Τμήμα Ηλεκτρολόγων Μηχανικών
και Μηχανικών Υπολογιστών

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Τυπική αναπαράσταση του νομοθετικού πλαισίου της προστασίας προσωπικών δεδομένων»

Επιμέλεια / Συγγραφή

Δεσύλλα Ελένη ΑΜ: 2271
Μπάμπου Χαρά-Λουκία ΑΜ:0969

Επιβλέπων καθηγητής

Ασημακόπουλος Γιώργος

Μάρτιος 2020

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Αντίρριο, _ _ / _ _ / _ _ _ _

1. [Ονοματεπώνυμο, Υπογραφή]
2. [Ονοματεπώνυμο, Υπογραφή]
3. [Ονοματεπώνυμο, Υπογραφή]

Ευχαριστίες

Αρχικά, θα θέλαμε να ευχαριστήσουμε τις οικογένειες μας για την πολύτιμη βοήθειά τους και τη στήριξή τους όλα αυτά τα χρόνια οι οποίες φρόντισαν για την καλύτερη δυνατή μόρφωσή μας. Επίσης θέλουμε να ευχαριστήσω θερμά την καθηγήτρια μας Σερεμέτη Λαμπρινή του τμήματος Μηχανικών Πληροφορικής Τ.Ε. Δυτικής Ελλάδας κυρίως για την εμπιστοσύνη που μας έδειξε και την υπομονή της κατά τη διάρκεια υλοποίησης της πτυχιακής μας εργασίας, όπως επίσης και για την πολύτιμη βοήθειά και καθοδήγησή της για την επίλυση διάφορων θεμάτων.

Περίληψη

Σκοπός της παρούσας εργασίας είναι η τυπική αναπαράσταση του νομοθετικού πλαισίου της προστασίας προσωπικών δεδομένων Μέσα από την ενδελεχή εξέταση ορισμένων εκ των πιο καίριων ζητημάτων που αναδύονται, αποσκοπούμε σε μια, όσο το δυνατόν πιο, ολιστική περιγραφή των ανωτέρω αυτών θεμάτων. Η ανασκόπηση της παγκόσμιας βιβλιογραφίας εξυπηρετεί ακόμα περισσότερο τον στόχο της εργασίας, καθότι δίδεται η ευκαιρία στον αναγνώστη να αποκτήσει άποψη για τις πιο σύγχρονες εξελίξεις,. Επίσης στην εργασία, γίνεται αναφορά στις οντολογίες που έχουν νομοθετικό περιεχόμενο και στην ανάπτυξη της οντολογίας Privacy Policy που αντιστοιχεί στην προστασία προσωπικών δεδομένων Στο πλαίσιο αυτό, η προστασία των προσωπικών δεδομένων αποτελεί ένα θέμα που προσελκύει το αυξανόμενο ενδιαφέρον της επιστημονικής και επαγγελματικής παγκόσμιας κοινότητας.

Λέξεις κλειδιά: Προσωπικά δεδομένα, προστασία, νομοθετικό πλαίσιο, κίνδυνοι

Abstract

The purpose of this paper is to formally represent the legal framework for the protection of personal data. Through a thorough examination of some of the most important issues that arise, we aim to provide as holistic a description of these issues as possible. A review of the world literature further serves the purpose of the work, as it gives the reader the opportunity to gain insight into the most up-to-date developments. Also in the work, reference is made to the ontologies that have legislative content and to the development of the Privacy Policy ontology corresponding to the protection of personal data.

Keywords: personal data, protection, legal framework, risks

Περιεχόμενα

Κεφάλαιο 1. Εισαγωγή

1.1 Ιστορία

Στην εποχή που ζούμε η επιστήμη και τεχνολογία έχουν φθάσει σε τέτοια επίπεδα προόδου, ώστε πλέον τα τεχνολογικά επιτεύγματα του σήμερα, αύριο να είναι πλέον ξεπερασμένα. Σήμερα η ανθρωπότητα περνά σε μια καινούργια εποχή της Ιστορίας της, είναι εποχή της «κοινωνίας της πληροφορίας ». Στη καινούργια αυτή εποχή, η εκτεταμένη εφαρμογή της τεχνολογίας των υπολογιστών και του διαδικτύου σε όλο και περισσότερες δραστηριότητες του ανθρώπου δεν μπορεί ν' αφήνει κανένα αδιάφορο, αφού οι καθημερινές συνέπειες είναι για όλους συνταρακτικές. Το δίκαιο και η απονομή της δικαιοσύνης δέχονται ραγδαίες τις επιπτώσεις των νέων τεχνολογιών σ' ολόκληρο τον κόσμο . Σε παγκόσμιο επίπεδο συντελείται μια αληθινή επανάσταση που αγγίζει όλους τους τομείς του δημόσιου και ιδιωτικού βίου και επηρεάζει τόσο την σταδιακή διαμόρφωση ενός καινούργιου καθεστώτος στην διαμόρφωση του δικαίου, όσο και τη διαμόρφωση άλλων ουσιαστικών και δικονομικών κανόνων απονομής της δικαιοσύνης[1].

Η ανάπτυξη των νέων τεχνολογιών και οι νέες μορφές διαφήμισης και ηλεκτρονικών συναλλαγών και κυρίως η συλλογή πάσης φύσεως πληροφοριών μέσω ηλεκτρονικών υπολογιστών οδήγησαν στην αυξημένη ζήτηση προσωπικών πληροφοριών από τον ιδιωτικό και δημόσιο τομέα. Οι προσωπικές αυτές πληροφορίες που αναφέρονται σε κάθε είδους δραστηριότητα, είτε προσωπική είτε επαγγελματική του ατόμου, ονομάζονται προσωπικά δεδομένα. Η προστασία δεδομένων προσωπικού χαρακτήρα εισήχθη στα προηγμένα τεχνολογικά κράτη πριν από σαράντα περίπου χρόνια με στόχο την προστασία των πολιτών από την αυτοματοποιημένη επεξεργασία των προσωπικών τους δεδομένων που τότε μόλις είχε αρχίσει να διενεργεί ο δημόσιος τομέας. Την εποχή εκείνη οι υπολογιστές ήταν πολύ ακριβοί και, πολύ ογκώδεις για να χρησιμοποιούνται από τον ιδιωτικό τομέα, ο οποίος άλλωστε δεν έδειχνε ιδιαίτερο ενδιαφέρον στη συλλογή και επεξεργασία προσωπικών στοιχείων. Η κατάσταση έχει αλλάξει σήμερα ριζικά. Ήδη από τη δεκαετία του '80 η υπολογιστική ισχύς αυξήθηκε γεωμετρικά και έγινε προσιτή στον καθένα[2].

Παράλληλα, το άνοιγμα των αγορών και η ανάγκη για αύξηση των πωλήσεων καθιέρωσαν

[1] Αλεξανδροπούλου-Αιγυπτιάδου, Ε., (2016). Προσωπικά Δεδομένα, Νομική Βιβλιοθήκη
[2] Allianz Global Corporate Specialty. (2015), "A Guide to Cyber Risk"

νέες υπηρεσίες, όπως το στρατηγικό marketing ή τη μεταπολιτική υποστήριξη. Η τεράστια πρόοδος της πληροφορικής, η ανάπτυξη νέων τεχνολογιών, οι νέες μορφές διαφήμισης και ηλεκτρονικών συναλλαγών και η ανάγκη της ηλεκτρονικής οργάνωσης του κράτους έχουν σαν συνέπεια την αυξημένη ζήτηση προσωπικών πληροφοριών από τον ιδιωτικό και δημόσιο τομέα. Η ανεξέλεγκτη καταχώριση και επεξεργασία των προσωπικών 2 δεδομένων σε ηλεκτρονικά και χειρόγραφα αρχεία υπηρεσιών, εταιρειών και οργανισμών μπορεί να δημιουργήσει προβλήματα στην ιδιωτική ζωή του πολίτη.Οι κίνδυνοι αυτοί αυξάνονται με τις νέες δυνατότητες ταχύτατης μεταφορά πληροφοριών παγκοσμίως μέσω του Internet. Αποτέλεσμα όλων αυτών ήταν η μαζική πλέον συλλογή και επεξεργασία προσωπικών δεδομένων από τον ιδιωτικό τομέα με σκοπό την επίτευξη κέρδους[3]. Η νομοθεσία περί προστασίας δεδομένων ήρθε έτσι αντιμέτωπη με μια ποσοτική και ποιοτική ανατροπή των στόχων της, που κλήθηκε να αντιμετωπίσει ουσιαστικά με τα ίδια νομικά μέσα. Η εξέλιξη των πραγμάτων ανέδειξε την προστασία δεδομένων ως τη μοναδική νομική τροχοπέδη στις σημαντικότερες τεχνολογικές και επιχειρηματικές εξελίξεις μέχρι και σήμερα. Πράγματι, η νομοθεσία περί προστασίας δεδομένων προσωπικού χαρακτήρα επιχείρησε να θέσει περιορισμούς κυρίως στο ηλεκτρονικό εμπόριο, στο στρατηγικό marketing, στη γενετική έρευνα και στις τηλεπικοινωνίες[4].

Οι περιορισμοί αυτοί δεν έγιναν σχεδόν ποτέ αποδεκτοί από την αγορά, αφού εν τέλει της στερούσαν επικερδείς δραστηριότητες. Έτσι, ενώ η αγορά συνεργάστηκε με τη νομική επιστήμη σε τομείς του δικαίου όπου ο κεντρικός έλεγχος ήταν ευπρόσδεκτος, λ.χ. στην προστασία της πνευματικής ιδιοκτησίας ή στα εγκλήματα χρήσης υπολογιστών, στην περίπτωση της προστασίας δεδομένων προσωπικού χαρακτήρα αναπτύχθηκε αναπόφευκτα μια αντιπαλότητα, η οποία βρίσκεται σήμερα σε έξαρση . Με αφορμή όμως, την αποκάλυψη γεγονότων διαφθοράς στην δημόσια ζωή του τόπου μας αλλά και διεθνώς, έχει ανοίξει μια τεράστια συζήτηση σχετικά με την δήθεν αντίθεση του ατομικού δικαιώματος της προστασίας των προσωπικών δεδομένων που απαντάται στη διάταξη του άρθρου 9Α του Συντάγματος και της αρχή της διαφάνειας που απαντάται στη διάταξη του άρθρου 10 παρ 3 του Συντάγματος για την ελεύθερη και αδιακώλυτη πρόσβαση στα διοικητικά έγγραφα αλλά και στις διατάξεις των άρθρων 14 παρ 9 ,29 παρ 2 , 102 παρ 5 103 παρ 7 Σ. Το ζήτημα ως προς τι ακριβώς πρέπει να γίνει, όταν στα διοικητικά έγγραφα ενσωματώνονται και προσωπικά δεδομένα, είναι θέμα καθημερινής πρακτικής στις δράσης της Διοικήσεως και των ελεγκτικών μηχανισμών του Κράτους. Νομίζω ότι το πρόβλημα αφορά την σωστή και αποτελεσματική λειτουργία της Πολιτείας, αλλά και την εύρυθμη

[3] Allianz Global Corporate Specialty. (2015), "A Guide to Cyber Risk"
[4] Κοτσαλής, Λ., (2016). Προσωπικά Δεδομένα, Ανάλυση-Σχόλια-Εφαρμογή, Νομική Βιβλιοθήκη

λειτουργία της Δημόσιας διοίκησης[5].

1.2 Προκλήσεις

Η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) υπογράφηκε στη Ρώμη στις 4/11/1950 μεταξύ των κρατών μελών του Συμβουλίου της Ευρώπης και τέθηκε σε ισχύ τον Σεπτέμβριο του 1953. Απέβλεπε να ενισχύσει την προστασία των δικαιωμάτων που αναφέρονταν στην Σχετική Οικουμενική Διακήρυξη, που είχε ψηφίσει το έτος 1948 η Γενική Συνέλευση των Ηνωμένων Εθνών. Δημιουργήθηκε, έτσι, το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου και προβλέπεται η ενώπιον του ατομική προσφυγή, αφού προηγουμένως εξαντληθούν τα ένδικα μέσα στα εθνικά δικαστήρια. Η σύμβαση αυτή ακυρώθηκε από το Ελληνικό κράτος με το Ν.2329/1953 και τέθηκε ξανά σε ισχύ με το Ν.Δ.53/1974, έκτοτε αποτελεί μέρος της Ελληνικής έννομης τάξης, με υπερέχουσα ισχύ έναντι των κοινών νόμων, ως διεθνής σύμβαση[6].

