουλες πρακτικές που έχουν να κάνουν με τα πληροφορικά συστήματα των οργανισμών, παρέχοντας ή αποσπώντας πληροφορίες, εκμεταλλευόμενοι τις αδυναμίες στις διαδικασίες ελέγχου πρόσβασης του οργανισμού. Σχεδόν όλοι οι οδηγοί ΑΕΙ που χρησιμοποιούνται στην Αυστραλία, τον Καναδά, τη Νέα Ζηλανδία, το Ηνωμένο Βασίλειο και τις ΗΠΑ εντοπίζουν τους κινδύνους που αντιμετωπίζει ένας οργανισμός που σχετίζεται με τη συλλογή και επεξεργασία των προσωπικών δεδομένων.

Είναι αρκετά χρήσιμο σε αυτό το σημείο να γίνει διάκριση μεταξύ των τρωτών σημείων των περιουσιακών στοιχείων, των απειλών και των κινδύνων, όπως ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) τις θέτει στις αξιολογήσεις κινδύνου των νέων τεχνολογιών της πληροφορίας και των επικοινωνιών. Ο ENISA ορίζει τον κίνδυνο ως «την δυνατότητα για μια συγκεκριμένη απειλή να εκμεταλλεύεται τα τρωτά σημεία ενός περιουσιακού στοιχείου ή μιας ομάδας περιουσιακών στοιχείων και έτσι να προκαλέσει βλάβη στον οργανισμό». Αυτός ο ορισμός ταυτίζεται με τον ορισμό που χρησιμοποιείται στο πρότυπο ISO 27005.

Σύμφωνα με το πρότυπο ISO 27005, ένα περιουσιακό στοιχείο είναι κάτι που έχει αξία σε έναν οργανισμό και το οποίο συνεπώς απαιτεί προστασία. Ο προσδιορισμός των περιουσιακών στοιχείων είναι ένα σύνθετο και δύσκολο εγχείρημα, αλλά πολύ

σημαντικό, δεδομένου ότι αυτό θα αποτελέσει τη βάση επί της οποίας θα πραγματοποιηθεί η αξιολόγηση των επιπτώσεων και των κινδύνων της ιδιωτικότητας.

Ο προσδιορισμός των περιουσιακών στοιχείων θα πρέπει να γίνεται ιδανικά σε ένα κατάλληλο βαθμό λεπτομερειών και σύμφωνα με τις ανάγκες και το πεδίο εφαρμογής της αξιολόγησης του κινδύνου. Τα περιουσιακά στοιχεία μπορεί να είναι επιχειρηματικές διαδικασίες και δραστηριότητες, πληροφορίες ή στοιχεία λογισμικού (και hardware), δίκτυο, προσωπικό, κ.α. Το περιουσιακό στοιχείο αξιολογείται επίσης, αφού η αξία του είναι ένας καθοριστικός παράγοντας για την εκτίμηση των επιπτώσεων ενός συμβάντος παραβίασης της ιδιωτικότητας. Υπάρχουν πολλές διαφορετικές προσεγγίσεις που μπορεί να ακολουθηθούν για γίνει η αξιολόγηση των επιπτώσεων στα περιουσιακά στοιχεία, όπως ο έλεγχος των δαπανών που προκύπτουν από μια παραβίαση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας ως αποτέλεσμα ενός συμβάντος παραβίασης της ιδιωτικότητας.

Μια «απειλή» αναφέρεται σε μια πτυχή ενός συστήματος ή διαδικασίας, η οποία μπορεί να αξιοποιηθεί για διαφορετικούς σκοπούς από εκείνους που προορίζονται αρχικά, στις αδυναμίες, στα κενά ασφαλείας ή στα ελαττώματα μιας εφαρμογής που είναι πιθανόν να απειλείται. Μια ευπάθεια δεν προκαλεί ζημιά από μόνη της: για να θεωρείται μία αδυναμία κίνδυνος, θα πρέπει να αξιοποιηθεί από μια απειλή. Επιπλέον, τα ευάλωτα σημεία είναι ανεξάρτητα από οποιαδήποτε συγκεκριμένη απειλή. Η κατανόηση των τρωτών σημείων αποτελεί σημαντικό μέρος της εκτίμησης ενός κινδύνου, διότι τα ευάλωτα σημεία μπορεί να αυξήσουν τον κίνδυνο, είτε αυξάνοντας την πιθανότητα κάποιου γεγονότος ή τη σοβαρότητα των συνεπειών, ή και των δύο. Οι αποφάσεις σχετικά με το πώς να διαχειρίζονται οι όποιοι δυνητικοί κίνδυνοι θα πρέπει επίσης να περιλαμβάνουν την εξέταση των τρόπων για τη μείωση των τρωτών σημείων. Παρακάτω αναφέρονται μερικά παραδείγματα διαφορετικών τύπων τρωτών σημείων:

- Απροστάτευτες συσκευές αποθήκευσης δεδομένων προσωπικού χαρακτήρα
- Ανεπαρκής έλεγχος του λογισμικού ή ανεπαρκής μηχανισμός ελέγχου ταυτότητας χρηστών
- Απροστάτευτες γραμμές επικοινωνίας
- Ανεπαρκής έλεγχος νέων προσλήψεων ή ανεπαρκής κατάρτιση προσωπικού

- Έλλειψη τακτικών ελέγχων από εξωτερικούς ελεγκτές και μη εισαγωγή του λογισμικού σε λειτουργικά συστήματα.

Μια απειλή έχει τη δυνατότητα να βλάψει ή να θέσει σε κίνδυνο τα περιουσιακά στοιχεία ενός οργανισμού, όπως πληροφορίες, διαδικασίες και συστήματα. Οι απειλές μπορεί να είναι φυσικής ή ανθρώπινης προέλευσης, και μπορεί να είναι ακούσιες ή εκούσιες. Μια απειλή μπορεί να προκύψει από το εσωτερικό ή από το εξωτερικό περιβάλλον της επιχείρησης. Οι φυσικές ή περιβαλλοντικές απειλές, όπως πυρκαγιές, σεισμοί, πλημμύρες ή μια βλάβη στην παροχή ρεύματος ή τηλεπικοινωνιακών υπηρεσιών μπορεί να προκαλέσουν βλάβη στους υπολογιστές, στους servers και στα δίκτυα που χρησιμοποιούνται από μια οργάνωση για την αποθήκευση ή την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Αυτά τα δεδομένα μπορεί επίσης να τεθούν σε κίνδυνο από άλλες απειλές, όπως είναι οι ακόλουθες:

- Η παρακολούθηση των επικοινωνιών
- Κατασκοπεία
- Κλοπή εξοπλισμού (κινητά τηλέφωνα, φορητοί υπολογιστές, κάρτες μνήμης)
- Δεδομένα από αναξιόπιστες πηγές
- Η επέμβαση σε υλικό ή λογισμικό, συμπεριλαμβανομένων των ιών και άλλων κακόβουλων προγραμμάτων
- Παρακολούθηση θέσης - μέσω εντοπισμού κινητών τηλεφώνων
- Η μη εξουσιοδοτημένη χρήση του εξοπλισμού ή παράνομη επεξεργασία των δεδομένων
- Απώλεια των δεδομένων, π.χ., λόγω διακοπής λειτουργίας του δικτύου ή ανθρώπινου λάθους

Μία απροστάτευτη γραμμή επικοινωνίας αποτελεί ένα τρωτό σημείο για έναν οργανισμό. Πιθανές υποκλοπές σε αυτή τη γραμμή αποτελούν μια απειλή. Ο κίνδυνος είναι η πιθανότητα ότι κάποιος θα διαπράξει μία υποκλοπή, η συνέπεια είναι η ζημία που θα προκύψει. Ο κίνδυνος μπορεί να είναι ήσσονος σημασίας ή μείζονος, αναλόγως των συνομιλητών και του περιεχομένου της συνομιλίας. Οι επιχειρήσεις και οι οργανισμοί μπορεί να μην ενθαρρύνουν τους εργαζόμενους τους να χρησιμοποιούν ισχυρούς κωδικούς πρόσβασης, και αυτό δημιουργεί την απειλή ενός χάκερ να εισέλθει σε

ιδιωτικά αρχεία της επιχείρησης. Ο κίνδυνος είναι η πιθανότητα ότι θα το κάνει και η συνέπεια είναι τα αποτελέσματα για την επιχείρηση αν τελικά μπορέσει και εισέλθει. Ο προσδιορισμός του κινδύνου που προέρχεται από διάφορα τρωτά σημεία και απειλές απαιτεί κάποια ανάλυση και αξιολόγηση, που ουσιαστικά αποτελεί την αξιολόγηση των επιπτώσεων της ιδιωτικότητας.

5.2 Η ΑΕΙ και ο Έλεγχος της Ιδιωτικότητας

Η ΑΕΙ διαφέρει από τον έλεγχο της ιδιωτικότητας ή την συμμόρφωση με το απόρρητο της ιδιωτικότητας τόσο στον χρόνο που πραγματοποιούνται όσο και δυνητικά στο πεδίο εφαρμογής. Οι έλεγχοι προστασίας προσωπικών δεδομένων ή οι αναφορές συμμόρφωσης με τους κανονισμούς προστασίας της ιδιωτικότητας συνήθως αναζητούν τα προσωπικά στοιχεία τα οποία χειρίζεται ένα σύστημα. Από την άλλη, η ΑΕΙ θα πρέπει να είναι διερευνητική και να διενεργεί την εκτίμηση ενός συστήματος προτού αυτό αρχίσει να λειτουργεί. Στην πράξη, βέβαια, η διάκριση αυτή είναι συχνά λιγότερο σαφής, καθώς οι οργανισμοί συχνά αναθέτουν την διαδικασία της ΑΕΙ αργά, και έτσι η ΑΕΙ συχνά συμπίπτει με την έναρξη των εργασιών. Αυτό μπορεί να έχει πλεονεκτήματα, όπως ότι η ΑΕΙ χρησιμοποιείται ως εργαλείο για να κριθεί κατά πόσον ορισμένες επιδράσεις συμβαίνουν, και κατά πόσο τα συνιστώμενα μέτρα δεν αποφέρουν τα επιδιωκόμενα οφέλη.

Οι έλεγχοι προστασίας προσωπικών δεδομένων όπως υποδηλώνει και το όνομα τους, αφορούν αξιολογήσεις συμμόρφωσης με τους κανόνες και εστιάζουν αυστηρά στη συμμόρφωση με τους ισχύοντες νόμους περί προσωπικού απορρήτου, κανονιστικές ρυθμίσεις ή άλλους κανόνες στους οποίους ο χρήστης των δεδομένων υπόκειται. Η ΑΕΙ σε αντίθεση εξετάσει ευρύτερες επιπτώσεις στην ιδιωτική ζωή, συμπεριλαμβανομένου του τρόπου με το οποίον ένα έργο μπορεί να γίνει αντιληπτό από τα υποκείμενα των δεδομένων ή την ευρύτερη κοινότητα. Μία ΑΕΙ η οποία εξετάζει μόνο την αυστηρή τήρηση των κανονισμών δεν θα έχει να παρέχει πολλά στον χρήστη, παρά μόνο τις τυπικές προδιαγραφές τήρησης της ιδιωτικότητας. Μια λεπτομερής ΑΕΙ θα προσδιορίσει τα ζητήματα προστασίας της ιδιωτικότητας που ο ενδιαφερόμενος οργανισμός θα πρέπει

να διαχειριστεί, ακόμη κι αν δεν είναι παραβιάσεις των ισχυόντων ρυθμιστικών κανόνων (Wright & De Hert, 2011).

Το τυπικό μοντέλο που υιοθετήθηκε για την υιοθέτηση και την χρηματοδότηση μιας AEI είναι ότι ο ενδιαφερόμενος που θέλει να αξιολογηθεί επιλέγει τον αξιολογητή και τον πληρώνει για την AEI. Είναι ίσως έκπληξη το γεγονός ότι έχει σημειωθεί σχόλιο σχετικά με την κριτική του μοντέλου αυτού. Το μοντέλο αυτό σαφώς και γεννά ερωτηματικά αφού ο ενδιαφερόμενος που είναι υπό αξιολόγηση, είναι και ο εργοδότης, και έτσι μπορεί να υπάρχει σύγκρουση συμφερόντων. Υπάρχει μια εγγενής τάση για τους αξιολογητές να προσαρμόσουν τα ευρήματά τους με τις προσδοκίες του πελάτη τους – δηλαδή να πουν στον πελάτη ό, τι θέλουν να ακούσει. Ανάλογα με το πόσο ηθικά ακέραιος είναι ο αξιολογητής, μπορεί να είναι περισσότερο ή λιγότερο επιρρεπής στην τάση αυτή. Η παραπάνω διαπίστωση δεν αποτελεί κριτική - εκτός εάν ένας αξιολογητής κλίνει προς τον πραγματισμό που παραλείπει να επιστήσει την προσοχή του πελάτη σε σημαντικές επιπτώσεις. Ιδανικά, η AEI πραγματοποιείται από έναν τρίτο, ενδιάμεσο φορέα ο οποίος αναθέτει την αξιολόγηση σε έναν αξιολογητή, ο οποίος θα πληρωθεί από τον ενδιαφερόμενο. Αυτό θα μπορούσε να απομονώσει τον αξιολογητή από τις πιέσεις που εμπλέκονται σε άμεση σχέση με το έργο (Wright & De Hert, 2011).

5.3 Privacy by Design

Η λογική της προστασίας της ιδιωτικότητας από τον σχεδιασμό καλείται “Privacy by Design (PbD)”. Με την ενσωμάτωση της PbD ο κίνδυνος επέμβασης στην ιδιωτική σφαίρα είναι δυνατό να ελαχιστοποιηθεί ή και να εξαλειφθεί τελείως.

Οι στόχοι του σχεδιασμού της ιδιωτικότητας περιλαμβάνουν τη χρήση πληροφοριακών συστημάτων που να μπορούν να ικανοποιήσουν τους στόχους μιας εταιρίας. Οι τρεις αυτοί στόχοι, αποσκοπούν και στο να υποστηρίξουν τη διαχείριση του ρίσκου της ιδιωτικότητας ενθαρρύνοντας συνεπείς και μετρήσιμες αποφάσεις σχεδιασμού.

1) **Προβλεψιμότητα**: δίνει τη δυνατότητα στα άτομα να πάρουν αξιόπιστες αποφάσεις σχετικά με τη χρήση των προσωπικών πληροφοριών. Η

προβλεψιμότητα βρίσκεται στον πυρήνα της δημιουργίας ενός περιβάλλοντος εμπιστοσύνης και αυτό-προσδιορισμού: ο στόχος είναι να σχεδιαστούν συστήματα έτσι, ώστε οι χρήστες να μην εκπλήσσονται από τον τρόπο που γίνεται η διαχείριση των προσωπικών πληροφοριών. Η λογική αυτή διευκολύνει τους χειριστές να αξιολογήσουν την επίπτωση από τις όποιες αλλαγές υπάρχουν σε ένα πληροφοριακό σύστημα και να εφαρμόσουν τους σχετικούς ελέγχους. Ακόμη και σε ένα σύστημα όπου δημιουργούνται απρόβλεπτα ή άγνωστα έως τώρα αποτελέσματα, η προβλεψιμότητα μπορεί να προσφέρει πληροφόρηση σχετικά με το πώς να ελεγχθεί το ρίσκο που μπορεί να προκύψει σχετικά με την ιδιωτικότητα. Για παράδειγμα, αν τα αποτελέσματα μιας μελέτης είναι εγγενώς απρόβλεπτα, οι χειριστές μπορούν να εφαρμόσουν ελέγχους ώστε να περιορίσουν την πρόσβαση ή τη χρήση αυτών των αποτελεσμάτων.

2) **Δυνατότητα Διαχείρισης**: η ύπαρξη δυνατότητας διαχείρισης των προσωπικών πληροφοριών, συγκαταλεγμένων των δυνατοτήτων αλλαγής, διαγραφής, μετατροπής και επιλεκτικής αποκάλυψης. Η δυνατότητα αυτή, δεν είναι ένα απόλυτο δικαίωμα αλλά περισσότερο μια ιδιοκτησία του συστήματος που επιτρέπει στα άτομα να ελέγχουν την πληροφορία ενώ παράλληλα ελαχιστοποιούν τις πιθανές διενέξεις στη λειτουργία του συστήματος. Το σε τι ακριβώς συνίσταται η δυνατότητα αυτή, θα το κατανοήσουμε αν σκεφτούμε ένα σύστημα για το οποίο υπάρχουν ανησυχίες απάτης. Σε ένα τέτοιο σύστημα, η δυνατότητα αυτής της διαχείρισης, μπορεί να περιορίσει την ικανότητα των ατόμων να επεξεργαστούν ή να διαγράψουν οι ίδιοι τους πληροφορίες, δίνοντας τη δυνατότητα σε έναν διαχειριστή να κάνει αλλαγές ώστε να συντηρήσει την ακριβής και την σωστή αντιμετώπιση των υποκειμένων.
3) **Δυνατότητα αποσύνδεσης πληροφοριών**: σε ένα πληροφοριακό σύστημα πρέπει να υπάρχει η δυνατότητα να γίνεται επεξεργασία προσωπικών πληροφοριών ή γεγονότων χωρίς να συσχετίζονται με τα άτομα ή τις συσκευές που χρησιμοποιούν. Κάποιες αλληλεπιδράσεις, όπως η παροχή υπηρεσιών υγείας ή οι πληρωμές με πιστωτική κάρτα, βασίζονται στην αρχή της ιδιωτικότητας ενώ παράλληλα απαιτείται και ταυτοποίηση του υποκειμένου. Την έννοια αυτή, την αντιλαμβανόμαστε καλύτερα σε αντιπαραβολή με την έννοια της

εμπιστευτικότητας (confidentiality), η οποία εστιάζει στο να αποτρέπεται η χωρίς άδεια πρόσβαση σε πληροφορίες. Η έννοια της δυνατότητας αποσύνδεσης (αποσυσχετισμού) δεδομένων αναγνωρίζει ότι το ρίσκο της παραβίασης της ιδιωτικότητας μπορεί να απορρέει από την έκθεση σε κάτι, ακόμη κι όταν η πρόσβαση επιτρέπεται ή να απορρέει από μια συναλλαγή. Η αρχή επιτρέπει στους σχεδιαστές του συστήματος να ζυγίσουν σκόπιμα τις ανάγκες ταυτοποίησης ενάντια στο ρίσκο παραβίασης της ιδιωτικότητας σε κάθε επίπεδο του σχεδιασμού.

Αυτές οι τρεις αρχές σχεδιασμού στοχεύουν στο να παρέχουν έναν βαθμό ακριβείας και μετρησιμότητας έτσι ώστε οι σχεδιαστές των συστημάτων και οι μηχανικοί, να μπορούν, καθώς δουλεύουν με τα τμήματα που ελέγχουν την πολιτική μιας εταιρίας / ενός οργανισμού κτλ., χρησιμοποιώντας τις αρχές αυτές, να γεφυρώσουν το χάσμα ανάμεσα στις αρχές που υπάρχουν σε υψηλό επίπεδο με πρακτικές εφαρμογές ενός λειτουργικού συστήματος.

Αν και οι Τεχνολογίες Προστασίας της Ιδιωτικότητας και η Ιδιωτικότητα μέσω του Σχεδιασμού δεν είναι αυστηρά καθορισμένες ως προς την έννοια τους, ωστόσο δεν μπορούμε να τις ταυτίσουμε. Οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας[2] είναι εφαρμογές ή εργαλεία με στόχο την προσέγγιση μίας μόνο πλευράς της προστασίας της ιδιωτικότητας, όπως η ανωνυμία, η εμπιστευτικότητα και ο έλεγχος επί των προσωπικών δεδομένων. Συχνά, οι ΤΕΙ μπορεί να προστεθούν μετέπειτα σε ήδη υπάρχοντα συστήματα είτε από τους σχεδιαστές με σκοπό να τις ενισχύσουν, είτε από τους ίδιους τους χρήστες οι οποίοι είναι περισσότερο ευαισθητοποιημένοι σε θέματα ιδιωτικότητας. [16]. Αντιθέτως η Ιδιωτικότητα μέσω του Σχεδιασμού δεν αναφέρεται σε μια συγκεκριμένη τεχνολογία ή προϊόν αλλά σε μια συστηματική προσέγγιση για τον σχεδιασμό οποιασδήποτε νέας τεχνολογίας που ενσωματώνει την προστασία της ιδιωτικότητας στις βασικές προδιαγραφές της.

Με τον τρόπο αυτό η Ιδιωτικότητα δια του σχεδιασμού επιδιώκει να εφαρμόσει τα νομοθετικά και ρυθμιστικά πλαίσια καθώς και τα των Δίκαια Πληροφοριακά Πρακτικά (Fair Information Practices). Αυτό μπορεί από τη μια να πραγματοποιηθεί με τη χρήση

[2] (εν συντομία ΤΕΙ)

υφιστάμενων Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας ή τη δημιουργία νέων, για την αντιμετώπιση των αναδυόμενων κινδύνων κατά της ιδιωτικότητας. Ένας άλλος τρόπος είναι η υιοθέτηση διαδικασιών, συστημάτων, διαδικασιών και πολιτικών που προτείνει η Προστασία της Ιδιωτικότητας δια του Σχεδιασμού. Στα τελευταία μπορούμε να αναφερόμαστε συνολικά με τον όρο διασφαλίσεις της ιδιωτικότητας (privacy safe guards). Οι υπεύθυνοι της Ευρωπαϊκής Ένωσης σε θέματα προστασίας της ιδιωτικότητας έχουν εδώ και καιρό υιοθετήσει τις ΤΕΙ ενώ πιο πρόσφατα άρχισαν να υιοθετούν την Προστασία της Ιδιωτικότητας δια του Σχεδιασμού και να δίνουν έμφαση στην χρήση ορθών πρακτικών στον σχεδιασμό των πληροφοριακών συστημάτων (European Commission, 2015).

5.4 Διαχείριση Κινδύνου Ιδιωτικότητας (Privacy Risk Management)

Οι υπάρχουσες διαδικασίες διαχείρισης ρίσκου, είναι σε θέση να ενσωματώσουν την ιδιωτικότητα και τις 7 θεμελιώδεις αρχές της Ιδιωτικότητας δια του Σχεδιασμού ώστε με τον τρόπο αυτό να οδηγήσουν στη δημιουργία της Διαχείρισης Κινδύνου Ιδιωτικότητας (Privacy Risk Management - PRM). Η επιτυχία της συγκεκριμένης, σχετίζεται τόσο από τον τρόπο χειρισμού των θεμάτων από τον οργανισμό όσο και από τους κανόνες που έχουν θεσπιστεί για την αντιμετώπιση του κινδύνου.

Παρατηρείται ότι οι οργανισμοί με μέτριες έως προηγμένες δυνατότητες διαχείρισης κινδύνου τείνουν να επενδύουν στην Διαχείριση Κινδύνου Ιδιωτικότητας. Με την ενσωμάτωση της ιδιωτικότητας στα ήδη υπάρχοντα προγράμματα τους μπορούν να καταφέρουν να διαχειριστούν με παρόμοιο τρόπο άλλων κινδύνων, τους κινδύνους που σχετίζονται με την προστασία των προσωπικών δεδομένων. Αξιοποιώντας την PRM, ένας οργανισμός ενισχύει το κύρος του και τις επιδόσεις του καθώς τα μέτρα δρουν προληπτικά και όχι αντιδραστικά. Τα άτομα που σχετίζονται με την Διαχείριση Κινδύνου Ιδιωτικότητας μπορούν να γίνουν κοινωνοί της αλλαγής του ρόλου της ιδιωτικότητας στον οργανισμό. Εφόσον βέβαια υπάρξει και η κατάλληλη υποστήριξη από τα διευθυντικά στελέχη.

5.5 Επιπτώσεις Ιδιωτικότητας και Αντιμετώπιση

Η ΑΕΙ δεν θα πρέπει μόνο να εξετάζει τις επιπτώσεις στην προστασία της ιδιωτικής ζωής, αλλά και τις επιπτώσεις σε μια οργάνωση που απορρέουν από το συμβιβασμό της που προκαλεί η ιδιωτικότητα. Πολλοί οργανισμοί αδιαφορούν για την προστασία της ιδιωτικότητας, ώστε να μπορέσουν να πειστούν οι διοικούντες τους σχετικά με τα πλεονεκτήματα της ΑΕΙ. Σε αυτές τις περιπτώσεις, βασικότερο είναι να εστιάσει η ΑΕΙ στις επιπτώσεις της ιδιωτικότητας στην ίδια την επιχείρηση. Οι επιπτώσεις μπορεί να είναι άμεσες ή έμμεσες. Ένας οργανισμός κινδυνεύει να υποστεί διάφορες συνέπειες από τη μη λήψη επαρκούς προστασίας των προσωπικών δεδομένων που έχει στη διάθεσή της, και μερικές από αυτές αναφέρονται παρακάτω (Culnan and Williams, 2009):

- Αρνητική εικόνα στα ΜΜΕ
- Απώλεια της εμπιστοσύνης των πελατών, απώλεια της αξιοπιστίας, και ανεπανόρθωτη ζημία στην φήμη της επιχείρησης (η οποία μπορεί να οδηγήσει σε απώλεια πελατών ή / και προμηθευτών)
- Παράβαση των νόμων ή / και των κανονισμών που οδηγούν σε δικαστικές διαδικασίες και κυρώσεις ή την επιβολή νέων ρυθμιστικών ελέγχων
- Άμεση οικονομική ζημία από τα πρόστιμα ή τις κυρώσεις
- Μετασκευές ή ανασχηματισμοί των έργων ή ολοκληρωτική ακύρωση τους
- Απροσδόκητες, άδικες ή ανεπιθύμητες συνέπειες, ως αποτέλεσμα των εσφαλμένων δεδομένων προσωπικού χαρακτήρα ή της εσφαλμένης αξιολόγησης της σημαντικότητάς τους
- Απώλεια ανταγωνιστικού πλεονεκτήματος

Εκτός από τις συνέπειες που επιφέρονται για την ίδια την επιχείρηση ή οργανισμό, και άλλοι μπορεί να δεχτούν τις επιπτώσεις της παραβίασης της ιδιωτικότητας. Άτομα των οποίων τα δεδομένα έχουν εκτεθεί σε κίνδυνο δαπανούν πολύ χρόνο, χρήμα και άγχος για την ανάκτηση των δεδομένων τους.