Το άρθρο 8 της ΕΣΔΑ αναφέρεται στο σεβασμό της ιδιωτικής και οικογενειακής ζωής, χωρίς ειδική αναφορά του δικαιώματος προστασίας των προσωπικών δεδομένων. Σύμφωνα με την νομολογία του Δικαστηρίου Ανθρωπίνων Δικαιωμάτων το άρθρο 8 ΕΣΔΑ ερμηνεύθηκε ώστε τα προσωπικά δεδομένα να θεωρηθούν ειδικότερη έκφανση του γενικού δικαιώματος στην προστασία της ιδιωτικής ζωής. Η τεχνολογική επανάσταση της πληροφορικής και επικοινωνιών και των επιπτώσεων τους στην προστασία της ιδιωτικής ζωής, υποχρέωσε τα κράτη μέλη του Συμβουλίου της Ευρώπης στην υπογραφή της 108/28.1.1981 Σύμβασης του Συμβουλίου της Ευρώπης για τη προστασία των προσώπων έναντι της αυτοματοποιημένης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που κυρώθηκε από όλα τα κράτη μέλη της Ε.Ε. Η Σύμβαση αυτή που ισχύει τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα[7].

Το έτος 1977 με Κοινή Δήλωση το Συμβούλιο, το Κοινοβούλιο και η Επιτροπή διακήρυξαν πανηγυρικά ότι οφείλουν κατά την άσκηση των καθηκόντων τους να σέβονται τα ανθρώπινα δικαιώματα, όπως αυτά κατοχυρώνονται στα εθνικά συντάγματα των κρατών μελών και στην ΕΣΔΑ. Η ίδια διατύπωση επαναλαμβάνεται στην Ενιαία Ευρωπαϊκή Πράξη (το πρώτο κείμενο που τροποποίησε ουσιαστικά τις Συνθήκες) του έτους 1987. Στις 24 Οκτωβρίου 1995 το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο

[5] Anderson, R. and Moore, T. (2006), "The Economics of Information Security", Science, 314 (5799), pp. 610-613
[6] Γαμπά, Δ., (2018). Σημειώσεις: Παραβίαση της Ασφάλειας των Προσωπικών Δεδομένων
[7] Anderson, R. and Moore, T. (2006), "The Economics of Information Security", Science, 314 (5799), pp. 610-613

θέσπισαν την Οδηγία 95/46 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών Πρόκειται για ένα από τα πληρέστερα παγκοσμίως κείμενα για την προστασία προσωπικών δεδομένων, το οποίο δεσμεύει τα κράτη μέλη της Ε.Ε. να εισαγάγουν και να εφαρμόσουν ένα συγκεκριμένο νομικό σύστημα. Υπό την ισχύ του Συντάγματος του 1975 προστατεύονταν η ιδιωτική και οικογενειακή ζωή, δεν υπήρχε όμως πρόβλεψη για την προστασία των προσωπικών δεδομένων. Είχε, όμως, κριθεί αυτό από το ΣτΕ ότι στην ιδιωτική ζωή περιλαμβάνονταν, μεταξύ άλλων και προστατεύονταν κάθε τι που αφορά την υγεία του προσώπου, οι θρησκευτικές του πεποιθήσεις, η οικογενειακή συμπεριφορά του και η ερωτική του ζωή.

Άλλωστε, το δικαίωμα στην προστασία από την επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορούσε να θεμελιωθεί και επί των συνταγματικών διατάξεων σεβασμού της αξίας του ανθρώπου και της ελεύθερης ανάπτυξης της προσωπικότητας που προστατεύονται εξ άλλου και με την σύμβαση για τα ανθρώπινα δικαιώματα (ΕΣΔΑ). Το έτος 1995 εκδόθηκε η γνωστή Οδηγία 95/46 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου προς τα Κράτη – μέλη «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», η οποία και τα υποχρέωσε να θέσουν σε ισχύ τις αναγκαίες νομοθετικές κανονιστικές και διοικητικές διατάξεις για να συμμορφωθούν προς το περιεχόμενό της.[8]

Το Ελληνικό κράτος συμμορφώθηκε με την ως άνω επιταγή και εξέδωσε τον Ν.2472/1997 «περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» και ίδρυσε τη ανεξάρτητη Αρχή Προστασίας Προσωπικών Δεδομένων με σκοπό την εποπτεία και έλεγχο της τήρησης του νόμου αυτού, καθώς και άλλων ρυθμίσεων όπως αυτών του Ν.2774/1999 για τις δημόσιες τηλεπικοινωνίες, καθώς και τον πιο πρόσφατο ν.3471/2006 όπως επίσης και την ενάσκηση των αρμοδιοτήτων που κάθε φορά της ανατίθενται[9]. Με το ψήφισμα της Ζ΄ Αναθεωρητικής Βουλής των Ελλήνων της 6ης Απριλίου 2001 προστέθηκε στο Σύνταγμα η διάταξη του άρθρου 9Α με την οποία η προστασία των προσωπικών δεδομένων στην Ελλάδα κατοχυρώθηκε και συνταγματικά . Σύμφωνα με το άρθρο 286 της Συνθήκης για την ΕΚ, η Κοινότητα αυτοδεσμεύεται να τηρεί και η ίδια την Οδηγία. Σύμφωνα με την Οδηγία αυτή, «προσωπικά δεδομένα» είναι

[8] Antonucci, D. (2017), "The Cyber Risk Handbook, Creating and Measuring Effective Cybersecurity Capabilities", Published by John Wiley & Sons, Inc. Hoboken, New Jersey

[9] Μυρτίδης, Δ., (2008). Μέσα Τραπεζικής Εργασίας, Τραπεζική Πληροφορική, τόμος Β, ΕΑΠ, Πάτρα

κάθε πληροφορία που αναφέρεται σε έναν άνθρωπο, η ταυτότητα του οποίου μπορεί να προσδιοριστεί. Καμία χρήση («επεξεργασία») αυτών των δεδομένων δεν επιτρέπεται, αν ο σκοπός της δεν είναι νόμιμος, θεμιτός και καθορισμένος[10].

Για να είναι νόμιμη η χρήση πρέπει τα δεδομένα να είναι κατάλληλα, ακριβή, συναφή προς τον σκοπό συλλογής και χρήσης και όχι περισσότερα από όσα χρειάζονται ενόψει αυτού του σκοπού. Η χρήση των δεδομένων για άλλο σκοπό από αυτόν που αρχικά συγκεντρώθηκαν, απαγορεύεται! Επίσης δεν πρέπει να διατηρούνται για χρονική διάρκεια πέραν από την αναγκαία για την εξυπηρέτηση του σκοπού για τον οποίο έγινε η συλλογή (άρθρο 5). Αξίζει να ξέρουμε ότι η Ευρωπαϊκή Ένωση για λόγους δημόσιας ασφάλειας, έχει εκδώσει την Οδηγία διατήρησης τηλεπικοινωνιακών δεδομένων για αντεγκλητικούς σκοπούς, το Σχέδιο Απόφασης-Πλαισίου του Συμβουλίου ΕΕ για την προστασία προσωπικών δεδομένων στο πεδίο της αστυνομικής και δικαστικής συνεργασίας των κρατών σε ποινικές υποθέσεις. Στη Ευρωπαϊκή Ένωση υπάρχει ένας νέος κοινοτικός θεσμός: του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ο οποίος αποτελεί την αρμόδια ανεξάρτητη αρχή της ΕΕ[11].

[10] Μυρτίδης, Δ., (2008). Μέσα Τραπεζικής Εργασίας, Τραπεζική Πληροφορική, τόμος Β, ΕΑΠ, Πάτρα
[11] Κοτσαλής, Λ., Μενουδάκος, Κ., (2018). Γενικός Κανονισμός για την Προστασία Προσωπικών Δεδομένων GDPR, Νομική Βιβλιοθήκη

Κεφάλαιο 2. Νομοθετικό πλαίσιο προστασίας προσωπικών δεδομένων

2.1 Ορισμός προσωπικών δεδομένων

Προσωπικά δεδομένα είναι κάθε πληροφορία που αναφέρεται στο πρόσωπο του κάθε ατόμου, όπως: το όνομα και το επάγγελμά του, η οικογενειακή του κατάσταση, η ηλικία του, ο τόπος κατοικίας, η φυλετική του προέλευση, τα πολιτικά του φρονήματα, η θρησκεία που πιστεύει, οι φιλοσοφικές του απόψεις, η συνδικαλιστική του δράση, η υγεία του, η ερωτική του ζωή και οι τυχόν ποινικές του διώξεις και καταδίκες. Δεν θεωρούνται προσωπικά δεδομένα πληροφορίες από τις οποίες δεν δύναται να ταυτοποιηθεί ένα συγκεκριμένο άτομο. Ειδικότερα, πολλά από τα προαναφερθέντα προσωπικά δεδομένα είναι ευαίσθητα, έχουν δηλαδή ιδιαίτερη βαρύτητα για το σχηματισμό της εικόνας της προσωπικότητας του ατόμου. Αυτά είναι η φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, οι θρησκευτικές ή φιλοσοφικές πεποιθήσεις, η συμμετοχή σε ένωση, σωματείο και συνδικαλιστική οργάνωση, η υγεία, η κοινωνική πρόνοια και η ερωτική ζωή, καθώς και τα σχετικά με ποινικές διώξεις ή καταδίκες[12].

Πριν προχωρήσουμε σε οποιουδήποτε είδους ανάλυση της προστασίας των δεδομένων προσωπικού χαρακτήρα κρίνεται απαραίτητη η αναφορά μερικών σχετικών με το θέμα ορισμών. Πρόκειται για τους ορισμούς που αναφέρονται στο άρθρο 2 του Ν. 2472/1997, οι οποίοι ουσιαστικά είναι οι ίδιοι με αυτούς του άρθρου 2 της Οδηγίας 95/46/ΕΚ. Εδώ αξίζει να επισημανθεί το γεγονός ότι ο νομοθέτης επέλεξε να συμπεριλάβει στο κείμενο του νόμου τους ορισμούς αυτούς, οι οποίοι σε μεγάλο βαθμό είχαν αποτελέσει ήδη αντικείμενο επεξεργασίας στα πλαίσια της οδηγίας. Παρόλο, δηλαδή, που ο έλληνας νομοθέτης θα μπορούσε να παραλείψει τη δεσμευτική αυτή ως προς το περιεχόμενο της αναφορά των συγκεκριμένων ορισμών στο κείμενο του νόμου, ακολούθησε αυτή τη σχετικά νέα νομοθετική πρακτική της παράθεσης στο κείμενο του νόμου των σχετικών ορισμών. Αυτό μπορεί να ερμηνευθεί είτε ως απόπειρα όσο το δυνατόν πιο πιστής μεταφοράς του κειμένου της οδηγίας στην ελληνική έννομη τάξη είτε ως αποφυγή ασαφειών (ειδικά για «τεχνικά θέματα» όπως είναι σε μεγάλο βαθμό αυτά που σχετίζονται με την προστασία προσωπικών δεδομένων) και συνεπώς ερμηνευτικών παρεκκλίσεων που θα μπορούσαν να θέσουν σε κίνδυνο την ορθή εφαρμογή του νόμου[13].

---

[12] Baer, W. S. and Parkinson, A. (2007), "Cyberinsurance in IT Security Management," IEEE Security and Privacy, 5 (3), pp. 50–56

[13] Baer, W. S. and Parkinson, A. (2007), "Cyberinsurance in IT Security Management," IEEE Security and Privacy, 5 (3), pp. 50–56

Λέγοντας **δεδομένα προσωπικού χαρακτήρα** εννοούμε κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων[14].

Υποκατηγορία των παραπάνω αποτελούν τα **ευαίσθητα δεδομένα,** τα οποία έχουν ιδιαίτερη βαρύτητα για το σχηματισμό της εικόνας της προσωπικότητας του υποκειμένου των δεδομένων και γι' αυτό προστατεύονται με ιδιαίτερη αυστηρότητα. Ως ευαίσθητα χαρακτηρίζονται από το νόμο τα δεδομένα εκείνα, τα οποία αφορούν[15]:

- τη φυλετική ή εθνική προέλευση,
- τα πολιτικά φρονήματα,
- τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις,
- τη συμμετοχή σε ένωση, σωματείο και συνδικαλιστική οργάνωση,
- την υγεία,
- την κοινωνική πρόνοια,
- την ερωτική ζωή, και
- ποινικές διώξεις και καταδίκες.