Στη σημερινή σύγχρονη κοινωνία της πληροφορίας υπάρχουν πλέον εξελιγμένες τεχνολογίες πληροφοριών και επικοινωνιών. Αν και τα νέα αυτά πληροφοριακά συστήματα διευκολύνουν σε μεγάλο βαθμό τις συναλλαγές του πολίτη με το δημόσιο και

παράλληλα ενισχύουν την καθημερινή επικοινωνία και ανταλλαγή πληροφοριών μεταξύ των ατόμων, δημιουργούν ωστόσο ζητήματα προστασίας της ιδιωτικότητας.

Για την αντιμετώπιση και την εξασφάλιση αυτών των ζητημάτων οι οργανισμοί υιοθετούν την Ιδιωτικότητα δια του Σχεδιασμού, η οποία μπορεί να θεωρηθεί ιδιαίτερα χρήσιμη στα πλαίσια του ανταγωνισμού και παράλληλα ένα σημαντικό εργαλείο για την ενίσχυση της ιδιωτικότητας των οργανισμών. Παρόλα αυτά, για την εκπλήρωση αυτού του σκοπού ενός οργανισμού, θεμελιώδη ρόλο έχει και η σωστή ενσωμάτωσή της σε αυτόν.

Η Privacy by Design ιδανικό θα ήταν να μην εφαρμόζεται αποσπασματικά με πολλαπλά και διαδοχικά έργα (projects), αλλά με ενιαίο τρόπο σε ολόκληρο τον οργανισμό. Πρακτικά βέβαια οι καινοτομίες ως προς την προστασία της ιδιωτικότητας προκύπτουν κατά την διάρκεια ενός έργου. Ωστόσο με τέτοιου είδους χρήση, δημιουργείται ο κίνδυνος μια συγκεκριμένη διαδικασία ή ένα έργο να βοηθά μεμονωμένα στην προστασία της ιδιωτικότητας, και να μην υπάρχει συνολική προστασία σε όλο τον οργανισμό, με αποτέλεσμα να μην υπάρχει και σωστή εφαρμογή της προστασίας των προσωπικών δεδομένων του πολίτη.

Όταν η εφαρμογή της πραγματοποιείται μέσω διαδοχικών έργων θα πρέπει να θεωρείται μόνο μία μεταβατική φάση για τον οργανισμό. Παράλληλα με την πλήρη ενσωμάτωση της στον οργανισμό θα πρέπει να γίνεται η εφαρμογή της σε όλα τα πληροφοριακά συστήματα, στις επιχειρηματικές πρακτικές, στον σχεδιασμό της δικτυακή υποδομής και γενικά σε κάθε πτυχή του οργανισμού.

Όπως προαναφέρθηκε, για την προστασία της ιδιωτικότητας γενικά, αλλά και για την επιτυχημένη εφαρμογή της Ιδιωτικότητας δια του Σχεδιασμού ειδικά, πρέπει να υπάρξει δέσμευση από τα διευθυντικά στελέχη ως προς την προώθηση και την ανάπτυξη μιας κουλτούρας διαφύλαξης της ιδιωτικότητας. Με τον τρόπο αυτό η ιδιωτικότητα μπορεί να αποτελέσει μέρος των καθημερινών λειτουργιών του οργανισμού σε όλα τα επίπεδα. Επίσης, τα διευθυντικά στελέχη έχουν τη δυνατότητα ενός ουσιαστικού ρόλου στην εφαρμογή της Privacy by Design με τέτοιο τρόπο που να είναι συνυφασμένος με την δομή, τις διαδικασίες αλλά και τις απαιτήσεις των πελατών και των μετόχων σε θέματα ιδιωτικότητας.

Ως προς την εφαρμογή της Ιδιωτικότητας δια του Σχεδιασμού σε οργανωτικό επίπεδο, οι οργανισμοί θα έχουν τη δυνατότητα επιλογής μεταξύ κάποιων εργαλείων που περιλαμβάνουν Αξιολογήσεις Επιπτώσεων στην Ιδιωτικότητα (Privacy Impact Assessments), διαδικασίες διαχείρισης επικινδυνότητας (risk management processes), καθώς και ελέγχους ιδιωτικότητας (privacy audits) και πιστοποιήσεις. Προκειμένου να υπάρξει σωστή προστασία όλων αυτών των στοιχείων είναι ορθή η προληπτική ενσωμάτωση κανόνων ιδιωτικότητας από το στάδιο του σχεδιασμού του πληροφοριακού συστήματος.

Όταν ένας οργανισμός κατά τη διαδικασία του σχεδιασμού εφαρμόσει την Αξιολόγηση Επιπτώσεων της Ιδιωτικότητας, που συνήθως πραγματοποιείται παράλληλα με τις αξιολογήσεις απειλών/επικινδυνότητας, έχει ως αποτέλεσμα τη δυνατότητα να κρίνει με βάση τα πορίσματά της σε σχέση με τους κινδύνους το πώς θα αντιμετωπίσει τα ζητήματα της προστασίας της ιδιωτικότητας που προκύπτουν. Για να επιτευχθεί αυτό, προϋπόθεση αποτελεί η ορθή ενσωμάτωση της ιδιωτικότητας δια του σχεδιασμού, διότι θα πρέπει να εκμεταλλευτεί κατάλληλα τα αποτελέσματα της ΑΕΙ και με τη χρήση Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας και PbD να αντιμετωπίσει τους κινδύνους. Ακόμη, η ΑΕΙ θα πρέπει να εστιάζει στις επιπτώσεις του ενδιαφερόμενου οργανισμού, με στόχο τη συμμόρφωσή του ως προς τις νομικές και ρυθμιστικές απαιτήσεις που αφορούν την ιδιωτικότητα.

5.6 Τρόποι Αντιμετώπισης και Ελαχιστοποίησης Απειλών και Κινδύνων

Προκειμένου να υπάρξουν ελάχιστες πιθανότητες να μετατραπεί μια απειλή σε κίνδυνο, χρειάζεται τα μέτρα ασφαλείας να αντιμετωπίζουν ικανοποιητικά τις απαιτήσεις ασφάλειας (Security Requirements) καθώς επίσης και να περιλαμβάνουν, όταν θεωρείται απαραίτητο, τις παρακάτω υπηρεσίες ασφάλειας (Security Services):

• ***Αυθεντικοποίηση (Authentication),*** *η οποία σχετίζεται με το επίπεδο εμπιστοσύνης το οποίο οι συναλλασσόμενοι απαιτούν, σε σχέση με την ταυτότητα των εμπλεκόμενων μερών.*

• ***Εξουσιοδότηση (Authorization)****, η οποία σχετίζεται με τα δικαιώματα που διαθέτει κάθε οντότητα, στο πλαίσιο μιας συναλλαγής.*

• ***Ακεραιότητα (Integrity****) των δεδομένων, που αφορά στην απαίτηση περί μη τροποποίησης του περιεχομένου των μηνυμάτων κατά τη διάρκεια μιας συναλλαγής.*

• ***Μη-αποποίηση (Non-repudiation****) αποστολής και λήψης δεδομένων, που αφορά την παροχή στοιχείων, με βάση τα οποία μία οντότητα δε θα δύναται, κατ' αρχάς, σε μεταγενέστερο χρόνο να αρνηθεί ότι έχει συμμετάσχει σε μία συγκεκριμένη ηλεκτρονική συναλλαγή.*

• ***Υπηρεσίες διασφάλισης της Εμπιστευτικότητας (Confidentiality)*** *των ανταλλασσόμενων μηνυμάτων και γενικότερα της Ιδιωτικότητας (Privacy) των εμπλεκομένων οντοτήτων σε μία ηλεκτρονική συναλλαγή.*

5.7 Πλεονεκτήματα από την ΑΕΙ

Μια εταιρεία ή κυβερνητικός οργανισμός που αναλαμβάνει την Αξιολόγηση των επιπτώσεων της ιδιωτικότητας με πρόθεση την συμμετοχή όλων των εμπλεκομένων, έχει την ευκαιρία να κερδίσει την εμπιστοσύνη των πολιτών ή των καταναλωτών, αναλόγως σε τι οργανισμό αναφερόμαστε. Ο βαθμός στον οποίο κερδίζεται η εμπιστοσύνη τους, εξαρτάται από το πόσο ανοικτή και διαφανής η οργάνωση κάνει τη διαδικασία της αξιολόγησης των επιπτώσεων της ιδιωτικότητας. Όσο πιο ανοικτή και διαφανής η διαδικασία είναι, τόσο πιο πιθανό είναι ο οργανισμός να ξεπεράσει τους φόβους, τις υποψίες και την δυσπιστία ως προς την ανάπτυξη μιας νέας υπηρεσίας, προϊόντος, πολιτικής, προγράμματος ή έργου. Ακόμα κι αν μια νέα υπηρεσία δεν γεννά ανησυχίες στο κοινό και δεν υπάρχει καμία ανησυχία ή δυσπιστία σχετικά με αυτήν, ο οργανισμός μπορεί να κερδίσει την υπεραξία μέσα από μία ανοικτή και διαφανή διαδικασία που θα ακολουθήσει. Οι επιχειρήσεις είναι σε θέση να διατηρήσουν ένα υψηλό επίπεδο εμπιστοσύνης και αξιοπιστίας και έτσι μέσω αυτής της τακτικής μπορούν να διαφοροποιηθούν από τους ανταγωνιστές τους και να αποκτήσουν ανταγωνιστικό πλεονέκτημα (Wright, 2012).

5.8 ΑΕΙ και συμμετοχή όλων των εμπλεκομένων

Με την συμμετοχή των ενδιαφερομένων στη διαδικασία της ΑΕΙ, ένας οργανισμός μπορεί να επωφεληθεί από τις ιδέες που αυτοί θα έχουν και που μπορεί να μην έχουν εξεταστεί στο παρελθόν λόγω του ότι δεν είχε δοθεί η δέουσα βαρύτητα. Ακόμη και αν τα ενδιαφερόμενα μέρη δεν καταφέρουν να δημιουργήσουν κάποια νέα ζητήματα, ο οργανισμός έχει τουλάχιστον την ευκαιρία να κερδίσει την εμπιστοσύνη τους.

Η διαφάνεια στη διαδικασία αυτή μπορεί επίσης να είναι ένας τρόπος για την αποφυγή των μελλοντικών ευθυνών που μπορεί να βαρύνουν τα χαμηλότερα επίπεδα διοίκησης ενός οργανισμού. Εάν ο οργανισμός είναι σε θέση να αποδείξει ότι είχε συμμετάσχει και διαβουλευθεί με ένα ευρύ φάσμα εμπλεκομένων, με διαφορετικές απόψεις, θα είναι πιο δύσκολο για άλλους εμπλεκόμενους να υποστηρίξουν πως η οργάνωση ήταν αμελής.

Όπως αναφέρθηκε παραπάνω, η ΑΕΙ είναι μια μορφή αξιολόγησης κινδύνων, και έτσι αποτελεί αναπόσπαστο μέρος της διαχείρισης κινδύνων ενός οργανισμού ή επιχείρησης. Ενθαρρύνει τις οικονομικά αποδοτικές λύσεις, δεδομένου ότι προ-δραστικός ο χαρακτήρας της, με σκοπό την οικοδόμηση «προστασίας της ιδιωτικότητας εξαρχής στον σχεδιασμό» σε έργα, πολιτικές και τεχνολογίες, και άλλες πρωτοβουλίες. Έτσι, προκύπτει ότι είναι μια διαδικασία λιγότερο δαπανηρή από το στάδιο κατόπιν κάποιας επιπλοκής που θα συμβεί σε θέματα παραβίασης της ιδιωτικότητας. Μερικές απλές προσαρμογές είναι αρκετές ώστε να κάνει τη διαφορά ανάμεσα σε ένα έργο που είναι τρωτό από παρεμβάσεις σχετικά με την προστασία της ιδιωτικότητας, και σε ένα που έχει κατασκευαστεί σύμφωνα με τις απαραίτητες διασφαλίσεις. Έτσι, η ΑΕΙ δημιουργεί μια ευκαιρία για τους οργανισμούς για την πρόβλεψη και την αντιμετώπιση των πιθανών επιπτώσεων, για να προβλέψει τα προβλήματα και να προσδιορίσει τι πρέπει να γίνει ώστε να σχεδιαστούν με βάση χαρακτηριστικά που ελαχιστοποιούν τυχόν συνέπειες για την ιδιωτικότητα.

5.9 Η ΑΕΙ ως εμπειρία μάθησης

Η ΑΕΙ θα πρέπει επίσης να θεωρηθεί ως μια εμπειρία μάθησης, τόσο για την οργάνωση που αναλαμβάνει την πραγμάτωσή της, όσο και για τους φορείς που εμπλέκονται στη διαδικασία αυτή. Μια ανοιχτή διαδικασία ΑΕΙ βοηθά το κοινό να καταλάβει τι πληροφορίες συλλέγει ο οργανισμός, γιατί συλλέγονται, πώς οι πληροφορίες αυτές θα χρησιμοποιηθούν από κοινού, πώς μπορεί να είναι προσβάσιμες οι πληροφορίες αυτές και τέλος πώς θα πρέπει να αποθηκεύονται με ασφάλεια. Ο εκπαιδευτικός ρόλος της ΑΕΙ είναι ένας τρόπος για να αποδειχθεί ότι η οργάνωση έχει αναλύσει κριτικά πώς το έργο θα ασχοληθεί με τα προσωπικά δεδομένα. Υπάρχουν και οι περιπτώσεις όπου συγκεκριμένοι κίνδυνοι για την ιδιωτικότητα δεν μπορούν να μετριαστούν και πρέπει να γίνουν αποδεκτοί. Η έκθεση της ΑΕΙ, ως αποτέλεσμα μια σαφούς και συστηματικής διαδικασίας, είναι κάτι στο οποίο οι ενδιαφερόμενοι μπορούν να αναφέρονται και να ενημερώνονται. Αυτό κυρίως αφορά τους λόγους για τους οποίους ορισμένες παραδοχές και υποθέσεις έχουν ληφθεί υπόψη.

Η αξιολόγηση των επιπτώσεων της ιδιωτικότητας μπορεί να χρησιμοποιηθεί για την επιβολή ή την ενθάρρυνση της λογοδοσίας. Η ΑΕΙ καθιστά σαφές το ποιος και γιατί προτίθεται να κάνει τι και ποιος θα είναι υπεύθυνος για τι. Το οποιοδήποτε έργο είναι κατ' ελάχιστο συμβατό με τους νόμους προστασίας της ιδιωτικότητας, τους κανονισμούς και τους σχετικούς κώδικες δεοντολογίας. Αν ένα στέλεχος μιας επιχείρησης, γνωρίζει ότι θα πρέπει να λογοδοτήσει για θέματα ιδιωτικότητας, τότε μπορεί να είναι λιγότερο διατεθειμένος να προχωρήσει σε επιλογές που μπορεί να προκαλέσουν το κοινό ή να διεγείρει το ενδιαφέρον των ΜΜΕ.

6. Η περίπτωση των RFID υπό το ισχύον Ευρωπαϊκό καθεστώς

Οι Αξιολογήσεις Επιπτώσεων στην Ιδιωτικότητα εφαρμόζονται σε πολλές χώρες παγκοσμίως και σε ποικίλα επιχειρησιακά περιβάλλοντα, τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Στο πλαίσιο αυτό μάλιστα η Ευρωπαϊκή Επιτροπή τα τελευταία χρόνια συνέστησε την διενέργεια τους σε σχέση με τις κάρτες ταυτοποίησης μέσω ραδιοσυχνοτήτων (Remote Frequency Identification – RFID tags).

Πολλές νέες εφαρμογές των Τεχνολογιών Πληροφορικής και Επικοινωνιών έχουν σημαντικές προοπτικές και πιθανόν να επιφέρουν μείζονες οικονομικές και κοινωνικές συνέπειες, ενώ παράλληλα θα διαδραματίσουν θεμελιώδη ρόλο στη συνάρθρωση και τη σύγκλιση διαφορετικών τεχνολογιών. Μεταξύ αυτών των νέων τεχνολογιών συγκαταλέγονται τα ευρέως διαδεδομένα δίκτυα, που επιτρέπουν την παρακολούθηση ατόμων και αντικειμένων και παρέχουν τη δυνατότητα παρακολούθησης, καταγραφής, αποθήκευσης και επεξεργασίας των πληροφοριών σε πραγματικό χρόνο. Το κόστος ορισμένων εφαρμογών, όπως η ραδιοσυχνική αναγνώριση (Radio Frequency Identification) και άλλες τεχνολογίες αισθητήρων, μειώνεται συνεχώς, οι επενδύσεις αυξάνονται και οι εφαρμογές εμπορευματοποιούνται. Οι υπηρεσίες εντοπισμού θέσης χρησιμοποιούν μια ποικιλία τεχνολογιών εντοπισμού για την παρακολούθηση της θέσης αντικειμένων και χρηστών. Οι πιο κοινές εφαρμογές των τεχνολογιών αυτών απαντούν στη ναυσιπλοΐα και την παρακολούθηση περιουσιακών στοιχείων.

Η παρακολούθηση των προϊόντων μέσα στις εφοδιαστικές αλυσίδες είναι σχεδόν αδύνατη. Η τεχνολογία προσδιορισμού ραδιοσυχνότητας (RFID) βοηθά τις επιχειρήσεις να προσδιορίσουν και να ακολουθήσουν τα προϊόντα τους σε όλες τις φάσεις της κατασκευής τους, αλλά και κατά την διάρκεια της μεταφοράς τους έως και στον τελικό καταναλωτή.

Το RFID αποτελεί την πλέον σύγχρονη -όσον αφορά στην εφαρμογή της- τεχνολογία ηλεκτρονικής ταυτοποίησης. Στηρίζεται στη χρήση ραδιοκυμάτων και επιτρέπει την αυτόματη αναγνώριση ανθρώπων ή, κατά κύριο λόγο, αντικειμένων (προϊόντων) τα οποία φέρουν RFID tags (ετικέτες που ενσωματώνουν μικροεπεξεργαστή και κεραία) και μπορούν να ανιχνευθούν αυτόματα από σταθερούς ή φορητούς αναγνώστες (readers)

RFID, χωρίς να είναι απαραίτητη η σάρωση του κάθε μεμονωμένου αντικειμένου. Η κεραία επιτρέπει στο μικροεπεξεργαστή να μεταφέρει τις πληροφορίες αναγνώρισης στον αναγνώστη, ο οποίος με τη σειρά του μετατρέπει τα ραδιοκύματα που «αντανακλώνται» από την ετικέτα RFID σε ψηφιακές πληροφορίες. Οι πληροφορίες αυτές μπορούν στη συνέχεια να «περάσουν» σε υπολογιστές για περαιτέρω χρήση.

Όπως αναφέραμε παραπάνω, τα πλεονεκτήματα της τεχνολογίας RFID έναντι αυτής των barcodes είναι αρκετά. Στα παραπάνω θα πρέπει να προσθέσουμε ότι:

α) Μια ετικέτα RFID μπορεί να μεταφέρει αρκετά πιο χρήσιμες πληροφορίες από ένα barcode, όπως για παράδειγμα την ημερομηνία λήξεως, στοιχείο ιδιαίτερα χρήσιμο για πολλά ευπαθή προϊόντα όπως π.χ. το γάλα.

β) Τα barcodes είναι μια «line-of-sight» τεχνολογία, κάτι που σημαίνει ότι ο scanner θα πρέπει να «βλέπει» το γραμμωτό κώδικα για να τον διαβάσει. Αντίθετα, οι ετικέτες RFID δεν απαιτούν από τον αναγνώστη κάτι τέτοιο και μπορούν να διαβαστούν όσο βρίσκονται μέσα στην ακτίνα ανάγνωσής του.

Παρόλα αυτά, και για το άμεσο τουλάχιστον μέλλον, δεν διαφαίνεται αντικατάσταση των barcodes, τα οποία είναι σαφώς φθηνότερα από τις ετικέτες RFID, αλλά και αποτελεσματικά σε συγκεκριμένους τομείς. Έτσι, το πιο πιθανό είναι τα barcodes και το RFID να συνυπάρχουν για αρκετά χρόνια.

Όπως αναφέρθηκε, οι ετικέτες RFID αποθηκεύουν πληροφορίες σχετικές με τους ανθρώπους ή τα αντικείμενα που τις φέρουν. Έτσι, στην πράξη, μπορούν να βρουν εφαρμογή σε πληθώρα τομέων όπου η αναγνώριση ανθρώπων ή αντικειμένων είναι απαραίτητη. Για παράδειγμα, μπορούν να χρησιμοποιηθούν στη συσκευασία των προϊόντων, σε βιβλιοθήκες, σε πιστωτικές κάρτες, ή ακόμα και σε ένα σήμα ή έγγραφο ταυτοποίησης όπως η ταυτότητα, το διαβατήριο, ή το δίπλωμα οδήγησης. Ασφαλώς, μία από τις πλέον συνήθεις εφαρμογές τους είναι ο χώρος της εφοδιαστικής αλυσίδας, όπου μπορούν να αναγνωρίζουν προϊόντα είτε κατά τη διάρκεια της μεταφοράς τους, είτε εντός βιομηχανικών μονάδων, είτε αυτά βρίσκονται σε παλέτες, αποθήκες ή στα ράφια των καταστημάτων.

Η συνολική αγορά RFID αναμένεται να κοστίζει περίπου $18,68 δις μέχρι το 2026. Η έρευνα του IDTechEx παρακολουθεί την αγορά από το 1999. Η έρευνα του βασίζεται σε χρόνια έρευνας που καλύπτουν πολλές αγορές όπου υπάρχει η εφαρμογή των RFID. Προσφέρει έτσι μια αποκαλυπτική οπτική του μεγέθους της αγοράς RFID: το 2015, η συνολική αξία της αγοράς είναι στα $10,1 δις, από $9,5 δις το 2014 και $8,8 δις το 2013. Αυτό περιλαμβάνει τις ετικέτες, τους αναγνώστες και το λογισμικό / υπηρεσίες για κάρτες RFID, ετικέτες, τηλεχειριστήρια και όλες τις άλλες μορφές παραγόντων, για παθητικό και ενεργητικό RFID. Η IDTechEx προβλέπει ότι η αγορά θα αυξηθεί σε $13,2 δις το 2020[3].

Στον κλάδο του εμπορίου μόνο, όπου τα RFID χρησιμοποιούνται ως αναγνωριστικά στα ενδύματα, η εφαρμογή θα απαιτεί 4,6 δις RFID ταμπελάκια το 2016, με ποσοστό διείσδυσης μόνο 15% της συνολικής αγοράς. Για τις μεταφορές και τα εισιτήρια, φτάνουν τα 800 εκατομμύρια για το 2016. Για τα κατοικίδια και την κτηνοτροφία, αγγίζει τα 430 εκατομμύρια για το 2016. Συνολικά, το IDTechEx αναμένει 8,9 δις RFID ταμπελάκια να πουληθούν το 2015 και 10,4 δις το 2016.

Μετά από εκτενείς συνεντεύξεις με τους προμηθευτές, το IDTechEx διαπίστωσε ότι υπάρχουν τώρα αναδυόμενοι και εγκατεστημένοι ηγέτες στις περισσότερες θέσεις της αλυσίδας αξίας στις διάφορες τεχνολογίες - όμως ακόμα πολύ λίγες εταιρείες έχουν πωλήσεις άνω των $100 εκατομμυρίων[4].

Η τεχνολογία RFID στην ΕΕ

Η Ευρώπη έχει ήδη νόμους προστασίας της ιδιωτικής ζωής με στόχο την προστασία των καταναλωτών σε όλη την ήπειρο. Για παράδειγμα, τα καταστήματα λιανικής πώλησης πρέπει να γνωστοποιούν την ύπαρξη ετικετών RFID στα προϊόντα όπως και την παρουσία των συσκευών ανάγνωσης (readers), το πώς ο πωλητής προτίθεται να συγκεντρώσει και να ελέγξει τις πληροφορίες, τους σκοπούς για τους οποίους θα χρησιμοποιηθούν οι πληροφορίες, πως θα ελέγχονται τα δεδομένα, πώς να απορρίψουν

[3] http://www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2016-2026-000451.asp
[4] http://www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2016-2026-000451.asp

οι καταναλωτές την ετικέτα του προϊόντος, πώς να ασκήσουν το δικαίωμα πρόσβασης στις πληροφορίες σχετικά με την ετικέτα κ.ο.κ.[5]

Στην πορεία προέκυψαν θέματα σχετικά με τα RFID που χρήζουν προσοχής. Η τεχνολογία RFID αυξάνει τη δυνατότητα για direct marketing έχοντας σε κάθε προϊόν και μια ετικέτα παρακολούθησης, αφού οι καταναλωτές μπορούν να αναγνωρισθούν και οι κινήσεις τους να ανιχνευτούν όσο είναι μέσα στο κατάστημα.