Υποκείμενο των δεδομένων είναι το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική[16].

Τέλος, λέγοντας **επεξεργασία** εννοούμε κάθε εργασία ή σειρά εργασιών που πραγματοποιείται από το Δημόσιο ή από την ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα. Τέτοιες ενέργειες είναι[17]:

- η συλλογή

[14] Tikkinen-Piri, C., Rohunen, A. and Markulla, J. (2018), "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", Computer Law & Security Review, 34 (1), pp. 134-153

[15] Tikkinen-Piri, C., Rohunen, A. and Markulla, J. (2018), "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", Computer Law & Security Review, 34 (1), pp. 134-153

[16] Ulsch, M. (2014), "Cyber Threat! How to manage the growing risk of cyber attacks", Published by John Wiley & Sons, Ltd.

[17] Ulsch, M. (2014), "Cyber Threat! How to manage the growing risk of cyber attacks", Published by John Wiley & Sons, Ltd.,

- η καταχώριση
- η οργάνωση
- η διατήρηση ή αποθήκευση
- η τροποποίηση
- η εξαγωγή
- η χρήση
- η διαβίβαση
- η διάδοση ή κάθε άλλης μορφής διάθεση
- η συσχέτιση ή ο συνδυασμός
- η διασύνδεση
- η δέσμευση (κλείδωμα)
- η διαγραφή
- η καταστροφή.

2.2 Λόγος προστασίας τους σε σχέση με την εξέλιξη της τεχνολογίας

Η εποχή μας χαρακτηρίζεται από τεχνολογικές εξελίξεις οι οποίες μεταμορφώνουν δραστικά τον τρόπο που ζούμε και εργαζόμαστε. Η πρόοδος των Τεχνολογιών Πληροφορίας και Επικοινωνίας έχει δώσει την ώθηση για την ανάπτυξη και παροχή προηγμένων ηλεκτρονικών υπηρεσιών και τη δημιουργία έξυπνων περιβαλλόντων, με συνέπεια τα όρια μεταξύ του πραγματικού και του ψηφιακού κόσμου των ηλεκτρονικών υπολογιστών να γίνονται πολλές φορές δυσδιάκριτα.[18]

Ωστόσο, η αξιοσημείωτη αυτή πρόοδος η οποία γενικά βελτιώνει την ποιότητα ζωής του σύγχρονου ανθρώπου, εγκυμονεί σοβαρούς κινδύνους για την ιδιωτική ζωή των πολιτών. Περισσότερο από έναν αιώνα από τη δημοσίευση της πρώτης πραγματείας αναφορικά με το γεγονός ότι η ιδιωτική ζωή των πολιτών τίθεται σε κίνδυνο από την τεχνολογική πρόοδο, ποτέ άλλοτε στην ιστορία οι πολίτες δεν ήταν τόσο ανήσυχοι σχετικά με το θέμα αυτό. Τα έξυπνα περιβάλλοντα χαρακτηρίζονται από εκείνο που συνήθως αναφέρεται σαν "πανταχού παρούσα υπολογιστική" (ubiquitous computing). Ο όρος αυτός προέρχεται από ένα άρθρο – ορόσημο του Mark Weiser το οποίο δημοσιεύτηκε πριν από περισσότερο από 15 χρόνια και αναφερόταν σε έναν ιδεατό κόσμο όπου τα υπολογιστικά στοιχεία βρίσκονται παντού, λειτουργούν στο παρασκήνιο με τρόπο διακριτικό και σχεδόν αόρατο,

[18] Wachter, S. (2018), "Internet of Things: Privacy, profiling, discrimination, and the GDPR", Computer Law & Security Review, 34 (3), pp. 436-449

απαλλάσσοντας τον άνθρωπο από ένα μεγάλο μέρος των κουραστικών και τετριμμένων διαδικασιών, τόσο στην προσωπική όσο και στην επαγγελματική του ζωή[19].

Το 1999, η Συμβουλευτική Ομάδα για τις Τεχνολογίες της Κοινωνίας της πληροφορίας (Information Society Technology Advisory Group – ISTAG) της Ευρωπαϊκής Ένωσης χρησιμοποίησε τον όρο ’’περιβάλλουσα ευφυΐα’’ (ambientintelligence) με παρόμοιο τρόπο. Ο όρος χρησιμοποιήθηκε προκειμένου να περιγράψει έναν κόσμο όπου οι άνθρωποι θα περιβάλλονται από έξυπνες και διαισθητικές διεπαφές, ενσωματωμένες σε καθημερινά αντικείμενα και από ένα περιβάλλον το οποίο θα αναγνωρίζει και θα ανταποκρίνεται αναλόγως στην παρουσία των ανθρώπων με τρόπο διακριτικό και αόρατο. Η πανταχού παρούσα υπολογιστική και η περιβάλλουσα ευφυΐα σε συνδυασμό με τη ραγδαία ανάπτυξη και διάδοση των Διαδικτυακών υπηρεσιών και επικοινωνιών και των άλλων μορφών ηλεκτρονικής επικοινωνίας ορίζουν αυτό που στην παρούσα Διατριβή ονομάζεται ‘‘έξυπνα περιβάλλοντα’’. Τα έξυπνα περιβάλλοντα, πέρα από τις προφανείς θετικές πλευρές τους, δημιουργούν σοβαρούς κινδύνους για την προσωπική ζωή[20].

Αυτό οφείλεται κυρίως στους παρακάτω λόγους:

Η κλίμακα της συλλογής προσωπικών δεδομένων αυξάνεται ραγδαία. Πράγματι, όσο τα υπολογιστικά συστήματα καθίστανται ‘‘αόρατα’’ και ενσωματώνονται στο περιβάλλον, η συλλογή όλο και περισσότερων δεδομένων λαμβάνει χώρα, δεδομένων μάλιστα που στο παρελθόν δεν ήταν δυνατό να αποτελέσουν αντικείμενο συλλογής. Χαρακτηριστικό παράδειγμα αποτελεί το ίχνος της γεωγραφικής θέσης σε συνεχή και πραγματικό χρόνο[21].

Ο τρόπος συλλογής προσωπικών δεδομένων είναι διαφορετικός. Στα έξυπνα περιβάλλοντα, όχι μόνο τα υπολογιστικά συστήματα βρίσκονται παντού αλλά διαθέτουν προηγμένες δυνατότητες συλλογής προσωπικών δεδομένων. Χαρακτηριστικά παραδείγματα αποτελούν οι ‘‘έξυπνες’’ κάμερες παρακολούθησης και οι διάφοροι αισθητήρες, όπως είναι οι συσκευές ραδιοσυχνότητας για προσδιορισμό ταυτότητας (Radio Frequency Identification – RFID). Σε πολλές μάλιστα περιπτώσεις, τα προσωπικά δεδομένα συλλέγονται χωρίς τη σχετική γνώση του ατόμου το οποίο αφορούν[22].

[19] Wachter, S. (2018), “Internet of Things: Privacy, profiling, discrimination, and the GDPR”, Computer Law & Security Review, 34 (3), pp. 436-449
[20] Westby, J., R. (2010), “Governance of enterprise security: Cy Lab 2010 report”, Pittsburgh, PA: Carnegie Mellon
[21] Zerlang, J. (2017), “GDPR: a milestone in convergence for cybersecurity and compliance”, Network Security, 17 (6), pp. 8-11
[22] Ανακοινώσεις Τραπεζών Μελών https://www.hba.gr/Media/Details/358

Συλλέγονται νέοι τύποι προσωπικών δεδομένων. Η εξέλιξη της τεχνολογίας έχει δημιουργήσει τις προοπτικές για τη συλλογή δεδομένων που μέχρι πριν από λίγα χρόνια περιοριζόταν από την ικανότητες της ανθρώπινης όρασης και ακοής[23].

Η καταγραφή του ήχου από μεγάλη απόσταση, η παρακολούθηση των επικοινωνιών, ή η παρακολούθηση ολόκληρων γεωγραφικών περιοχών μέσω δορυφόρων που καταγράφουν εικόνες υψηλής ανάλυσης αποτελούν μερικά μόνο χαρακτηριστικά παραδείγματα. Οι προηγμένες υπηρεσίες συλλέγουν από καταναλωτικές συνήθειες και μέχρι ιατρικά δεδομένα και πολιτισμικές ή κοινωνικές συνήθειες και απόψεις. Ακόμα και τα συναισθήματα ενός ανθρώπου θα είναι δυνατό να καταγραφούν στο κοντινό μέλλον με εξαιρετική ακρίβεια μέσω ειδικών συστημάτων[24].

Η ευκολία πρόσβασης στα δεδομένα και οι πρωτοφανείς δυνατότητες που αυτή προσφέρει. Στα έξυπνα περιβάλλοντα, τα προσωπικά δεδομένα όχι μόνο συλλέγονται αλλά και αποθηκεύονται για μεγάλα χρονικά διαστήματα, δυνητικά για πάντα. Τεράστια ποσότητα προσωπικών πληροφοριών εδράζει σε βάσεις δεδομένων σε ολόκληρο τον κόσμο. Μάλιστα, σε αρκετές περιπτώσεις η ίδια οντότητα συλλέγει ετερόκλητα προσωπικά δεδομένα τα οποία συλλέγονται από εντελώς διαφορετικές υπηρεσίες, όπως είναι το φαινόμενο της εταιρείας "google", η οποία έχει εξαγοράσει ένα μεγάλο αριθμό εταιρειών που αφορούν σε παροχή προηγμένων υπηρεσιών που συλλέγουν και αποθηκεύουν προσωπικά δεδομένα. Καθίσταται λοιπόν σαφές ότι οι δυνατότητες εξαγωγής συμπερασμάτων που αφορούν στην προσωπική ζωή μέσω συνδυασμού ακόμα και εντελώς ετερόκλητων δεδομένων καθίσταται εύκολη, ιδιαιτέρως με τη χρήση τεχνολογιών[25].

Είναι βέβαιο ότι η πρόοδος της τεχνολογίας προηγείται της νομοθεσίας. Η συμπόρευση τους είναι μείζον θέμα το οποίο απασχολεί έντονα τις αρχές. Ο νέος κανονισμός GDPR στοχεύει στην προστασία των φυσικών προσώπων και των προσωπικών τους δεδομένων και η ημερομηνία της 25.5.2018 βρίσκει την Ε.Ε. με ενιαίο νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων. Οι προσδοκίες του νέου Κανονισμού είναι μεγάλες για την αντιμετώπιση των κινδύνων, όμως η αποτελεσματικότητά του θα διαπιστωθεί κατά τη διάρκεια της εφαρμογής του. Τα τελευταία σαράντα χρόνια

[23] ΑΠΔΠΧ, Χρηματοπιστωτικά, Σημαντικά αρχεία http://www.dpa.gr/portal/page?_pageid=33,124336&_dad=portal&_schema=PORTAL
[24] Απόρρητο και το Ψηφιακό Μέλλον, 2018, http://oecdobserver.org/news/fullstory.php/aid/6040/Privacy_and_your_digital_future
[25] Ασφάλεια Πληροφοριακών Συστημάτων https://el.wikipedia.org/wiki

δημιουργήθηκε η ανάγκη για κατοχύρωση της προστασίας των προσωπικών δεδομένων και αυτό γιατί διαπιστώθηκε η ανεπάρκεια του Δικαίου προστασίας. Από το 1975 το Σύνταγμα προστάτευε την ιδιωτική οικογενειακή ζωή, όμως δεν προστάτευε το δικαίωμα του ατόμου να γνωρίζει λεπτομέρειες για την επεξεργασία των προσωπικών του δεδομένων. Είναι υποχρέωση κάθε Κράτους να παρέχει ασφάλεια στους πολίτες του σε θέματα που σχετίζονται με τα προσωπικά τους δεδομένα[26].