Ακόμη, υπάρχει ανησυχία για τη χρήση των εφαρμογών που συνδέουν τα RFID με τον τραπεζικό λογαριασμό του καταναλωτή. Οι κατασκευαστές του σχετικού εξοπλισμού και των εφαρμογών RFID πρέπει να θεωρηθούν εξίσου υπεύθυνοι για την δημιουργία ετικετών και εξοπλισμού που θα προστατεύουν το δικαίωμα των καταναλωτών στην ιδιωτική ζωή. Η ομάδα έρευνας της ΕΕ τονίζει ότι υπάρχει συνεχής ανάγκη για περαιτέρω έρευνα και ανάπτυξη σε θέματα που σχετίζονται με την κρυπτογράφηση για την προστασία των προσωπικών πληροφοριών σχετικά με τις ετικέτες. Θέλει να βεβαιωθεί ότι η ετικέτα RFID δεν αποκαλύπτει πληροφορίες που θα συνδέουν τον καταναλωτή με το προϊόν που ο καταναλωτής αγοράζει. Αν η ετικέτα είναι μόνιμα τοποθετημένη στο ένδυμα, για παράδειγμα, η ομάδα εργασίας αναφέρει ότι θα πρέπει να υπάρχει ένας τρόπος έτσι ώστε ο καταναλωτής να μπορεί να διαγράψει τις πληροφορίες που αναγράφονται στην ετικέτα RFID ή να την αφαιρέσει με την αγορά.

Σε ένα άλλο επίπεδο, για τα διαβατήρια και άλλα κυβερνητικά στοιχεία ταυτότητας που εκδίδονται που δεν πρέπει να αλλοιώνονται, η ομάδα εργασίας προτείνει τη χρήση τυποποιημένων πρωτοκόλλων ελέγχου ταυτότητας από τον Οργανισμό Διεθνών Προτύπων για την κρυπτογράφηση των δεδομένων ώστε να μην καταστεί διαθέσιμη σε όσους δεν διαθέτουν άδεια[6].

«RFID in Europe» (Raising Awareness and Competitiveness on RFID in Europe)

Το "RFID in Europe" είναι ένα Ευρωπαϊκό έργο και δίκτυο αποτελούμενο από ένα μεγάλο αριθμό Ευρωπαϊκών οργανισμών (πάνω από 200 μέλη) οι οποίοι εμπλέκονται με

[5] http://www.informationweek.com/the-european-union-works-out-rfid-privacy-legislation/d/d-id/1030178
[6] http://www.informationweek.com/the-european-union-works-out-rfid-privacy-legislation/d/d-id/1030178

την τεχνολογία RFID. Στόχος του δικτύου αυτού είναι να προάγει την τεχνολογία RFID σε όλη την Ευρώπη. Απώτερος σκοπός είναι να καθιερώσει την Ευρώπη ως τον παγκόσμιο κεντρικό φορέα και ηγέτη όσον αφορά στην επιτυχημένη υιοθέτηση και υλοποίηση της τεχνολογίας RFID. Πάνω από 15 ευρωπαϊκές χώρες είναι φορείς αυτού του δικτύου, όπως: Ελλάδα, Μ. Βρετανία, Γαλλία, Γερμανία, Δανία, Ισπανία, Ιταλία, Τσέχικη Δημοκρατία, Σουηδία. Το "RFID in Europe" ξεκίνησε τη δράση του το Μάρτιο του 2009 και ολοκληρώνεται στα τέλη του Φεβρουαρίου του 2012, μετά από τρία χρόνια. Οι φορείς του δικτύου σκοπεύουν να συνεχίσουν τη δράση του "RFID in Europe" και τα επόμενα χρόνια. Μια από τις βασικές δραστηριότητες αυτού του δικτύου είναι να προάγει και να γνωστοποιεί best practices, case studies, αναφορές, οδηγίες, υπηρεσίες, συνέδρια και άλλες εκδηλώσεις που αφορούν στην χρήση της τεχνολογίας αυτής[7].

6.1 Ανάπτυξη πλαισίου Αξιολόγησης Επιπτώσεων Ιδιωτικότητας

Τον Μάιο του 2009 όλα τα ενδιαφερόμενα μέρη από τον κλάδο, τους οργανισμούς τυποποίησης, τις οργανώσεις καταναλωτών, ομάδες πολιτών, και τις συνδικαλιστικές ενώσεις, συμφώνησαν να ακολουθήσουν σύσταση της Ευρωπαϊκής Επιτροπής που έθετε τις αρχές για την προστασία της ιδιωτικής ζωής και των δεδομένων κατά τη χρήση των έξυπνων ετικετών (βλ. IP/09/740). Το σημερινό πλαίσιο ΑΕΙ είναι μέρος της υλοποίησης της σύστασης του 2009. Οι πληροφορίες που συγκεντρώθηκαν κατά τη διάρκεια της διαδικασίας κατάρτισης του πλαισίου ΑΕΙ θα αποτελέσουν επίσης πολύτιμη συμβολή στις συζητήσεις για την αναθεώρηση των κανόνων της ΕΕ όσον αφορά την προστασία των δεδομένων (βλ. IP/10/1462 και MEMO/10/542), καθώς και για τον τρόπο αντιμετώπισης των νέων προβλημάτων στην προστασία των προσωπικών δεδομένων, προβλημάτων που οφείλονται στις τεχνολογικές εξελίξεις.

Η Ευρωπαϊκή Επιτροπή υπέγραψε το 2011 εθελοντική συμφωνία με τον κλάδο, την κοινωνία των πολιτών, τον ENISA (Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών) και τους εποπτικούς φορείς για την προστασία της ιδιωτικής ζωής και των δεδομένων στην Ευρώπη σχετικά με τη χάραξη κατευθυντήριων γραμμών για όλες

[7] http://www.eltrun.gr/rfid-in-europe-4/#sthash.nx9uup5d.dpuf

τις εταιρείες στην Ευρώπη, με σκοπό να αντιμετωπιστούν οι επιπτώσεις των έξυπνων ετικετών στην προστασία των δεδομένων (Συσκευές ραδιοσυχνικής αναγνώρισης - RFID) πριν από τη διάθεσή τους στην αγορά. Η χρήση των έξυπνων αυτών ετικετών γενικεύεται ραγδαία (περίπου ένα δισεκατομμύριο το 2011 στην Ευρώπη), υπάρχει όμως διάχυτη ανησυχία για τις επιπτώσεις τους στην ιδιωτική ζωή. Οι RFID βρίσκονται σε πολλά αντικείμενα, από τις κάρτες επιβατών στα λεωφορεία έως τις έξυπνες κάρτες για πληρωμή διοδίων σε αυτοκινητοδρόμους. Οι μικροηλεκτρονικές συσκευές μπορούν να επεξεργάζονται αυτόματα τα δεδομένα από ετικέτες RFID όταν αυτές βρεθούν κοντά στις συσκευές ανάγνωσης που τις ενεργοποιούν, δέχονται το ραδιοσήμα τους και ανταλλάσσουν δεδομένα. Η συμφωνία αυτή αποτελεί μέρος της υλοποίησης σύστασης της Επιτροπής που εγκρίθηκε το 2009 (βλ. IP/09/740), στην οποία, μεταξύ άλλων, επισημαίνεται ότι όταν οι καταναλωτές αγοράζουν προϊόντα που φέρουν έξυπνες ετικέτες πρέπει οι ετικέτες να απενεργοποιούνται αυτόματα, αμέσως και χωρίς επιβάρυνση, εκτός εάν ο καταναλωτής δηλώσει ρητά την εν προκειμένω αντίθεσή του.

Η συμφωνία που υπογράφηκε, με τίτλο «Πλαίσιο για την εκτίμηση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων όσον αφορά εφαρμογές RFID», αποσκοπεί στην εξασφάλιση της ιδιωτικότητας των καταναλωτών πριν από τη μαζική εισαγωγή των ετικετών RFID (βλ. IP/09/952). Το 2011 περίπου πουλήθηκαν γύρω στα 2,8 δισεκατομμύρια έξυπνες ετικέτες, από τις οποίες το ένα τρίτο περίπου στην Ευρώπη. Ο κλάδος εκτιμά όμως ότι έως το 2020 θα μπορούσαν να υπάρχουν στην Ευρώπη έως και 50 δις συνδεδεμένες ηλεκτρονικές συσκευές.

Οι ετικέτες RFID σε συσκευές όπως κινητά τηλέφωνα, υπολογιστές, ψυγεία, ηλεκτρονικά βιβλία και αυτοκίνητα προσφέρουν πολλά δυνητικά πλεονεκτήματα στις επιχειρήσεις, τις δημόσιες υπηρεσίες και τα καταναλωτικά προϊόντα. Για παράδειγμα αναφέρονται η βελτίωση της αξιοπιστίας των προϊόντων, η ενεργειακή απόδοση και οι διαδικασίες ανακύκλωσης, η πληρωμή διοδίων με διέλευση χωρίς στάση, ο περιορισμός του χρόνου αναμονής για τις αποσκευές στα αεροδρόμια και η μείωση του περιβαλλοντικού αποτυπώματος προϊόντων και υπηρεσιών.

Ωστόσο, οι ετικέτες RFID συνεπάγονται επίσης ενδεχόμενους κινδύνους όσον αφορά την προστασία της ιδιωτικής ζωής, την ασφάλεια και την προστασία των δεδομένων·

συμπεριλαμβάνεται η δυνατότητα πρόσβασης τρίτων σε προσωπικά δεδομένα (π.χ. τη γεωγραφική θέση) χωρίς την άδειά των χρηστών ή τελικών καταναλωτών.

Για παράδειγμα, πολλοί οδηγοί πληρώνουν ηλεκτρονικά διόδια οδικής κυκλοφορίας, τέλη στάθμευσης σε αεροδρόμια και χώρους στάθμευσης αυτοκινήτων με βάση τα δεδομένα που συλλέγονται μέσω των ετικετών RFID που είναι τοποθετημένες στο παρμπρίζ του αυτοκινήτου τους. Αν δεν αναληφθεί προληπτική δράση, οι συσκευές ανάγνωσης RFID που βρεθούν ενδεχομένως έξω από τις συγκεκριμένες αυτές θέσεις θα μπορούσαν ακούσια να προκαλέσουν διαρροές δεδομένων ιδιωτικότητας, αποκαλύπτοντας την θέση του οχήματος. Πολλά νοσοκομεία χρησιμοποιούν ετικέτες RFID για την παρακολούθηση των αποθεμάτων και την ταυτοποίηση ασθενών. Η εν λόγω τεχνολογία μπορεί μεν να βελτιώσει τη συνολική ποιότητα της υγειονομικής περίθαλψης, πρέπει όμως τα οφέλη να σταθμίζονται με τις ανησυχίες όσον αφορά την προστασία της ιδιωτικής ζωής και την ασφάλεια.

Τα θέματα της ιδιωτικότητας και της ασφάλειας στην RFID τεχνολογία αναδεικνύονται από το γεγονός ότι οι άνθρωποι δεν μπορούν να αντιληφθούν την RF ακτινοβολία που χρησιμοποιείται για την ανάγνωση των tags και επιπλέον τα tags δεν κρατούν ιστορικό του τι διαβάστηκε και από ποιόν. Ως αποτέλεσμα, τα tags μπορούν να διαβαστούν από οντότητες διαφορετικές από αυτές των κατόχων τους και χωρίς οι κάτοχοι τους να έχουν επίγνωση.

Πιο συγκεκριμένα, το θέμα της ασφάλειας των συστημάτων και της αυθεντικοποίησης στο RFID, αφορά το πρόβλημα καλώς συμπεριφερόμενων readers τα οποία διαβάζουν πληροφορίες κακόβουλων tags, ειδικότερα πλαστών. Μέχρι πρόσφατα δεν διαφαινόταν να υπάρχει κίνδυνος αντιγραφής ενός tag, αλλά ειδικοί απέδειξαν σημαντικές αδυναμίες ασφάλειας όπως η αντιγραφή ενός διαβατηρίου νέας γενιάς ή ενός συστήματος immobilizer με μη εξειδικευμένο χαμηλού κόστους εξοπλισμό.

Από την άλλη, η ιδιωτικότητα στο RFID αφορά το πρόβλημα κακόβουλων readers που διαβάζουν πληροφορίες από tags στα οποία δεν έχουν εξουσιοδότηση. Οι περισσότεροι κίνδυνοι παραβίασης της προσωπικής ζωής των πολιτών προκύπτουν από το γεγονός ότι τα tags με τη μοναδικότητα του σειριακού αριθμού τους, μπορούν εύκολα να συσχετιστούν με τη ταυτότητα ενός ατόμου. Αναφορικά, παρακάτω επισημαίνουμε

μερικούς από τους κινδύνους αυτούς που σχετίζονται με τη παραβίαση της ιδιωτικότητας του ατόμου:

Κίνδυνος παρακολούθησης των κινήσεων

Μπορεί να βγει ένα συμπέρασμα για τη συμπεριφορά ενός ατόμου με βάση τα δεδομένα που λαμβάνεται από μια ομάδα tags.

Κίνδυνος συσχέτισης

Όταν ένας πελάτης αγοράσει ένα προϊόν το οποίο φέρει ένα tag, η ταυτότητα αυτού του ατόμου μπορεί να συσχετιστεί με τον ηλεκτρονικό σειριακό αριθμό του αντικειμένου.

Κίνδυνος αποκάλυψης θέσης

Άτομα τα οποία φέρουν ένα tag μοναδικού σειριακού αριθμού μπορεί να παρακολουθούνται στο χώρο και η τοποθεσία τους να φανερώνεται, με την προϋπόθεση αυτός που κάνει την παρακολούθηση να γνωρίζει την αντιστοιχία ατόμου με tag.

Κίνδυνος αποκάλυψης προτιμήσεων

Επιπλέον το tag σε ένα αντικείμενο φανερώνει τον κατασκευαστή, τον τύπο του, την μοναδική ταυτότητα του, αλλά και την τιμή του. Αυτό αποκαλύπτει τις προτιμήσεις του πελάτη σε ανταγωνιστικές εταιρίες ή άλλα αδιάκριτα άτομα.

Κίνδυνος κατηγοριοποίησης / χαρακτηρισμού ανθρώπων

Κάποιοι μπορούν να κατηγοριοποιήσουν τα άτομα σε διάφορες ομάδες με βάση τα tags που φέρουν, και να τα εντοπίσουν χωρίς καν να γνωρίζουν την ταυτότητα τους.

Κίνδυνος αποκάλυψης συναλλαγών

Όταν ένα αντικείμενο που φέρει tag αλλάξει ομάδα μπορεί κάποιος να συμπεράνει μια συναλλαγή μεταξύ των ατόμων που συσχετίζονται με αυτές τις ομάδες.

Κίνδυνος απαρχαιωμένων στοιχείων

Οι καταχωρήσεις που αφορούν ένα άτομο σε μια βάση δεδομένων δεν ενημερώνονται όταν το άτομο αποκόπτεται από το προϊόν που φέρει το tag, άλλα το συσχετίζουν εφόρου

ζωής με αυτό με αποτέλεσμα σε πολλές περιπτώσεις να εξάγονται λάθος συμπεράσματα για το άτομο αυτό.

Για τα προβλήματα και τους κινδύνους των συστημάτων RFID έχουν προταθεί διάφοροι τρόποι επίλυσής τους:

- Καταστροφή των tags κατά την αγορά τους, μέσω ενός kill command, ή αφαίρεση της ετικέτας χειροκίνητα όπου αυτό επιτρέπεται. Σαν μέτρο αποφυγής κακόβουλων kill commands απαιτείται ο reader που θα αποστείλει το kill command να έχει μεταδώσει και συγκεκριμένο PIN, το οποίο θα επαληθεύσει την ενέργεια αυτή. Η πρόταση της καταστροφής των tags, εξαλείφει όλα τα πλεονεκτήματα του RFID που μπορεί να αξιοποιήσει ο καταναλωτής.
- Για τα επαναχρησιμοποιήσιμα tags μία πρόταση είναι η απενεργοποίηση τους μέσω κάποιας sleep command και η ενεργοποίηση τους με κάποια wake up command, κάτι που όμως περικλείει προβλήματα αυθεντικοποίησης των readers ή διαχείρισης κωδικών.
- Η ασφάλεια των tags μπορεί ακόμα να επιτευχθεί με χρήση απλών υλικών από μέταλλο τα οποία μπλοκάρουν και διαχέουν την RF ακτινοβολία, για παράδειγμα μια κονσέρβα ή 27mm περιτύλιγμα με αλουμινόχαρτο είναι ικανά να θωρακίσουν το tag. Επίσης υλικά με υγρότητα απορροφούν τα RFID σήματα, για παράδειγμα 1mm περίβλημα θαλασσινού νερού έχει το ίδιο αποτέλεσμα. Ακόμα και τα πλαστικά αλλά και κάθε αγώγιμο υλικό έχει σαν αποτέλεσμα την αποδυνάμωση του σήματος της κεραίας, για παράδειγμα ένα tag μέσα σε μια ανθρώπινη γροθιά θα μπορούσε ίσως να αποτρέψει την ικανότητα ανάγνωσης του.
- Τέλος μπορεί να αποτραπεί πλήρως η λήψη ενέργειας από ένα tag αν απλώς τοποθετηθεί μέσα σε ένα κλωβό Faraday, ενώ παρομοίως μπορεί να αποτραπεί η επιτυχής αποστολής σημάτων από έναν reader αν αυτός τοποθετηθεί σε μία τέτοιου είδους περίφραξη η οποία εμποδίζει τα ηλεκτρομαγνητικά κύματα, όπως είναι ο κλωβός Faraday.

Μελέτη Περιπτώσεων RFID

Παρά τις εγγενείς αδυναμίες στην εφαρμογή των απαιτήσεων PIA, υπάρχουν μερικές περιπτώσεις στο Αμερικανικό παράδειγμα, που έχουν ενσωματώσει τις απαιτήσεις αυτές και τους στόχους, στις διαδικασίες τους. Τα δύο παραδείγματα στα οποία θα κάνουμε αναφορά παρακάτω είναι η περίπτωση του προγράμματος e-Passport και η περίπτωση της πρωτοβουλίας του US-VISIT. Και στις δυο περιπτώσεις, πρόκειται για τη χρήση της τεχνολογίας RFID σε ταξιδιωτικά έγγραφα. Οι εμπειρίες αυτές καταδεικνύουν τις θετικές και τις αρνητικές πλευρές της χρήσης της τεχνολογίας αυτής με όρους ιδιωτικότητας.

e-Passport

Τον Φεβρουάριο του 2005, προτάθηκε το πρόγραμμα e-Passport, σύμφωνα με το οποίο, στο παραδοσιακό διαβατήριο θα προστίθετο και ένα ηλεκτρονικό τσιπ που θα εμπεριείχε πληροφορίες από τη σελίδα δεδομένων του διαβατηρίου και ένα ψηφιακό αρχείο με την φωτογραφία του ιδιοκτήτη. Το τσιπάκι αυτό, μέσω της συχνότητάς του, μπορεί να αναγνωσθεί χωρίς φυσική επαφή, μέσω ασύρματης τεχνολογίας. Στα επιχειρήματα υιοθέτησής του, συγκαταλέγεται το ότι είναι πιο δύσκολο να «πειραχτεί» και να πλαστογραφηθεί (Wright & Hert, 2012).

Ωστόσο, η πρόταση δεν αντιμετώπιζε τα θέματα ασφάλειας δεδομένων και ιδιωτικότητας που προέκυπταν σχετικά με τις προσωπικές πληροφορίες που περιέχει το RFID για τον ιδιώτη. Ακόμη, σύμφωνα με μελέτες, δεν γίνεται αναφορά στα ενδεχόμενα ρίσκα που δημιουργούνται, ούτε παρέχει πληροφορίες για τη δοκιμαστική διαδικασία της τεχνολογίας, αλλά και για τα δεδομένα όπου βασίστηκε η πρόταση (Wright & Hert, 2012).

Σε γενικές γραμμές, η πρόταση του e-Passport χωρίς να λαμβάνει υπόψη τις επιπτώσεις της τεχνολογίας στην πρόσβαση δεδομένων και τη συλλογή τους, απέρριπτε τις σχετικές με την ιδιωτικότητα ανησυχίες με το σκεπτικό πως «τα προσωπικά δεδομένα που συμπεριλαμβάνονται στο τσιπ του διαβατηρίου αποτελεί μια απλή καταγραφή των πληροφοριών που παραδοσιακά υπάρχουν στην πρώτη σελίδα του εγγράφου σήμερα» (Wright & Hert, 2012).

Η «σιωπή» αυτή σχετικά με τους κινδύνους της τεχνολογίας RFID είναι ιδιαίτερα περίεργη. Παραλείπεται η ανησυχία σχετικά με την μη εξουσιοδοτημένη ασύρματη πρόσβαση στα δεδομένα του ατόμου χωρίς τη δική του γνώση ή συγκατάθεση. Τα τεστ για να εξακριβωθεί το πόσο ευάλωτο είναι το σύστημα, αναθεωρήθηκαν τον Φεβρουάριο του 2005, αρκετούς μήνες μετά την ολοκλήρωση του εγχειρήματος. Στις βελτιώσεις ασφαλείας που βασίζονται στα πορίσματα του Αμερικανικού Εθνικού Ινστιτούτου Standards και Τεχνολογίας (NIST) συμπεριλαμβάνεται η ενσωμάτωση ενός υλικού που δεν αφαιρείται από το κάλυμμα του διαβατηρίου, ένας κωδικός κλειδώματος που περιορίζει τη πρόσβαση σε αναγνώστες που έχουν τη σχετική εξουσιοδότηση και μια κρυπτογράφηση εκπομπών. Το ερώτημα του κατά πόσο η τεχνολογία RFID ήταν η κατάλληλη για τη χρήση αυτή, δεν απαντήθηκε ποτέ από τους αρμόδιους (Wright & Hert, 2012).

US-VISIT

Ύστερα από την Πράξη Πρόληψης κατά της Τρομοκρατίας το 2004, το τμήμα Εθνικής Ασφάλειας (Homeland Security) επέλεξε παρόμοια τεχνολογία για να ελέγξει τις μεταναστευτικές ροές στο Αμερικανικό έδαφος. Πρότεινε τη χρήση RFID τσιπ που θα ενσωματώνεται στο έντυπο I-94 κατά την άφιξη / αναχώρηση από τις ΗΠΑ για να παρακολουθείται η είσοδος και έξοδος των ξένων επισκεπτών στα χερσαία σύνορα - σημεία διαβάσεων εισόδου. Το τσιπ αυτό θα αποθηκεύει στοιχεία προσωπικής αναγνώρισης και ένα μοναδικό αναγνωριστικό που θα συνδέεται με τις πληροφορίες του επισκέπτη στη βάση δεδομένων του US-VISIT (Wright & Hert, 2012).

Σχετικά με το έργο US-VISIT, έχουν δημοσιευθεί αναφορές που περιέχουν σχετικά λεπτομερείς πληροφορίες για την αρχιτεκτονική του συστήματος, τις ροές δεδομένων και τους ελέγχους πρόσβασης, ενώ παράλληλα εξετάζουν τις απειλές κατά της ιδιωτικότητας και παρουσιάζουν τεχνικές μετριασμού με σαφή διαγράμματα. Σε μια προσπάθεια, το έργο να προωθηθεί με τη συμμετοχή του κοινού το Γραφείο Προστασίας Προσωπικών Δεδομένων πραγματοποίησε συναντήσεις με τις οργανώσεις προστασίας της ιδιωτικής ζωής και της μετανάστευσης για να διερευνήσει περαιτέρω τις ανησυχίες που προκύπτουν από την χρήση RFID σχετικά με την ιδιωτικότητα.

Γενικά το έργο θεωρείται ως υψηλής ποιότητας όσον αφορά τα θέματα ιδιωτικότητας, «που μπορεί να χρησιμεύσει ως πρότυπο για άλλα εθνικά συστήματα που αφορούν την ασφάλεια» (Wright & Hert, 2012), παρά τις κριτικές πως από τη διαβούλευση έλειψαν τα ουσιαστικά συμπεράσματα.

Virginia High School

Η εταιρία παροχής συστήματα RFID, Ekahau, ανακοίνωσε την εισαγωγή των RFID-over-WiFi real-time location system (RTLS) στο Γυμνάσιο Patrick Henry, στο Glade Spring. Το σχολείο χρησιμοποιεί αυτή την τεχνολογική λύση για να εξασφαλίσει την ασφάλεια και να υποστηρίξει τις διαδικασίες αντιμετώπισης καταστάσεων έκτακτης ανάγκης. Το σύστημα αποτελείται από WiFi-based ετικέτες RFID, υπέρυθροι (IR) φάροι και το λογισμικό ανάγνωσης και ελέγχου Vision της Ekahau.

Το σχολείο αρχικά δοκίμασε το σύστημα για τυχόν προβλήματα και δυσκολίες σε χρόνο τριών ημερών, ελέγχοντας αν μπορεί να ανταποκριθεί σε καθημερινό επίπεδο αλλά και σε καταστάσεις έκτατης ανάγκης. Σήμερα το γυμνάσιο έχει 60 Ekahau B4 κονκάρδες (badges) για τα μέλη ΔΕΠ, συμπεριλαμβανομένων των διαχειριστών, των εκπαιδευτικών, των επιστατών, καθώς και του προσωπικού της καφετέριας και τη νοσοκόμα.

Η κονκάρδα B4 μπορεί να εντοπιστεί και να παρακολουθηθεί από το λογισμικό Ekahau RTLS μέσω οποιουδήποτε εκπομπής WiFi σήματος και έτσι μπορεί να επιτευχθεί μεγάλο επίπεδο ακρίβειας. Το κάθε RFID badge εκπέμπει ένα μοναδικό ID αριθμό το οποίο σχετίζετε με τις πληροφορίες του εκάστοτε εργαζομένου που είναι αποθηκευμένες και ταυτοποιούνται μέσω του λογισμικού.