2.3 Κίνδυνοι

Τόσο τα μεμονωμένα άτομα, όσο και οι επιχειρήσεις, προσπαθούν να οργανώσουν τα μελλοντικά τους σχέδια, βασισμένοι σε ένα πλήθος παραγόντων, εναλλακτικών καταστάσεων και αβεβαιότητας. Ο παράγοντας που μπορεί να προκαλέσει σε δεδομένη μελλοντική περίοδο την εμφάνιση εναλλακτικών καταστάσεων και να επιφέρει αβεβαιότητα (uncertainty) καλείται κίνδυνος (risk). Σύμφωνα με τον Ελευθεριάδη (2018), ο κίνδυνος είναι μια από τις παραμέτρους της καθημερινής μας ζωής και επηρεάζει σχεδόν το σύνολο των δραστηριοτήτων των οικονομικών μονάδων, ενώ παράλληλα υπάρχει σε όλες εκείνες τις περιπτώσεις στις οποίες δεν είναι δυνατό να προβλέψουμε με βεβαιότητα το αποτέλεσμα μιας δραστηριότητας. Η κάθε επιχειρηματική δραστηριότητα θα πρέπει να προσδιορίζει ποιος είναι ο κίνδυνος που συνδέεται με την υλοποίησή της και ποια είναι τα μέτρα που πρέπει να ληφθούν για την αποτελεσματική διαχείρισή του[27].

Συνεχίζοντας, αναφέρει ότι ο κίνδυνος μπορεί να χρησιμοποιηθεί για να περιγράψει την αβεβαιότητα που συνδέεται με διαδικασίες και τα αποτελέσματά τους, που μπορεί να έχουν σημαντικές επιπτώσεις, είτε θετικές είτε αρνητικές στην: α) Λειτουργική απόδοση, β) Την επίτευξη των σκοπών και των στόχων και γ) Την εκπλήρωση των προσδοκιών των μετόχων. Ο κίνδυνος επίσης μπορεί να ορισθεί ως ο συνδυασμός της πιθανότητας ενός γεγονότος και των συνεπειών του (ISO-IEC Guide 73). Σε όλους τους τύπους των δραστηριοτήτων, υπάρχει το ενδεχόμενο για γεγονότα και συνέπειες που συνιστούν ευκαιρίες προς όφελος (upside) ή απειλές της επιτυχίας (downside). Συνεπώς, ο κίνδυνος είναι η αβεβαιότητα της μελλοντικής έκβασης ενός γεγονότος. Είναι κάτι που συμβαίνει στο μέλλον αλλά δεν μπορεί να προβλεφθεί ακριβώς σήμερα επειδή υπάρχει αβεβαιότητα. Κίνδυνος υφίσταται όταν ένα τυχαίο γεγονός θα επιδράσει αρνητικά στην πιθανότητα της πραγματοποίησης ενός εφικτού στόχου. Μαθηματικά ο κίνδυνος μπορεί να εκφρασθεί σαν το προϊόν της πιθανότητας των περιστατικών και των συνεπειών της απώλειας που

[26] Απόρρητο και το Ψηφιακό Μέλλον, 2018, http://oecdobserver.org/news/fullstory.php/aid/6040/Privacy_and_your_digital_future

[27] Ελευθεριάδης, Ι. (2018). *Διοίκηση Εταιρικών Κινδύνων*. Πανεπιστημιακές Σημειώσεις

προκλήθηκε από τον κίνδυνο. Οι καταστάσεις αβεβαιότητας προκύπτουν, όταν υπάρχει μια άγνωστη, απροσδιόριστη κατανομή πιθανότητας στο σύνολο των πιθανών εκβάσεων[28].

Η αβεβαιότητα σε αυτό το πλαίσιο έχει δύο διαστάσεις[29]:

- Το εύρος των πιθανών εκβάσεων ενός γεγονότος ή μιας δράσης το οποίο μπορεί να είναι στενό, περιορισμένο ή άγνωστο.
- Την πιθανότητα εμφάνισης μιας έκβασης. Σε μερικές περιπτώσεις αυτό είναι σχετικά εύκολο να καθοριστεί. Σε πολλές άλλες περιπτώσεις μπορεί να μην είναι δυνατό να υπολογιστεί μια πιθανότητα ακριβώς. Η ακόμη και να μην είναι δυνατό να υπολογιστεί μια πιθανότητα καθόλου.

Στην Αφρική, 19 χώρες (Αγκόλα, Μπενίν, Μπουρκίνα Φάσο, Τσαντ, Ισημερινή Γουινέα, Μάλι, Γκαμπόν, Γκάνα, Ακτή Ελεφαντοστού, Λεσόθο, Μαδαγασκάρη, Μαλάουι, Μαρόκο, Νίγηρας, Σενεγάλη, Νότιος Αφρική, Τυνησία, Ζάμπια) έχουν θεσπίσει νόμους για την ασφάλεια των πληροφοριών και την προστασία των δεδομένων. Έξι χώρες έχουν νόμους που είναι στα πρώτα στάδια (συμπεριλαμβανομένης της Κένυας, Νιγηρία, Τόγκο, Τανζανία, Ουγκάντα και τη Ζιμπάμπουε). Οι υπόλοιπες χώρες είτε δεν έχουν νομοθεσία είτε έχουν αλλά δεν υπάρχουν διαθέσιμα αρχεία. Ως ήπειρος, η Αφρικανική Ένωση συνέθεσε τη Σύμβαση της Αφρικανικής ένωσης για την ασφάλεια στον κυβερνοχώρο και την προστασία των προσωπικών δεδομένων το 2014. Μόνο δέκα χώρες (Μπενίν, Τσαντ, Κομόρες, Κονγκό, Γκάνα, Γουινέα-Μπισάου, Μαυριτανία, Σιέρα Λεόνε, Σάο Τομέ & Principe και Ζάμπια) είναι συμβαλλόμενα μέρη και μόνο δύο (Μαυρίκιος και Σενεγάλη) έχουν επικυρώσει τη σύμβαση. Σε γενικό επίπεδο, υπάρχει προσπάθεια να διασφαλίζεται η προστασία των δεδομένων σε πλαίσιο περιφερειακών συνασπισμών. Για παράδειγμα η Κοινότητα της Νότιας Αφρικής έχει αναπτύξει ένα μοντέλο δικαίου εναρμονίζοντας πολιτικές για την προστασία των αγορών στη νότια περιοχή της Σαχάρας, η οποία περιλαμβάνει στοιχεία για την προστασία δεδομένων[30].

Η οικονομική κοινότητα των Δυτικοαφρικανικών Κρατών έχει δημιουργήσει μία συμπληρωματική πράξη στην προστασία προσωπικών δεδομένων εντός αυτής. Πολλές γαλλόφωνες χώρες (Μπενίν, Μπουρκίνα Φάσο, Ακτή Ελεφαντοστού, Γκαμπόν, Μαλί,

[28] Ασφάλεια πληροφοριών και Κυβερνοέγκλημα https://lawandtech.eu/sectors/cybercrime_infosec/
[29] Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) https://pofee.gr/images/books/GDPR-pofee-april2018.pdf
[30] Ασφάλεια πληροφοριών και Κυβερνοέγκλημα https://lawandtech.eu/sectors/cybercrime_infosec/

Μαρόκο, Σενεγάλη και Τυνησία) αποτελούν μέρος της γαλλόφωνης κοινότητας προστασίας προσωπικών δεδομένων που προωθεί τις αρχές προστασίας των δεδομένων προσωπικού χαρακτήρα και κανόνων στις γαλλόφωνες χώρες. Τόσο στην Αυστραλία όσο και στη Νέα Ζηλανδία έχουν νομοθεσία γύρω από την προστασία των δεδομένων. Στην Ασία, δεκαπέντε χώρες (Μπουτάν, Κίνα, Χονγκ Κονγκ, Ινδία, Ινδονησία, Ιράν, Ισραήλ, Ιαπωνία, Νότια Κορέα, Μαλαισία, Νεπάλ, Ομάν, Φιλιππίνες, Ταϊβάν, Ηνωμένα Αραβικά Εμιράτα, Βιετνάμ, Υεμένη) διαθέτουν νομοθεσία. Τέσσερις είναι στη διαδικασία κατάρτισης (Ιράκ, Ιορδανία, Πακιστάν, Ταϊλάνδη), ενώ οι άλλες είτε δεν έχουν καμία ή δεν έχουν διαθέσιμο κανένα δεδομένο[31].

Σε περιφερειακό επίπεδο, η ήπειρος έχει πλαίσιο ιδιωτικού απορρήτου οικονομικής συνεργασίας Ασίας-Ειρηνικού, που αποσκοπεί να αναπτύξει ομοιόμορφα πρότυπα νομοθεσίας περί προστασίας δεδομένων σε όλη την περιοχή. Μόνο Κίνα, Χονγκ Κονγκ, Ινδονησία, Ιαπωνία, Κορέα, Μαλαισία, Φιλιππίνες, Σιγκαπούρη και Βιετνάμ είναι μέρος αυτού του περιφερειακού μπλοκ. Σε αντίθεση με το ΓΚΠΔ, το σύστημα περί προστασίας δεδομένων της οικονομικής συνεργασίας Ασίας-Ειρηνικού δεν εκτοπίζει ούτε αλλάζει τους εσωτερικούς νόμους και κανονισμούς μιας χώρας. Σε όλη την Βόρεια Αμερική και τη Λατινική Αμερική δεκαεπτά χώρες (Καναδάς, ΗΠΑ, Μεξικό, Νικαράγουα, Τζαμάικα, Τρινιντάντ και Τομπάγκο, Νικαράγουα, Κόστα Ρίκα, Κολομβία, Περού, Βολιβία, Χιλή, Αργεντινή, Παραγουάη, Ουρουγουάη, Μπαχάμες, Δομινικανή Δημοκρατία) διαθέτουν νομοθεσία. Τέσσερις είναι σε διαδικασία σύνταξης (Ισημερινός, Ονδούρα, Παναμάς, Βραζιλία, Τζαμάικα), ενώ οι άλλοι είτε δεν είχαν καμία νομοθεσία είτε δεν διέθεταν στοιχεία για την προστασία δεδομένων. Εκτός της ειδικής νομοθεσίας που έχουν θεσπίσει στις χώρες τους, οι ΗΠΑ και η ΕΕ έχουν συντάξει ένα πλαίσιο απορρήτου μεταξύ τους, το οποίο σχεδιάστηκε από το Υπουργείο Εμπορίου των ΗΠΑ και την Ευρωπαϊκή Επιτροπή και παρέχει στις επιχειρήσεις από τις δύο πλευρές του Ατλαντικού έναν μηχανισμό προστασίας δεδομένων κατά τη μεταφορά προσωπικών δεδομένων από την Ευρωπαϊκή Ένωση προς τις Ηνωμένες Πολιτείες συνυφασμένο με τους κανονισμούς της ΕΕ, για την υποστήριξη του διατλαντικού εμπορίου. Οι χώρες της Λατινικής Αμερικής είναι επίσης μέρος της Ιβηρο-Αμερικανικής προστασίας δεδομένων δικτύου, που αποτελείται από 22 αρχές προστασίας των δεδομένων από την Ανδόρα, Αργεντινή, Χιλή, Κολομβία, Κόστα Ρίκα, Μεξικό, Περού και Ουρουγουάη. Την τελευταία δεκαετία, ο οργανισμός έχει προωθήσει την ανάπτυξη ολοκληρωμένης προστασίας των δεδομένων και την εισαγωγή

[31] Εθνική Τράπεζα της Ελλάδος, Δήλωση προστασίας δεδομένων προσωπικού χαρακτήρα nbg-privacy_statement.pdf

αρχών προστασίας δεδομένων σε όλη την Λατινική Αμερική.[32]

Μια έρευνα καταναλωτών το 2016 διαπίστωσε ότι στη Λατινική Αμερική η ανησυχία για το πώς συλλέγονται δεδομένα ατόμων και ο φόβος για απώλεια της ιδιωτικής ζωής είναι σχετικά υψηλά σε σύγκριση με όλες τις άλλες περιοχές. Το 70% των ερωτηθέντων από τη Λατινική Αμερική και την Καραϊβική δήλωσαν ότι οι καταναλωτές πολύ σπάνια κατανοούν και έχουν τον έλεγχο του πώς τα δεδομένα τους συλλέγονται, αποθηκεύονται και χρησιμοποιούνται[33].