Οι εργαζόμενοι του σχολείου φορούν το RFID badge τους καθ’ όλη την παρουσία τους στον χώρο του γυμνασίου και σε περίπτωση ιατρικού περιστατικού, περιστατικών εμπλοκής μαθητών σε παράτυπες δραστηριότητες ή άλλου είδους καταστάσεις, έχουν την δυνατότητα να πατήσουν τον διακόπτη ασφάλειας που υπάρχει πάνω στην κονκάρδα προκειμένου να ειδοποιήσουν τους συναδέλφους τους και να αποστείλουν μήνυμα έκτακτης ανάγκης στην αστυνομία εάν η κατάσταση το απαιτεί. Μέσα σε δευτερόλεπτα μεταδίδεται μήνυμα μέσω των κονκάρδων, στους κατάλληλους εργαζόμενους που

βρίσκονται μέσα στις εγκαταστάσεις του σχολείου, και έτσι ενημερώνεται το προσωπικό για την φύση της κατάστασης και την τοποθεσία που συμβαίνει.

Η κονκάρδα B4 διαθέτει τρία πλήκτρα κλήσης και ένα διακόπτη συναγερμού, τα οποία μπορούν να προγραμματιστούν για την κλήση διαφορετικών καταστάσεων για κάθε χρήστη. Για παράδειγμα, το πάτημα ενός κουμπιού μπορεί να σημαίνει μία κλήση για απλή βοήθεια, ενώ ο διακόπτης συναγερμού μπορεί να χρησιμοποιηθεί για να καλέσει συναδέλφους που βρίσκονται σε κοντινή απόσταση ώστε να βοηθήσουν σε ένα έκτακτο περιστατικό. Επίσης, το λογισμικό του συστήματος επιτρέπει στην διεύθυνση του σχολείου να στέλνει μαζικά μηνύματα σε όλο το προσωπικό, τα οποία εμφανίζονται στην οθόνη τεχνολογίας LED του RFID badge του κάθε χρήστη. Επιπλέον, η εφαρμογή αυτομάτως καταγράφει και αποθηκεύει όλα τα περιστατικά έκτακτης ανάγκης, κρατώντας στην μνήμη της την ώρα, την τοποθεσία του περιστατικού και τον τρόπο που αυτό διευθετήθηκε, με σκοπό την διάθεση και την χρήση αυτών των πληροφοριών από το διοικητικό συμβούλιο του σχολείου και την αστυνομία.

Το Γυμνάσιο της Virginia εγκατέστησε επίσης ετικέτες RFID για την παρακολούθηση της θερμοκρασίας κατά την διάρκεια του καλοκαιριού, των διακοπών και γενικότερα των ωρών που μένει κλειστό και έτσι ο έλεγχος των εγκαταστάσεων δεν γίνεται πλέον χειροκίνητα. Το σύστημα Ekahau's RTLS συνήθως χρησιμοποιείται σε νοσοκομεία και άλλες εγκαταστάσεις υγείας, αλλά με τον καιρό όλο και περισσότερα σχολεία εισάγουν την τεχνολογία αυτή[8].

6.2 Συνολική εκτίμηση των κινδύνων για την προστασία της ιδιωτικής ζωής

Στο πλαίσιο της συμφωνίας οι εταιρείες, πριν από την εισαγωγή στην αγορά κάθε νέας εφαρμογής έξυπνης ετικέτας, θα διεξάγουν συνολική εκτίμηση των κινδύνων για την ιδιωτικότητα και θα λαμβάνουν μέτρα για την αντιμετώπιση των κινδύνων που έχουν

[8] http://www.rfidportal.gr/%CE%9C%CE%B5%CE%BB%CE%AD%CF%84%CE%B5%CF%82-%CE%A0%CE%B5%CF%81%CE%AF%CF%80%CF%84%CF%89%CF%83%CE%B7%CF%82/%CE%9A%CE%BB%CE%AC%CE%B4%CE%BF%CF%82-%CE%95%CE%BA%CF%80%CE%B1%CE%AF%CE%B4%CE%B5%CF%85%CF%83%CE%B7%CF%82/virginia-high-school/

εντοπιστεί. Θα συμπεριλαμβάνονται πιθανές επιπτώσεις στην προστασία της ιδιωτικής ζωής από συνδέσεις μεταξύ των δεδομένων που συλλέγονται και διαβιβάζονται, και άλλων δεδομένων. Αυτό είναι ιδιαίτερα σημαντικό στην περίπτωση ευαίσθητων προσωπικών δεδομένων, όπως είναι τα βιομετρικά, τα δεδομένα υγείας ή ταυτότητας.

Με το πλαίσιο ΑΕΙ θεσπίστηκε για πρώτη φορά στην Ευρώπη μια σαφής μέθοδος για την αξιολόγηση και την άμβλυνση των επιπτώσεων από κινδύνους για την ιδιωτικότητα που προέρχονται από έξυπνες ετικέτες· η μέθοδος μπορεί να εφαρμοστεί από όλους τους κλάδους που χρησιμοποιούν έξυπνες ετικέτες (για παράδειγμα, από τις μεταφορές, την εφοδιαστική, το λιανικό εμπόριο, την έκδοση εισιτηρίων, την ασφάλεια και την υγειονομική περίθαλψη).

Ειδικότερα, το πλαίσιο ΑΕΙ δεν θα παράσχει μόνο στις επιχειρήσεις την ασφάλεια δικαίου, ότι δηλαδή η χρήση των ετικετών τους είναι σύμφωνη με την ευρωπαϊκή νομοθεσία για την προστασία της ιδιωτικής ζωής, αλλά θα προσφέρει και καλύτερη προστασία στους ευρωπαίους πολίτες και καταναλωτές.

7.Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της ΕΕ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα

Σύμφωνα με το νέο Κανονισμό, σε περιπτώσεις όπου πραγματοποιείται επεξεργασία, χρησιμοποιώντας και νέες τεχνολογίες, λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της, που ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα ελευθερίας των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί εκτίμηση των επιπτώσεων στις πράξεις επεξεργασίας πριν την εκπλήρωσή τους. Απαιτείται ιδίως στις περιπτώσεις:

1) Συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία.
2) Μεγάλης κλίμακας επεξεργασίας δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.
3) Συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

Η εκτίμηση αυτή του υπεύθυνου επεξεργασίας περιέχει τουλάχιστον:

α) Την περιγραφή και τον σκοπό των πράξεων επεξεργασίας, περιλαμβανομένου του έννομου συμφέροντος που επιδιώκει.

β) Την εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων αυτών.

γ) Την εκτίμηση των κινδύνων για τα δικαιώματα των υποκειμένων.

δ) Τα μέτρα αντιμετώπισης των κινδύνων, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων.

Η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας από τους σχετικούς υπευθύνους επεξεργασίας λαμβάνεται δεόντως υπόψη κατά την εκτίμηση του αντίκτυπου των πράξεων επεξεργασίας που εκτελούνται, ιδίως για τους σκοπούς εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων.

Εφόσον έχει οριστεί ο υπεύθυνος προστασίας δεδομένων, ο υπεύθυνος επεξεργασίας ζητά τη γνώμη του κατά τη εκτέλεση της παραπάνω εκτίμησης.

Η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο στο Συμβούλιο Προστασίας Δεδομένων, ο οποίος περιλαμβάνει όποια επεξεργασία απαιτήθηκε ή μη να πραγματοποιηθεί για την εκτίμηση αντίκτυπου. Εάν οι κατάλογοι περιλαμβάνουν δραστηριότητες επεξεργασίας, οι οποίες σχετίζονται με την προσφορά αγαθών ή υπηρεσιών σε υποκείμενα των δεδομένων ή με την παρακολούθηση της συμπεριφοράς τους σε περισσότερα του ενός κράτη μέλη ή οι οποίες ενδέχεται να επηρεάζουν σημαντικά την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα στην Ένωση, η αρμόδια εποπτική αρχή εφαρμόζει τον μηχανισμό συνεκτικότητας.

Όπου ενδείκνυται, ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους για τη σχεδιαζόμενη επεξεργασία, με την επιφύλαξη της προστασίας εμπορικών ή δημόσιων συμφερόντων ή της ασφάλειας των πράξεων επεξεργασίας.

Αντίθετα, όταν η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπεύθυνου επεξεργασίας ή για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας και έχει νομική βάση στο δίκαιο της Ένωσης ή στο δίκαιο του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, δεν υποχρεώνεται να πραγματοποιήσει εκτίμηση αντικτύπου εκτός αν τα κράτη μέλη την κρίνουν απαραίτητη.

Σε περίπτωση μεταβολής ενός κινδύνου, ο υπεύθυνος επεξεργασίας προβαίνει σε επανεξέταση για να εκτιμήσει εάν το είδος της επεξεργασίας είναι σύμφωνο με τους κανόνες.

7.1 Αξιολόγηση επιπτώσεων σχετικά με την προστασία δεδομένων

Σε περιπτώσεις όπου υπάρχει υψηλός κίνδυνος στην επεξεργασία δεδομένων, προκειμένου να μην πληγούν τα δικαιώματα και οι ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας έχει την ευθύνη για τη διενέργεια της αξιολόγησης των επιπτώσεων της ιδιωτικότητας (Privacy Impact Assessment). Αυτό είναι σημαντικό κυρίως λόγω του ότι ο ίδιος ο υπεύθυνος θα μπορεί να κάνει μια αξιολόγηση σχετικά με τη φύση, την προέλευση και τη σοβαρότητα του συγκεκριμένου κινδύνου. Τα αποτελέσματα της αξιολόγησης των επιπτώσεων της ιδιωτικότητας σηματοδοτούν τα μέτρα που θα πρέπει να ληφθούν ώστε η επεξεργασία των προσωπικών δεδομένων να είναι σύμφωνη με τους κανονισμούς. Αν η αξιολόγηση υποδεικνύει ότι η επεξεργασία προσωπικών δεδομένων περιέχει στοιχεία υψηλού κινδύνου, τα οποία ο υπεύθυνος επεξεργασίας, με τη χρήση της τεχνολογίας και το κόστος εφαρμογής, δεν μπορεί να μειώσει, τότε θα πρέπει να υπάρξει διαβούλευση με την αρχή ελέγχου πριν την πραγματοποίηση της επεξεργασίας.

Με την οδηγία 95/46/ΕΚ προβλέπεται γενική υποχρεωτική γνωστοποίηση της επεξεργασίας των προσωπικών δεδομένων στις εποπτικές αρχές. Αν και η υποχρέωση αυτή είχε μεγάλη οικονομική και διοικητική επιβάρυνση, στην ουσία δεν περιορίστηκε σε όλες τις περιπτώσεις το πρόβλημα της προστασίας των προσωπικών δεδομένων. Για το λόγο αυτό, θα πρέπει να δημιουργηθούν αποτελεσματικότερες διαδικασίες και μηχανισμοί που θα εστιάζουν σε εκείνες τις επεξεργασίες δεδομένων που θα περιέχουν πιθανούς κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, εξαιτίας της φύσης, του πλαισίου, των σκοπών και του πεδίου εφαρμογής τους. Οι διαδικασίες και οι μηχανισμοί αυτοί θα πρέπει να συμφωνούν με τις νέες τεχνολογίες αλλά και να λειτουργούν χωρίς να χρειάζεται πάντα να υπάρχει πρωτίστως η αξιολόγηση για την προστασία των προσωπικών δεδομένων από τον υπεύθυνο επεξεργασίας.

Ο υπεύθυνος επεξεργασίας πριν γίνει η επεξεργασία στις παραπάνω περιπτώσεις, θα πρέπει να διενεργεί την αξιολόγηση σχετικά με την προστασία των δεδομένων, για να μπορέσει με αυτό τον τρόπο να εκτιμήσει τη σοβαρότητα και την πιθανότητα του υψηλού κινδύνου υπολογίζοντας τη φύση την έκταση, το πλαίσιο, τους σκοπούς αλλά και τις πηγές του υψηλού κινδύνου. Στην αξιολόγηση θα πρέπει να περιέχονται τα

διάφορα μέτρα, οι εγγυήσεις και οι μηχανισμοί καταπολέμησης του κινδύνου, τα οποία θα είναι σύμφωνα με τους κανονισμούς και θα προστατεύουν τα προσωπικά δεδομένα.