Οι αυξανόμενες ροές δεδομένων και πληροφοριών παράγουν περισσότερη οικονομική αξία από το παγκόσμιο εμπόριο αγαθών. Η παγκοσμιοποίηση εισέρχεται σε μία νέα φάση που ορίζεται από τις αυξανόμενες ροές δεδομένων και πληροφοριών. Πριν από 15 χρόνια οι ψηφιακές ροές ήταν ανύπαρκτες και τώρα έχουν μεγάλο αντίκτυπο στην αύξηση του ΑΕΠ. Αυτό το γεγονός δίνει τη δυνατότητα στις εταιρείες να εισχωρήσουν στις διεθνείς αγορές διαθέτοντας μικρότερο όγκο κεφαλαίου, όμως δημιουργούνται νέοι κίνδυνοι και πολιτικές προκλήσεις. Το εμπόριο περιοριζόταν κυρίως στις πολυεθνικές εταιρείες. Η νέα μορφή ψηφιακής παγκοσμιοποίησης ανοίγει το δρόμο στις μικρότερες επιχειρήσεις, στις νέες επιχειρήσεις και σε δισεκατομμύρια κόσμο. Πάρα πολλές επιχειρήσεις εξάγουν μέσω ηλεκτρονικού εμπορίου. Υπολογίζεται πως το 12% περίπου του παγκόσμιου εμπορίου αγαθών διεξάγεται μέσω του διεθνούς ηλεκτρονικού εμπορίου. Με τα σημερινά δεδομένα, μικρές νεοσύστατες επιχειρήσεις μπορούν να ανταγωνιστούν πολυεθνικές εταιρείες. Σε αυτή τη ψηφιακή εποχή οι μεγάλες εταιρείες μπορούν να διαχειρίζονται τις οικονομικές τους δραστηριότητες με πιο οικονομικό και αποτελεσματικό τρόπο. Οι ροές δεδομένων ενισχύουν την ανάπτυξη, αυξάνουν την παραγωγικότητα και δημιουργούν πιο αποδοτικές αγορές. Εκθέτουν νέες ιδέες, έρευνες, τεχνολογίες και βέλτιστες πρακτικές[34].

Η περίπτωση του Facebook και της μεγαλύτερης διαρροής προσωπικών δεδομένων

Ο βρετανικός Guardian και οι αμερικανοί New York Times έφεραν στο φως της δημοσιότητας το σκάνδαλο διαρροής προσωπικών δεδομένων χρηστών του Facebook από την εταιρεία ανάλυσης δεδομένων Cambridge Analytica, η οποία χρησιμοποίησε τα στοιχεία αυτά κατά τη διάρκεια της προεκλογικής καμπάνιας του Ντόναλντ Τραμπ,

[32] Ένας χρόνος εφαρμογής του GDPR. Τι έγινε, τι θα γίνει, τι πρέπει να γίνει, 2019 http://www.epixeiro.gr/article/126595
[33] Ένα έτος GDPR – Απογραφή https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en
[34] Ψηφιακή Παγκοσμιοποίηση: Η νέα εποχή των παγκόσμιων ροών, 2016

σημερινού προέδρου των ΗΠΑ. Τα προσωπικά δεδομένα τουλάχιστον 50 εκατομμύριων χρηστών διέρρευσαν. Το σκάνδαλο αυτό δημιουργεί ερωτήματα σχετικά με τη χρήση και την ασφάλεια της πιο δημοφιλής πλατφόρμας κοινωνικής δικτύωσης. Η Cambridge Analytica συγκέντρωσε πληροφορίες από το προφίλ 50 εκατομμυρίων Αμερικανών ψηφοφόρων. Με τα δεδομένα αυτά δημιούργησε ένα ισχυρό πρόγραμμα λογισμικού για την πρόβλεψη και επιρροή των ψηφοφόρων, με μεγάλο αντίκτυπο στις τελευταίες αμερικανικές εκλογές του 2016. (Τι συνέβη με το Facebook και τη μεγαλύτερη διαρροή προσωπικών δεδομένων, 2018) Η υπόθεση του Facebook αποκαλύπτει πως τα δεδομένα ενός ατόμου μπορούν με αόρατους τρόπους να ανταλλάσσονται μέσα στο Διαδίκτυο χωρίς τη γνώση ή την άδειά του. Είναι αξιοσημείωτο πως μετά από τρία χρόνια έγινε γνωστή η υπόθεσή του και αναζωπύρωσε θέματα σχετικά με την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων, καθώς και το ερώτημα πόσο αξιόπιστος είναι ο ψηφιακός μας κόσμος[35].

Σύμφωνα με το Guardian το 2014, ένας ακαδημαϊκός Ρώσσος από το πανεπιστήμιο του Cambridge, δημιούργησε μία εφαρμογή για το Facebook στην οποία καλούνταν να απαντήσουν πολλές χιλιάδες χρήστες σε ένα τεστ προσωπικότητας για ακαδημαϊκούς λόγους. Έτσι καταφέρνοντας να πείσει 270.000 χιλιάδες χρήστες να απαντήσουν στο τεστ, κατάφερε να συγκεντρώσει πληροφορίες και για τους φίλους τους. Έφτασε να έχει πρόσβαση στο προφίλ και στα προσωπικά δεδομένα 50 εκατομμυρίων χρηστών. Αυτά τα δεδομένα τα πούλησε ο Ρώσσος ακαδημαϊκός στην Cambridge Analytica, γεγονός που κατά τη Facebook αποτέλεσε παραβίαση των όρων χρήσης, καθώς δεν επιτρεπόταν στην εφαρμογή να χρησιμοποιήσει τα στοιχεία για εμπορικούς σκοπούς. Σύμφωνα με πρώην υπάλληλο της Cambridge Analytica είχαν ληφθεί προσωπικά δεδομένα χωρίς εξουσιοδότηση, ώστε να δημιουργηθεί ένα σύστημα το οποίο θα μπορούσε να φτιάξει το προφίλ μεμονωμένων ψηφοφόρων. Στόχος τους ήταν οι εξατομικευμένες πολιτικές διαφημίσεις[36].

Η εταιρεία Facebook σε ανακοίνωσή της δηλώνει: «Συνολικά, πιστεύουμε ότι οι προσωπικές πληροφορίες έως και 87 εκατομμυρίων χρηστών, οι περισσότεροι εκ των οποίων βρίσκονται στις ΗΠΑ, αποκτήθηκαν αθέμιτα από την Cambridge Analytica». Η εταιρεία κλήθηκε από τις παγκόσμιες αρχές να απολογηθεί για το σκάνδαλο. Κατανοεί τη σοβαρότητα του ζητήματος και ο πρόεδρος της Ζούκερμπεργκ αναλαμβάνει την ευθύνη

[35] Απόρρητο και το Ψηφιακό Μέλλον, 2018
[36] Ενημέρωση των πελατών της Attica Bank για την επεξεργασία των προσωπικών τους δεδομένων σύμφωνα με τον Κανονισμό (ΕΕ) 2016/679 και τη συναφή Ελληνική Νομοθεσία GDPR_ATTICA-BANK_gr.pdf

για την αθέμιτη πρόσβαση στα προσωπικά δεδομένα των χρηστών[37].

Μετά το περιστατικό αυτό, ο πρόεδρος της Facebook παρουσίασε τα σχέδια της εταιρείας για αυστηροποίηση της πολιτικής προστασίας των προσωπικών δεδομένων των χρηστών και μεγαλύτερη διαφάνεια αναφορικά με τους διαφημιζόμενους σε αυτό. Στο Αμερικανικό Κογκρέσο είπε ο Ζούκερμπεργκ: «Νομίζω το GDPR γενικώς θα είναι πολύ θετικό βήμα για το ιντερνέτ»[38].

Το Facebook και έχει αρχίσει να ενημερώνει τους Ευρωπαίους χρήστες του για τροποποιήσεις στους όρους χρήσης, ώστε να συμμορφωθεί προς την ευρωπαϊκή νομοθεσία. Όπως όλα τα κοινωνικά μέσα δικτύωσης σπεύδει να επικαιροποιήσει τις πολιτικές απορρήτου και οφείλει να λάβει τη συγκατάθεση των χρηστών του για τα προσωπικά τους δεδομένα.

Σύμφωνα με την επίσημη ηλεκτρονική σελίδα της Facebook, η εταιρεία δεσμεύεται και δηλώνει πως συμμορφώνεται με την τρέχουσα νομοθεσία περί προστασίας δεδομένων της Ε.Ε, τη GDPR. Η εταιρεία αναλαμβάνει δεσμεύσεις για διαφάνεια, έλεγχο και λογοδοσία. Η πολιτική δεδομένων του Facebook θα καθορίζει με ποιον τρόπο θα επεξεργάζονται τα προσωπικά δεδομένα των χρηστών, θα παρέχει στους χρήστες δυνατότητα ελέγχου και τρόπου χρήσης των δεδομένων τους και θα τους υπενθυμίζει τη διαχείριση για το απόρρητο[39].

Τον Ιανουάριο του 2019, η Γαλλική εποπτική αρχή προστασίας δεδομένων επέβαλλε πρόστιμο στη Google των πενήντα εκατομυρίων ευρώ, για παραβίαση του GDPR. Η αρχή της Γαλλίας διαπίστωσε ότι στους χρήστες Android, δεν εξηγούσε η Google με σαφήνεια τι πληροφορίες συλλέγει και για ποιους σκοπούς και δεν λάμβανε τη συγκατάθεση των χρηστών για κάθε περίπτωση. Το πόρισμα εναντίον της Google είναι η έλλειψη διαφάνειας, ανεπαρκής πληροφόρηση και έλλειψη έγκυρης συναίνεσης όσον αφορά στην εξατομίκευση των διαφημίσεων. Η εταιρεία βρίσκεται υπό έρευνα και από τις ιρλανδικές Αρχές. Άλλο μεγάλο πρόστιμο ύψους 400.000 ευρώ επιβλήθηκε από τις πορτογαλικές Αρχές σε νοσοκομείο του οποίου το προσωπικό χρησιμοποιούσε ψευδείς λογαριασμούς

[37] Ενημέρωση των πελατών της Attica Bank για την επεξεργασία των προσωπικών τους δεδομένων σύμφωνα με τον Κανονισμό (ΕΕ) 2016/679 και τη συναφή Ελληνική Νομοθεσία GDPR_ATTICA-BANK_gr.pdf
[38] Ένας χρόνος εφαρμογής του GDPR. Τι έγινε, τι θα γίνει, τι πρέπει να γίνει, 2019 http://www.epixeiro.gr/article/126595
[39] Ένας χρόνος εφαρμογής του GDPR. Τι έγινε, τι θα γίνει, τι πρέπει να γίνει, 2019 http://www.epixeiro.gr/article/126595

για να αποκτήσει πρόσβαση στα δεδομένα ασθενών. Από τις πολωνικές Αρχές επιβλήθηκε πρόστιμο ύψους 220.000 ευρώ σε εταιρεία που συνέλεγε προσωπικά δεδομένα μέσω του διαδικτύου για διαφημιστικούς λόγους[40].

2.4 Ανάγκη θέσπισης του νομοθετικού πλαισίου προστασίας προσωπικών δεδομένων

Η πρώτη πραγματεία αναφορικά με το γεγονός ότι η ιδιωτική ζωή των πολιτών τίθεται σε κίνδυνο από την τεχνολογική πρόοδο δημοσιεύτηκε ήδη το 19ο αιώνα, όταν δύο νομικοί στην πολιτεία της Βοστόνης των Ηνωμένων Πολιτειών επισήμαναν τον κίνδυνο για την ιδιωτική ζωή που εγκυμονούσε η σχετικά νέα τότε τεχνολογία της λήψης φωτογραφιών. Τα Ηνωμένα Έθνη αναγνώρισαν την ιδιωτικότητα σαν ένα από τα θεμελιώδη δικαιώματα του ανθρώπου, με το Άρθρο 12 της Οικουμενικής Διακήρυξης για τα Ανθρώπινα Δικαιώματα. Το ενδιαφέρον για την προστασία των προσωπικών δεδομένων αυξήθηκε ιδιαίτερα τις δεκαετίες του 1960 και 1970, με την έλευση των τεχνολογιών της πληροφορίας και τις προφανείς δυνατότητες παρακολούθησης και αρχειοθέτησης που αυτές έφερναν. Το 1970, υιοθετήθηκε ο πρώτος σύγχρονος νόμος προστασίας προσωπικών δεδομένων από το Hesse, ένα από τα ”κρατίδια” (Länder) της πρώην Δυτικής Γερμανίας[41].