Τα παραπάνω μέτρα θα πρέπει να ισχύουν κυρίως για επεξεργασία δεδομένων μεγάλης ποσότητας με περιφερειακή, εθνική ή υπερεθνική εμβέλεια, η οποία σχετίζεται με πολλά υποκείμενα των δεδομένων και πιθανότατα περιέχει υψηλούς κινδύνους. Οι κίνδυνοι αυτοί μπορούν για παράδειγμα να εμφανιστούν εξαιτίας π.χ. της ευαισθησίας της σε τεχνολογία ευρείας κλίμακας ή όταν σχετίζεται με τα δικαιώματα και τις ελευθερίες των υποκείμενων προσωπικών δεδομένων. Παράλληλα θα πρέπει να γίνεται αξιολόγηση για την προστασία προσωπικών δεδομένων όταν αυτά σχετίζονται με αποφάσεις που αφορούν συγκεκριμένα φυσικά πρόσωπα με ποινικές καταδίκες, αδικήματα και μέτρα ασφάλειας. Επιπλέον, απαραίτητη είναι η αξιολόγηση των επιπτώσεων της ιδιωτικότητας σε περιπτώσεις που η προστασία προσωπικών δεδομένων σχετίζεται με την παρακολούθηση δημόσιων χώρων και τη χρήση οπτικοακουστικών συσκευών σε αυτούς, καθώς εδώ πιθανώς περιέχονται κίνδυνοι καταπάτησης των δικαιωμάτων και των ελευθεριών των ατόμων, καθώς αδυνατούν να ασκήσουν κάποιο δικαίωμα , ή να χρησιμοποιήσουν μια σύμβαση. Η επεξεργασία των προσωπικών δεδομένων δεν βρίσκεται σε μεγάλη κλίμακα όταν αφορά δεδομένα ασθενών ή πελατών ιδιώτη γιατρού, ή επαγγελματία που σχετίζεται με τον τομέα της υγείας ή δικηγόρων. Στις συγκεκριμένες περιπτώσεις η αξιολόγηση των επιπτώσεων της ιδιωτικότητας δεν είναι υποχρεωτική.

Το αντικείμενο της αξιολόγησης των επιπτώσεων της ιδιωτικότητας που αφορά την προστασία δεδομένων, πολλές φορές μπορεί να υπερβαίνει ένα μεμονωμένο σχέδιο. Για παράδειγμα, περιπτώσεις όπου δημόσιες αρχές ή φορείς πρόκειται να εγκαθιδρύσουν μια κοινή εφαρμογή ή πλατφόρμα επεξεργασίας, ή όταν σχεδιάζεται μια κοινή εφαρμογή ή περιβάλλον επεξεργασίας σε ένα βιομηχανικό τομέα ή κλάδο ή για μια ευρέως χρησιμοποιούμενη οριζόντια δραστηριότητα από πολλούς υπεύθυνους επεξεργασίας.

Όταν η αξιολόγηση δηλώνει ότι η επεξεργασία δεδομένων που δεν χρησιμοποιεί διασφαλίσεις και μέτρα προστασίας, περιέχει υψηλούς κινδύνους καταπάτησης των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων και ο υπεύθυνος επεξεργασίας δεν είναι σε θέση να ελαχιστοποιήσει αυτούς τους κινδύνους, τότε πρέπει να διενεργείται διαβούλευση με την εποπτική αρχή πριν από την έναρξη των δραστηριοτήτων

επεξεργασίας. Οι κίνδυνοι αυτοί μπορεί να προέλθουν από διάφορες μορφές επεξεργασίας ή από τη συχνότητα και το βαθμό της επεξεργασίας, οι οποίοι είναι δυνατό να οδηγήσουν σε επεμβάσεις των δικαιωμάτων και των ελευθεριών, ακόμη και σε ζημία αυτών. Για το λόγο αυτό η εποπτική αρχή θα πρέπει να έχει άμεση ανταπόκριση στην εντολή για διαβούλευση, παρόλα αυτά όμως η μη τήρηση του χρονικού διαστήματος δεν σημαίνει ότι θίγονται οι παρεμβάσεις της και οι εξουσίες της, όπως π.χ. η εξουσία απαγόρευσης πράξεων επεξεργασίας. Μέσα σε αυτά τα πλαίσια μπορεί να γίνει γνωστοποίηση των αποτελεσμάτων στην εποπτική αρχή, αλλά και τα μέτρα που σχετίζονται με τη μείωση των κινδύνων για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων.

Συμπεράσματα

Η ιδιωτικότητα αποτελεί αρχικά ένα από τα βασικά ανθρώπινα δικαιώματα το οποίο μπορεί να είναι και αρκετά ευάλωτο. Το δικαίωμα αυτό περιλαμβάνει τουλάχιστον δυο εκδοχές, το δικαίωμα των ατόμων να ελέγχουν το φυσικό τους χώρο αλλά και των προσωπικών τους πληροφοριών.

Έτσι, η ιδιωτικότητα περιλαμβάνει το δικαίωμα του ατόμου να ελέγχει την συλλογή, χρήση και αποκάλυψη των προσωπικών του δεδομένων. Υπάρχουν πολλοί ορισμοί της ιδιωτικότητας οι οποίοι ποικίλουν ανάλογα με το περιβάλλον, την κουλτούρα και το πλαίσιο εφαρμογής της, αλλά το σίγουρο είναι πως σχετίζεται άμεσα με την ανθρώπινη προσωπικότητα. Πολλές φορές βέβαια παρατηρείται σύγχυση ή και ταύτιση της έννοιας όταν χρησιμοποιείται με τον προσδιορισμό του απορρήτου και της εμπιστευτικότητας. Οι συγκεκριμένοι όροι αν και παρουσιάζουν πολλά όμοια χαρακτηριστικά, ωστόσο δεν πρέπει να ταυτίζονται.

Σύμφωνα με τα όσα αναφέρθηκαν σε παραπάνω σημεία της παρούσας εργασίας, μπορούμε να την διαχωρίσουμε στην ιδιωτικότητα της πληροφορίας (information privacy), την ιδιωτικότητα των επικοινωνιών (privacy of communication), την σωματική ιδιωτικότητα (bodily privacy) και την εδαφική ιδιωτικότητα (territorial privacy).

Ως εργαλείο διασφάλισης της ιδιωτικότητας κατά τον σχεδιασμό ενός συστήματος ή μιας διαδικασίας οι οργανισμοί εφαρμόζουν την Αξιολόγηση Επιπτώσεων στην Ιδιωτικότητα, δηλαδή το κατά πόσο καλύπτονται οι ανάγκες του συστήματος σχετικά με την ιδιωτικότητα. Οι εφαρμογές της ΑΕΙ εφαρμόζονται με κατευθυνόμενες ερωτήσεις που βασίζονται στις απαιτήσεις της ιδιωτικότητας και είναι εξαιρετικές για την εφαρμογή των αρχών της Ιδιωτικότητας δια του Σχεδιασμού στον οργανισμό και πολλές φορές , οι Αξιολογήσεις Επιπτώσεων στην Ιδιωτικότητα, διεξάγονται παράλληλα με τις αξιολογήσεις απειλών/επικινδυνότητας που είναι βασικές για την συνολική προστασία της ιδιωτικότητας. Στόχοι μιας ΑΕΙ είναι η συμμόρφωση του οργανισμού ως προς τις νομικές και ρυθμιστικές απαιτήσεις που αφορούν την ιδιωτικότητα και το χτίσιμο και η εξωτερίκευση του προγράμματος διαχείρισης πληροφοριών και επικινδυνότητας του

οργανισμού, που συμπεριλαμβάνει την γνωστοποίηση των αρχών της Ιδιωτικότητας δια του Σχεδιασμού.

Μία ΑΕΙ η οποία εξετάζει μόνο την αυστηρή τήρηση των κανονισμών δεν θα έχει να παρέχει πολλά στον χρήστη, παρά μόνο τις τυπικές προδιαγραφές τήρησης της ιδιωτικότητας. Όμως, θα προσδιορίσει τα ζητήματα προστασίας της ιδιωτικότητας που ο ενδιαφερόμενος οργανισμός θα πρέπει να διαχειριστεί, ακόμη κι αν δεν είναι παραβιάσεις των ισχυόντων ρυθμιστικών κανόνων. Εκτός από τις συνέπειες που επιφέρονται για την ίδια την επιχείρηση ή τον οργανισμό, και άλλοι εμπλεκόμενοι μπορεί να δεχτούν τις επιπτώσεις της παραβίασης της ιδιωτικότητας.

Σύμφωνα με το νέο Κανονισμό, όταν πραγματοποιείται μια επεξεργασία ιδίως με τη χρήση νέων τεχνολογιών, που εγκυμονεί υψηλούς κινδύνους για τα δικαιώματα, ο υπεύθυνος επεξεργασίας διενεργεί εκτίμηση των επιπτώσεων σε αυτήν την πράξη, πριν την εκτέλεσή της. Η εποπτική αρχή ανακοινώνει τα περιεχόμενα των πράξεων που απαιτήθηκαν για την εκτίμηση αυτή στο Συμβούλιο Προστασίας Δεδομένων.

Έτσι, αντιλαμβανόμαστε ότι γίνεται γνωστοποίηση των αποτελεσμάτων της εκτίμησης επιπτώσεων στην εποπτική αρχή, αλλά και των μέτρων που σχετίζονται με τη μείωση των κινδύνων για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων.

Στη σημερινή σύγχρονη κοινωνία της πληροφορίας υπάρχουν πλέον εξελιγμένες τεχνολογίες πληροφοριών και επικοινωνιών. Αν και τα νέα αυτά πληροφοριακά συστήματα διευκολύνουν σε μεγάλο βαθμό στις καθημερινές συναλλαγές των ατόμων, και παράλληλα ενισχύουν την καθημερινή επικοινωνία και ανταλλαγή πληροφοριών μεταξύ των ατόμων, δημιουργούν ωστόσο ζητήματα προστασίας της ιδιωτικότητας. Η διαφάνεια στη διαδικασία αυτή μπορεί επίσης να είναι ένας τρόπος για την αποφυγή των μελλοντικών ευθυνών που μπορεί να βαρύνουν τα χαμηλότερα επίπεδα διοίκησης ενός οργανισμού αφενός σε γενικότερο επίπεδο, αλλά και το ατομικό δικαίωμα του καθενός στην ιδιωτικότητα.

Βιβλιογραφία

Ξένη

A Digital Agenda for Europe, European Commission, 2015 Διαθέσιμο στο: https://ec.europa.eu/digital-agenda/en

Auerbach, N. C. (2004). Anonymous digital identity in e-Government (Doctoral dissertation, Universität Zürich. Wirtschaftswiss. Fakultät).

Bloustein, E. J. (2002). Individual & Group Privacy (Ppr). Transaction Publishers.

Cavoukian, A (2002). Privacy and Digital Rights Management (DRM): An Oxymoron?. Information and Privacy Commissioner Ontario.

Cavoukian, A. (2011). Patience, persistence, and faith: Evolving the gold standard in privacy and data protection. In Future Challenges in Security and Privacy for Academia and Industry (pp. 1-16). Springer Berlin Heidelberg.

Cavoukian, A. (2013). Privacy by Design: Leadership, methods, and results. In European Data Protection: Coming of Age (pp. 175-202). Springer Netherlands.

Clarke, R. (2009). Privacy impact assessment: Its origins and development. Computer law & security review, 25(2), 123-135.

Culnan, M. J., & Williams, C. C (2009). How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. Mis Quarterly, 673-687.

Hustinx, P. (2005). Data protection in the European Union. Privacy & Informatie, 2, 62-65.

Miller, A. R. (1971). The assault on privacy: computers, data banks, and dossiers. University of Michigan Press.

Palanisamy, R., & Mukerji, B. (2012). Security and Privacy issues in e-Government. IGI Global, 236-248.

Rosenberg, R. S. (2013). The social impact of computers. Elsevier.

Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania law review, 477-564.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C., & Gritzalis, S. (2011). Unifying ISO Security Standards Practices into a Single Security Framework. In Proceedings of the South African Information Security Multi-Conference: Port Elizabeth, South Africa, 17-18 May 2010 (p. 188). Lulu. com.

Vrakas, N., Kalloniatis, C., Tsohou, A., & Lambrinoudakis, C. (2010). Privacy requirements engineering for trustworthy e-government services. In Trust and Trustworthy Computing (pp. 298-307). Springer Berlin Heidelberg.

Wright, D., & De Hert, P (2011). Privacy impact assessment (Vol. 6). Springer Science & Business Media.

Wright, D (2012). The state of the art in privacy impact assessment. Computer Law & Security Review, 28(1), 54-61.

Wright, D., & De Hert, P (2012). Introduction to privacy impact assessment. In Privacy Impact Assessment (pp. 3-32). Springer Netherlands.

Ελληνική

Ακριβοπούλου, Χ. (2009). Μεταξύ αυτονομίας και οικειότητας: αναπροσδιορίζοντας το δικαίωμα στην ιδιωτική ζωή (άρθρο 9 παρ. 1 Σ).

Ιγγλεζάκης, Ι., 2007. Εισαγωγή στο δίκαιο της πληροφορικής. 1η Έκδοση. Αθήνα: Σάκκουλα

Μήτρου, Λ., 2006. Προστασία Προσωπικών Δεδομένων, Σάμος: Πανεπιστήμιο Αιγαίου

Μήτρου, Λ., 2010. Η Προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνίες. Η νομική διάσταση. In: Κ. Λαμπρινουδάκης, ed. Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών. Αθήνα: Παπασωτηρίου, pp. 505 - 552.