Ο νόμος αυτός αποτέλεσε τη βάση για άλλες περιοχές της Δυτικής Γερμανίας, την ομοσπονδιακή της κυβέρνηση αλλά και χώρες πέρα από τη Γερμανία, όπως τη Σουηδία που το 1973 υιοθέτησε τον πρώτο παγκοσμίως εθνικό νόμο προστασίας προσωπικών δεδομένων. Αρκετές Ευρωπαϊκές χώρες υιοθέτησαν παρόμοιους νόμους πριν από το τέλος της δεκαετίας του 1970. Στις Ηνωμένες Πολιτείες της Αμερικής, το Κογκρέσο υιοθέτησε το “Νόμο περί Ιδιωτικότητας” (Privacy Act) το 1974, εκτιμώντας ότι τα πολύπλοκα υπολογιστικά συστήματα δημιουργούσαν απειλές για την προσωπική ιδιωτικότητα. Ο νόμος αυτός δέχτηκε αρκετές τροποποιήσεις μέχρι σήμερα με σημαντικότερες εκείνη του 1988, η οποία λάμβανε υπόψη τις τεχνολογικές εξελίξεις στο χώρο της πληροφορικής, καθώς και εκείνη του 2001, στο πλαίσιο του “Πατριωτικού Νόμου” (Patriot Act), ο οποίος ενεργοποιεί τη δυνατότητα για αυξημένη παρακολούθηση προσώπων υπερβαίνοντας κατά πολύ τις μέχρι τότε επιτρεπόμενες εισβολές στην προσωπική ιδιωτικότητα. Στο πλαίσιο

[40] Έντυπο ενημέρωσης για την επεξεργασία προσωπικών δεδομένων σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 και τη σχετική Ελληνική Νομοθεσία gdpr_A.indd=EUROBANK

[41] ΕΕΔΑ, Κατάλογος Διεθνών και Ευρωπαϊκών Συμβάσεων για τα Δικαιώματα του Ανθρώπου http://www.antigone.gr/files/gr/library/educationalmaterial/katalogos%20diethnon%20kai%20evropaikon%20symvaseon.pdf

αυτό ορίζονται ενδυναμωμένες διαδικασίες παρακολούθησης και γίνονται πιο χαλαροί οι κανόνες για την άρση του απορρήτου των τηλεπικοινωνιών και τη συλλογή προσωπικών δεδομένων. Στις αρχές της δεκαετίας του 1980, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (Organisation for Economic Co-operation and Development –OECD), στον οποίο συμμετέχει και η Ελλάδα, εξέδωσε τις Κατευθυντήριες Οδηγίες για την Προστασία της Ιδιωτικότητας και τη Διασυνοριακή Ροή των Προσωπικών Δεδομένων (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), οι οποίες αποτέλεσαν ορόσημο αναφορικά με την προστασία των προσωπικών δεδομένων[42].

Οι κατευθυντήριες αυτές οδηγίες είχαν σαν σκοπό να βοηθήσουν στον εναρμονισμό των εθνικών νομοθεσιών των κρατών – μελών του Οργανισμού γύρω από μία κοινή βάση για την προστασία των προσωπικών δεδομένων. Παρόλο που οι κατευθυντήριες οδηγίες είχαν στη φύση τους συμβουλευτικό και όχι νομοθετικό χαρακτήρα, επέδρασαν σε πολύ μεγάλο βαθμό στη σχετική νομοθεσία που ακολούθησε σε παγκόσμιο επίπεδο, ενώ οι βασικές αρχές για την προστασία των προσωπικών δεδομένων που όρισαν αποτέλεσαν τη βάση των σύγχρονων νομοθετικών και κανονιστικών πλαισίων και παραμένουν διαχρονικές. Τον Ιούλιο του 1990, η Ευρωπαϊκή Κοινότητα εξέδωσε την πρώτη πρόχειρη πρόταση για μία οδηγία περί της προστασίας των προσωπικών δεδομένων. Μετά από χρόνια διαβουλεύσεων, η τελική Οδηγία 95/46/ΕΚ "για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη διακίνηση των δεδομένων αυτών" υιοθετήθηκε από το Ευρωπαϊκό Συμβούλιο το 1995 και τέθηκε σε εφαρμογή στα κράτη – μέλη από τον Οκτώβρη του 1998[43].

Η Οδηγία αυτή αποτέλεσε ορόσημο και αποτέλεσε τη βάση για τη νομοθεσία όχι μόνο των κρατών – μελών της Ευρωπαϊκής Κοινότητας αλλά σε παγκόσμιο επίπεδο, αποτελώντας σήμερα το πιο επιδραστικό νομικό κείμενο περί της προστασίας των προσωπικών δεδομένων στον πλανήτη. Το Δεκέμβριο του 1997, η Ευρωπαϊκή Κοινότητα εξέδωσε την Οδηγία 97/66/ΕΚ, περί της "επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα", με σκοπό τη διασφάλιση του απορρήτου των τηλεπικοινωνιών των πολιτών Η Οδηγία αυτή ουσιαστικά εξειδίκευσε και συμπλήρωσε την Οδηγία 95/46/ΕΚ σε ότι αφορά τον τηλεπικοινωνιακό τομέα και γρήγορα αντικαταστάθηκε από την Οδηγία 2002/58/ΕΚ καθώς δεν ήταν σε θέση να διευθετήσει ζητήματα που αφορούσαν τις τελευταίες τεχνολογικές εξελίξεις. Η Οδηγία

[42] Ασφάλεια Πληροφοριακών Συστημάτων https://el.wikipedia.org/wiki
[43] Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) https://pofee.gr/images/books/GDPR-pofee-april2018.pdf

2002/58/ΕΚ καλύπτει όλο το φάσμα των ηλεκτρονικών επικοινωνιακών και των υπηρεσιών που παρέχονται μέσω αυτών. Πολύ πρόσφατα εκδόθηκε μία νέα Οδηγία, η Οδηγία 2006/24/ΕΚ, η οποία τροποποιεί την Οδηγία 2002/58/ΕΚ σε ότι αφορά τη διατήρηση ορισμένων δεδομένων που παράγονται ή υφίστανται επεξεργασία από παρόχους δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, ώστε να διασφαλιστεί ότι τα δεδομένα καθίστανται διαθέσιμα για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων[44].

Από τον 18ο αιώνα συντάχθηκαν τα κείμενα που περιελάμβαναν τα δικαιώματα του ιδιωτικού βίου. Αυτό το δικαίωμα αναγνωρίζεται το 1948 από τον ΟΗΕ και την Οικουμενική Διακήρυξη Δικαιωμάτων του Ανθρώπου και το 1950 από την Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου. Η Οικουμενική Διακήρυξη Δικαιωμάτων του Ανθρώπου συντάχθηκε μετά τη λήξη του Β΄ Παγκοσμίου Πολέμου και τη δημιουργία των Ηνωμένων Εθνών. Οι ηγέτες του κόσμου αποφάσισαν να συντάξουν μία λίστα με τα ανθρώπινα δικαιώματα. Επισήμαναν τη σημασία τα ανθρώπινα δικαιώματα να προστατεύονται υπό ένα καθεστώς δικαίου. Μέσα σε αυτή τη λίστα περιλαμβάνονταν η πίστη στην ανθρώπινη αξιοπρέπεια και προσωπικότητα, το δικαίωμα του κάθε ανθρώπου στη ζωή, την ελευθερία και την προσωπική ασφάλεια. Όπως επίσης ότι όλοι οι άνθρωποι είναι ίσοι απέναντι στο νόμο και έχουν δικαίωμα στην προστασία του νόμου, χωρίς καμία απολύτως διάκριση. Και σύμφωνα με το Άρθρο 12, κανείς δεν επιτρέπεται να υποστεί.αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, ούτε προσβολές της τιμής και της υπόληψης του. (Διεθνής Αμνηστία, Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου) Η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου υιοθετήθηκε το 1950 από το Συμβούλιο της Ευρώπης για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών. Βάσει της σύμβασης ιδρύθηκε και το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων[45].

Όλα τα κράτη-μέλη και εθνικά δικαστήρια είναι υποχρεωμένα να εφαρμόζουν τη Σύμβαση και να εγγυώνται τα θεμελιώδη δικαιώματα, όχι μόνο στους υπηκόους τους, αλλά και σε κάθε άτομο της δικαιοδοσίας τους. Στην πορεία των χρόνων η Σύμβαση εξελίσσεται και γίνονται προσθήκες περισσότερων δικαιωμάτων στο αρχικό της κείμενο. Αυτές οι προσθήκες κειμένων ονομάζονται Πρωτόκολλα. Μέχρι σήμερα έχουν προστεθεί

[44] Ενημέρωση των πελατών της Attica Bank για την επεξεργασία των προσωπικών τους δεδομένων σύμφωνα με τον Κανονισμό (ΕΕ) 2016/679 και τη συναφή Ελληνική Νομοθεσία GDPR_ATTICA-BANK_gr.pdf
[45] Ενημέρωση των πελατών της Attica Bank για την επεξεργασία των προσωπικών τους δεδομένων σύμφωνα με τον Κανονισμό (ΕΕ) 2016/679 και τη συναφή Ελληνική Νομοθεσία GDPR_ATTICA-BANK_gr.pdf

και τεθεί σε ισχύ 14 νέα Πρωτόκολλα. Με αυτόν τον τρόπο διευρύνονται τα προστατευόμενα δικαιώματα και συμβαδίζουν με τις απαιτήσεις της εποχής και την εξέλιξη της τεχνολογίας. Η Οικουμενική Διακήρυξη Δικαιωμάτων του Ανθρώπου και η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου αποτελούν πρόδρομο του νέου ΓΚΠΔ-GDPR[46].

Το δικαίωμα στην προστασία των προσωπικών δεδομένων ως συνέχεια του δικαιώματος ιδιωτικού βίου, κάνει την εμφάνισή του τη δεκαετία του 1970. Εμφανίζεται τόσο στη Νομοθεσία της Ευρώπης όσο και στη Νομοθεσία των Ηνωμένων Πολιτειών της Αμερικής. Το πρώτο Πρωτόκολλο προστέθηκε στην Ευρωπαϊκή Σύμβαση για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών το 1952 και το τελευταίο το 2004. Υπάρχουν άλλα δύο πρόσθετα Πρωτόκολλα το 2013, τα οποία όμως δεν έχουν τεθεί ακόμη σε ισχύ[47].

Τον Ιανουάριο του 1981 υπογράφηκε η Ευρωπαϊκή Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα. Τέθηκε σε ισχύ τον Οκτώβριο του 1985 και υπογράφτηκε από την Ελλάδα το 1983. Η επικύρωσή του από την Ελλάδα έγινε με το Νόμο 2068/1992. Η σύμβαση αυτή είναι διεθνώς η πρώτη που προστατεύει το άτομο από παραβιάσεις που ενδέχεται να συνοδεύουν τη συλλογή και επεξεργασία προσωπικών του δεδομένων. Επίσης ρυθμίζει τη διασυνοριακή ροή πληροφοριών προσωπικού χαρακτήρα. Παρέχει εγγυήσεις σε ότι αφορά τη συλλογή και επεξεργασία δεδομένων και κάνει πρώτη φορά αναφορά στα «ευαίσθητα» προσωπικά δεδομένα. Απαγορεύει δηλαδή την επεξεργασία και συλλογή δεδομένων σχετικά με την υγεία, θρησκεία, φυλή, σεξουαλική ζωή και άλλα πολλά «ευαίσθητα» δεδομένα, χωρίς την κάλυψη κατάλληλων νομικών διασφαλίσεων. Η Σύμβαση κατοχυρώνει το δικαίωμα του ατόμου να γνωρίζει την επεξεργασία πληροφοριών που το αφορούν και να ζητά ενδεχομένως τη διόρθωσή τους. Όταν βέβαια διακυβεύονται συμφέροντα κρατικής ασφάλειας περιορίζονται τα παραπάνω δικαιώματα και όπου δεν παρέχεται ισοδύναμη νομική προστασία υπάρχει επίσης περιορισμός στη διασυνοριακή ροή προσωπικών δεδομένων[48].

Τον Οκτώβριο του 1995 εκδόθηκε η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και

[46] Ulsch, M. (2014), "Cyber Threat! How to manage the growing risk of cyber attacks", Published by John Wiley & Sons, Ltd.
[47] ΕΕΔΑ, Κατάλογος Διεθνών και Ευρωπαϊκών Συμβάσεων για τα Δικαιώματα του Ανθρώπου, 2018
[48] ΕΕΔΑ, Κατάλογος Διεθνών και Ευρωπαϊκών Συμβάσεων για τα Δικαιώματα του Ανθρώπου, 2018

Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Με την Οδηγία αυτή εισήχθη στην Ευρώπη ένα πλήρες νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων, με στόχο την προστασία θεμελιωδών ελευθεριών και δικαιωμάτων των φυσικών προσώπων και κυρίως της ιδιωτικής ζωής, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Η Οδηγία 95/46/ΕΚ επικυρώθηκε από την Ελλάδα με το Νόμο 2472/1997. (ΕΕΔΑ, Κατάλογος Διεθνών και Ευρωπαϊκών Συμβάσεων για τα Δικαιώματα του Ανθρώπου, 2018). Το 2000 συντάσσεται ο Χάρτης Θεμελιωδών Δικαιωμάτων της Ε.Ε. Η Ένωση για να ενισχύσει την προστασία των θεμελιωδών δικαιωμάτων, υπό τη συνεχή εξέλιξη της τεχνολογίας και της κοινωνίας, αποτυπώνει τα δικαιώματα αυτά σε ένα Χάρτη. Έτσι η Ε.Ε. κατορθώνει να καθιερώσει ένα χώρο δικαιοσύνης, ελευθερίας και ασφάλειας για τους ανθρώπους της[49].

Το Νοέμβριο του 2001 πραγματοποιήθηκε πρόσθετο Πρωτόκολλο στην Ευρωπαϊκή Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα. Υπογράφτηκε από την Ελλάδα το 2001 και τέθηκε σε ισχύ τον Ιούλιο του 2004. Το νέο Πρωτόκολλο προβλέπει τη σύσταση εθνικών εποπτικών αρχών που είναι υπεύθυνες για τη συμμόρφωση με τους κανονισμούς περί προστασίας δεδομένων προσωπικού χαρακτήρα και για τις διασυνοριακές ροές πληροφοριών προσωπικών δεδομένων. Η ροή πληροφοριών προς τρίτες χώρες γίνεται μόνο εάν ο αποδέκτης παρέχει επαρκές επίπεδο[50].

2.5 Το νομοθετικό πλαίσιο

Όπως έχει αναφερθεί και ανωτέρω, ο Γενικός Κανονισμός Προστασίας Δεδομένων θεσπίζει τους κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα. Βασικό στόχος του κανονισμού είναι η προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων και ειδικότερα του δικαιώματός τους στην προστασία των δεδομένων προσωπικού χαρακτήρα. Στο άρθρο 1 του Κανονισμού 2016/679, αναφέρεται χαρακτηριστικά ότι η ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα εντός της Ευρωπαϊκής Ένωσης δεν περιορίζεται ούτε απαγορεύεται για λόγους που σχετίζονται με την προστασία των φυσικών

[49] Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης
[50] Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα[51].

Στο άρθρο 2 προσδιορίζεται ότι ο Κανονισμός εφαρμόζεται στην, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης. Η παραπάνω φράση συμπληρώνεται από τις αναφορές στο τρίτο άρθρο του σχετικού κανονισμού στο οποίο αναφέρεται ότι το πεδίο εφαρμογής του εμπίπτει στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ευρωπαϊκή Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ευρωπαϊκής Ένωσης. Επιπλέον, ο κανονισμός εφαρμόζεται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην Ευρωπαϊκή Ένωση, αλλά σε τόπο όπου εφαρμόζεται το δίκαιο κράτους μέλους δυνάμει του δημόσιου διεθνούς δικαίου. Ο κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων που βρίσκονται στην Ευρωπαϊκή Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ευρωπαϊκή Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με[52]:

- Την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ευρωπαϊκή Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή
- Την παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ευρωπαϊκής Ένωσης.

Στο άρθρο 5 του κανονισμού παρατίθενται οι αρχές που διέπουν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Βάσει αυτού, τα δεδομένα προσωπικού χαρακτήρα:

- Υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»).
- Συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς

[51] Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης
[52] Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς. («περιορισμός του σκοπού»).

- Είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»).
- Είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται. Πρέπει επίσης να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας («ακρίβεια»).
- Διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της περιόδου αποθήκευσης»).
- Υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»).
- Τέλος, ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τα όσα προβλέπονται στον σχετικό κανονισμό («λογοδοσία»).

Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις, σύμφωνα με το άρθρο 6 του κανονισμού:[53]

- Το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς.
- Η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης.
- Η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του

[53] ΕΕΔΑ, Κατάλογος Διεθνών και Ευρωπαϊκών Συμβάσεων για τα Δικαιώματα του Ανθρώπου, 2018

υπευθύνου επεξεργασίας.

- Η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.
- Η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.
- Η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Μεταξύ των σημαντικότερων προϋποθέσεων για την συγκατάθεση του υποκείμενου των δεδομένων του δικαιώματος χρήσης και επεξεργασίας των προσωπικών του δεδομένων, το άρθρο 7 του κανονισμού αναφέρει ότι, όταν η επεξεργασία βασίζεται σε συγκατάθεση, ο υπεύθυνος επεξεργασίας είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε για την επεξεργασία των δεδομένων του προσωπικού χαρακτήρα. Εάν η συγκατάθεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα, το αίτημα για συγκατάθεση υποβάλλεται κατά τρόπο ώστε να είναι σαφώς διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση[54].

Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της. Πριν την παροχή της συγκατάθεσης, το υποκείμενο των δεδομένων ενημερώνεται σχετικά. Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της. Επιπροσθέτως, κατά την εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης[55].

Στο άρθρο 12, περί της διαφανούς ενημέρωσης, ανακοίνωσης και των ρυθμίσεων για την

[54] ΕΕΔΑ, Κατάλογος Διεθνών και Ευρωπαϊκών Συμβάσεων για τα Δικαιώματα του Ανθρώπου, 2018
[55] ΕΕΔΑ, Κατάλογος Διεθνών και Ευρωπαϊκών Συμβάσεων για τα Δικαιώματα του Ανθρώπου, 2018

άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων, επεξηγείται περαιτέρω ότι ο υπεύθυνος επεξεργασίας των προσωπικών δεδομένων λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία σχετικά με την επεξεργασία των δεδομένων του, σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη ειδικά σε παιδιά. Οι πληροφορίες παρέχονται γραπτώς ή με άλλα μέσα, μεταξύ άλλων, εφόσον ενδείκνυται, ηλεκτρονικώς. Όταν ζητείται από το υποκείμενο των δεδομένων, οι πληροφορίες μπορούν να δίνονται προφορικά, υπό την προϋπόθεση ότι η ταυτότητα του υποκειμένου των δεδομένων είναι αποδεδειγμένη με άλλα μέσα[56].

Στα άρθρα 13 και 14 του κανονισμού προσδιορίζονται οι πληροφορίες που θα πρέπει να παρέχονται προς το υποκείμενο των δεδομένων, είτε εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων (άρθρο 13), είτε εάν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων (άρθρο 14). Βάσει των όσων αναφέρονται, ο υπεύθυνος επεξεργασίας, κατά τη λήψη των δεδομένων προσωπικού χαρακτήρα, παρέχει στο υποκείμενο των δεδομένων όλες τις ακόλουθες πληροφορίες[57]:

- Την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας.
- Τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, κατά περίπτωση.
- Τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία.
- Τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο.
- Τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, εάν υπάρχουν.
- Κατά περίπτωση, την πρόθεση του υπευθύνου επεξεργασίας να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό και την ύπαρξη ή την απουσία απόφασης επάρκειας της Επιτροπής.

Εκτός από τις ανωτέρω πληροφορίες, ο υπεύθυνος επεξεργασίας, κατά τη λήψη των δεδομένων προσωπικού χαρακτήρα, παρέχει στο υποκείμενο των δεδομένων τις εξής επιπλέον πληροφορίες που είναι αναγκαίες για την εξασφάλιση θεμιτής και διαφανούς

[56] ΕΕΔΑ, Κατάλογος Διεθνών και Ευρωπαϊκών Συμβάσεων για τα Δικαιώματα του Ανθρώπου, 2018
[57] ΕΕΔΑ, Κατάλογος Διεθνών και Ευρωπαϊκών Συμβάσεων για τα Δικαιώματα του Ανθρώπου, 2018

επεξεργασίας[58]:

- Το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα.
- Την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορούν το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην επεξεργασία, καθώς και δικαιώματος στη φορητότητα των δεδομένων.
- Την ύπαρξη του δικαιώματος να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε, χωρίς να θιγεί η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της.
- Το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή.
- Κατά πόσο η παροχή δεδομένων προσωπικού χαρακτήρα αποτελεί νομική ή συμβατική υποχρέωση ή απαίτηση για τη σύναψη σύμβασης, καθώς και κατά πόσο το υποκείμενο των δεδομένων υποχρεούται να παρέχει τα δεδομένα προσωπικού χαρακτήρα και ποιες ενδεχόμενες συνέπειες θα είχε η μη παροχή των δεδομένων αυτών.
- Την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ και σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

Στο άρθρο 16 αναφέρεται ότι το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης[59].

Όσον αφορά την διαγραφή των προσωπικών δεδομένων, στο άρθρο 17 αναφέρεται ότι το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη

[58] Ανακοινώσεις Τραπεζών Μελών https://www.hba.gr/Media/Details/358
[59] Ανακοινώσεις Τραπεζών Μελών https://www.hba.gr/Media/Details/358

καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους ακόλουθους λόγους[60]:

A. Τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.
B. Το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία και δεν υπάρχει άλλη νομική βάση για την επεξεργασία.
C. Το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία ή το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία.
D. Τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα. E
. Τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους, στην οποία υπόκειται ο υπεύθυνος επεξεργασίας.
F. Τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών.

Σχετικά με το δικαίωμα εναντίωσης περί της χρήσης και επεξεργασίας των προσωπικών δεδομένων, το άρθρο 21 αναφέρει ότι το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, περιλαμβανομένης της κατάρτισης προφίλ. Ο υπεύθυνος επεξεργασίας δεν υποβάλλει πλέον τα δεδομένα προσωπικού χαρακτήρα σε επεξεργασία, εκτός εάν ο υπεύθυνος επεξεργασίας καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων. Εάν δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, το υποκείμενο των δεδομένων δικαιούται να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν για την εν λόγω εμπορική προώθηση, περιλαμβανομένης της κατάρτισης προφίλ, εάν σχετίζεται με αυτήν την απευθείας εμπορική προώθηση. Επιπλέον, όταν τα υποκείμενα των δεδομένων αντιτίθενται στην επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, τα δεδομένα προσωπικού χαρακτήρα δεν υποβάλλονται πλέον σε επεξεργασία για τους σκοπούς αυτούς.

[60] Ανακοινώσεις Τραπεζών Μελών https://www.hba.gr/Media/Details/358

Αναφορικά με το δικαίωμα του περιορισμού της επεξεργασίας των προσωπικών δεδομένων, στο άρθρο 18 προσδιορίζεται ότι το υποκείμενο των δεδομένων δικαιούται να εξασφαλίζει από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας, όταν ισχύει ένα από τα ακόλουθα[61]:

- Η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται από το υποκείμενο των δεδομένων, για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να επαληθεύσει την ακρίβεια των δεδομένων προσωπικού χαρακτήρα.
- Η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους.
- Ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων.
- Το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία σύμφωνα με το άρθρο 21 του κανονισμού, παράγραφος 1, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερισχύουν έναντι των λόγων του υποκειμένου των δεδομένων.

[61] Ανακοινώσεις Τραπεζών Μελών https://www.hba.gr/Media/Details/358

Κεφάλαιο 3. Οντολογίες Νομοθετικού περιεχομένου

3.1 Καταγραφή οντολογιών που έχουν νομοθετικό περιεχόμενο

Στο σημείο αυτό θα αναφέρουμε κάποιες ήδη υπάρχουσες οντολογίες που προσεγγίζουν το πρόβλημα της ιδιωτικότητας σε περιβάλλοντα διάχυτου υπολογισμού, καθώς επίσης και οντολογίες σχετικές με την προστασία της ιδιωτικότητας και αφορούν ζητήματα ασφάλειας (security) και εμπιστοσύνης (trust). Πριν περιγράψουμε τις παραπάνω οντολογίες, είναι σημαντικό να δώσουμε τον ορισμό της έννοιας της πολιτικής (policy) καθώς η έννοια αυτή παίζει σημαντικό ρόλο στην προστασία των πόρων ενός συστήματος διάχυτου υπολογισμού. Η πολιτική είναι μια τεχνική που προκύπτει για τον έλεγχο και τη ρύθμιση της συμπεριφοράς χαμηλού επιπέδου του συστήματος καθορίζοντας υψηλού επιπέδου κανόνες του συστήματος. Η χρήση της πολιτικής είναι συνηθισμένη σε υπολογιστικά συστήματα που έχουν σαν γνώρισμα την ασφάλεια ή την προστασία της ιδιωτικότητας. Οι γλώσσες καθορισμού μιας πολιτικής, οι οποίες αναπαριστώνται μέσω των γλωσσών του σημασιολογικού ιστού (π.χ. RDFS, DAML+OIL και OWL) ορίζονται συνήθως σε όρους οντολογιών. Σε ένα περιβάλλον διάχυτου υπολογισμού, οι πολιτικές ορίζονται από τους χρήστες για να επιτρέψουν ή να απαγορεύσουν σε υπολογιστικές οντότητες να εκτελέσουν διαφορετικούς τύπους πράξεων. Έχουμε λοιπόν τις εξής οντολογίες που σχετίζονται με την ιδιωτικότητα:[62]

3.1.1 KAoS Policy Ontology

Η KAoS είναι από τις πρώτες προσπάθειες για την αναπαράσταση μιας πολιτικής χρησιμοποιώντας την γλώσσα OWL. Ξεκίνησε από τα μέσα της δεκαετίας του ’90 σαν ένα σύνολο υπηρεσιών ανεξαρτήτως πλατφόρμας (platform-independent) που επιτρέπει στους ανθρώπους να ορίσουν πολιτικές που εξασφαλίζουν επαρκή προβλεψιμότητα και ελεγξιμότητα τόσο σε συστήματα πρακτόρων όσο και σε κλασσικά κατανεμημένα συστήματα. Οι υπηρεσίες και τα εργαλεία που προσφέρει η KAoS, επιτρέπουν τον προσδιορισμό, τη διαχείριση και την επίλυση αντιθέσεων, και την εκτέλεση των πολιτικών στα ειδικά πλαίσια που καθορίζονται από το πεδίο της οντολογίας. Χρησιμοποιεί έννοιες

[62] Tikkinen-Piri, C., Rohunen, A. and Markulla, J. (2018), “EU General Data Protection Regulation: Changes and implications for personal data collecting companies”, Computer Law & Security Review, 34 (1), pp. 134-153

(concepts) οντολογιών (κωδικοποιημένες σε OWL) για να χτίσει πολιτικές. Η τωρινή έκδοση του πυρήνα των οντολογιών της KAoS ορίζει βασικές έννοιες για τους δράστες (actors), τις ενέργειες (actions), ομάδες (groups), τοποθεσίες, διάφορες οντότητες που σχετίζονται με τις δράσεις. Περιλαμβάνει περισσότερες από 100 κλάσεις και 60 ιδιότητες. Η οντολογία actor περιέχει κλάσεις για ανθρώπους και μέρη λογισμικού τα οποία μπορεί να είναι το αντικείμενο μιας πολιτικής. Οι ομάδες δραστών ή άλλων οντοτήτων μπορούν να διαχωριστούν ανάλογα με το αν το σύνολο των μελών ορίζεται εκτατικά (π.χ μέσω απαρίθμησης σε κάποια καταχώρηση) ή εκούσια (π.χ. βάσει ενός συγκεκριμένου μέρους όπου διάφορες οντότητες βρίσκονται αυτή τη στιγμή)[63].

Η οντολογία action ορίζει διάφορους τύπους βασικών ενεργειών όπως η πρόσβαση, η επικοινωνία, η κίνηση κλπ. Ο οντολογικός ορισμός μιας ενέργειας συνδέει την ενέργεια με μια λίστα ιδιοτήτων που περιγράφουν το περιεχόμενο της πράξης αυτής. Παραδείγματα ιδιοτήτων των κλάσεων των ενεργειών είναι: ο προορισμός της επικοινωνίας, το είδος κρυπτογράφησης, ο χρόνος, προηγούμενο ιστορικό κλπ. Κάθε ιδιότητα συνδέεται με εύρος τιμών που θα μπορούσε να έχει στην κλάση των ενεργειών. Ένα συγκεκριμένο στιγμιότυπο της κλάσης των ενεργειών μπορεί να πάρει τιμές για μια συγκεκριμένη ενέργεια μόνο μέσα από αυτό το εύρος. Για μια συγκεκριμένη εφαρμογή, οι οντολογίες του πυρήνα της KAoS συνήθως επεκτείνονται με επιπρόσθετες κλάσεις, στιγμιότυπα και κανόνες, που χρησιμοποιούν τις έννοιες των οντολογιών του πυρήνα σαν υπερσύνολα. Αυτό επιτρέπει στο πλαίσιο της KAoS (δημιουργία, διαχείριση, εξαγωγή συμπερασμάτων μέσω οντολογιών) να βρίσκει εξειδικευμένες έννοιες. Στην KAoS οι πολιτικές μπορεί να εκφράζουν εξουσιοδότηση (περιορισμοί που επιτρέπουν ή απαγορεύουν μια ενέργεια) ή υποχρέωση (περιορισμοί που απαιτούν μια ενέργεια για να εκτελεστούν) για κάποιο είδος ενέργειας που πραγματοποιείται από έναν ή περισσότερους δράστες, ενώ επιπλέον βοηθητικές πληροφορίες μπορούν να συνδέονται με μια πολιτική όπως π.χ. η ύπαρξη κάποιας ποινής για την παραβίαση μιας συγκεκριμένης πολιτικής[64].

Η πολιτική επομένως στην KAoS αναπαριστάται σαν ένα στιγμιότυπο μιας εκ' των τεσσάρων κλάσεων: positive ή negative authorization, και positive ή negative obligation. Το στιγμιότυπο κατέχει τιμές για διάφορες ιδιότητες που σχετίζονται με τη διαχείριση (π.χ. προτεραιότητα, time stamp) που προσδιορίζουν πώς μια δεδομένη πολιτική χειρίζεται

[63] Wachter, S. (2018), "Internet of Things: Privacy, profiling, discrimination, and the GDPR", Computer Law & Security Review, 34 (3), pp. 436-449
[64] Wachter, S. (2018), "Internet of Things: Privacy, profiling, discrimination, and the GDPR", Computer Law & Security Review, 34 (3), pp. 436-449

μέσα στο σύστημα. Η σημαντικότερη ιδιότητα είναι το όνομα της κλάσης της ενέργειας, όπου χρησιμοποιείται για να προσδιορίσει την πραγματική σημασία της πολιτικής. Οι πολιτικές εξουσιοδότησης χρησιμοποιούν την παραπάνω ιδιότητα για να προσδιορίσουν την πράξη που επιτρέπεται ή απαγορεύεται. Οι πολιτικές υποχρέωσης την χρησιμοποιούν για τον προσδιορισμό της πράξης που επιβάλλεται ή απαλλάσσεται. Οι ιδιότητες που αφορούν την ποινή μιας πολιτικής περιέχουν μια τιμή που αντιστοιχεί σε μια κλάση ενεργειών που πρέπει να γίνουν αφού παραβιαστεί μια πολιτική[65].

3.1.2 Rei Policy Ontology

Η Rei είναι μια γλώσσα καθορισμού πολιτικών που χρησιμοποιεί την γλώσσα OWL και επιτρέπει στους χρήστες να αναπτύσσουν πολιτικές που αφορούν οντολογίες πεδίου ενδιαφέροντος. Χρησιμοποιείται για να περιγράψει θετικές και αρνητικές παραχωρήσεις αλλά και υποχρεώσεις. Καθώς η Rei στρέφεται προς κατανεμημένα περιβάλλοντα, περιλαμβάνει και προδιαγραφές επίλυσης συγκρούσεων όπως για παράδειγμα ανάθεση προτεραιότητας μεταξύ πολιτικών ή μεταξύ των επιμέρους κανόνων μιας πολιτικής. Η Rei αποτελείται από διάφορες οντολογίες : ReiPolicy, ReiMetaPolicy, ReiEntity, ReiDeontic, ReiConstraint, ReiAnalysis, και ReiAction. Κάθε οντολογία περιγράφει τις κλάσεις και τις ιδιότητες που σχετίζονται με το πεδίο αυτό[66].

Παρακάτω περιγράφονται οι οντολογίες αυτές[67]:

1. Policy: Οι πολιτικές χρησιμοποιούνται για να οδηγήσουν τη συμπεριφορά των οντοτήτων μέσα στο πεδίο. Μια πολιτική κυρίως περιέχει μια λίστα κανόνων και το πλαίσιο που χρησιμοποιήθηκε για τον ορισμό του πεδίου της πολιτικής. Θα μπορούσε επίσης να περιλαμβάνει επίσης μια λίστα προεπιλογών που χρησιμοποιήθηκαν για την ερμηνεία της πολιτικής καθώς επίσης και ένα σύνολο προδιαγραφών για την επίλυση συγκρούσεων.
2. Deontic Object: Η κλάση αυτή χρησιμοποιείται για τη δημιουργία παραχωρήσεων, απαγορεύσεων, υποχρεώσεων και απαλλαγών (δεοντικά αντικείμενα) για τις διάφορες οντότητες του πεδίου της πολιτικής. Περιλαμβάνει δομές που

[65] Westby, J., R. (2010), "Governance of enterprise security: CyLab 2010 report", Pittsburgh, PA: Carnegie Mellon
[66] Westby, J., R. (2010), "Governance of enterprise security: CyLab 2010 report", Pittsburgh, PA: Carnegie Mellon
[67] Wachter, S. (2018), "Internet of Things: Privacy, profiling, discrimination, and the GDPR", Computer Law & Security Review, 34 (3), pp. 436-449

περιγράφουν πάνω σε ποιές ενέργειες το ένα δεοντικό αντικείμενο περιγράφεται, ποιός είναι ο δράστης μιας ενέργειας, καθώς και κάτω από ποιές συνθήκες εφαρμόζεται το δεοντικό αντικείμενο. Action: Η οντολογία αυτή είναι από τις πιο σημαντικές στις προδιαγραφές της Rei καθώς οι πολιτικές περιγράφονται πάνω σε πιθανές ενέργειες στο πεδίο. Η κλάση αυτή περιλαμβάνει ιδιότητες που απαιτούνται για όλες τις ενέργειες. Η Rei περιλαμβάνει ακόμα μια αναπαράσταση των ενεργειών που επιτρέπει την λήψη περισσότερων χρήσιμων πληροφοριών, κάνοντας έτσι ευκολότερη την κατανόηση της ενέργειας και των παραμέτρων της. Τέλος, επιτρέπει πληροφορίες εξαρτώμενες από το πεδίο για ενέργειες που πρόκειται να προστεθούν.

3. Constraint: Η κλάση αυτή περιλαμβάνει τους περιορισμούς, ορίζοντας ένα σύνολο αντικειμένων, ένα σύνολο ενεργειών και ένα σύνολο χρηστών. Υπάρχουν δύο είδη περιορισμών, SimpleConstraint και BooleanConstraint. Στην πρώτη περίπτωση οι περιορισμοί μοντελοποιούνται σαν μια τριάδα που αποτελείται από το υποκείμενο (subject), το κατηγόρημα (predicate) και το αντικείμενο (object). Οι περιορισμοί (απλοί και λογικοί) μπορούν να συνδυαστούν σαν ζευγάρια χρησιμοποιώντας τους λογικούς τελεστές and, or και not. Κάθε λογικός τελεστής είναι υποκλάση της κλάσης BooleanConstraint.
4. Entity: Κάθε χρήστης, πράκτορας ή πόρος υλικού περιγράφεται σαν μία οντότητα. Προς το παρόν η κλάση Entity έχει μόνο μία ιδιότητα, την affiliation, που περιγράφει τον οργανισμό στον οποίο ανήκει μία οντότητα. Η κλάση Entity χωρίζεται στις υποκλάσεις Agent, Object και Variable που προσδιορίζουν αν μια οντότητα είναι πράκτορας, κάποιος πόρος υλικού ή μια μεταβλητή για την περιγραφή των περιορισμών.
5. MetaPolicy: Οι προδιαγραφές της Rei περιλαμβάνουν δομές μεταπολιτικών (metapolicies) για το πώς ερμηνεύονται οι πολιτικές και το πώς μπορούν να επιλυθούν οι συγκρούσεις. Η Rei μοντελοποιεί δύο βασικούς τύπους μεταπολιτικών, έναν για τις προεπιλογές και έναν για την επίλυση συγκρούσεων, για τον χειρισμό διαφορετικών απαιτήσεων των πολιτικών.
6. Analysis: Για να είναι δυνατή η ανάπτυξη συνεκτικών και έγκυρων πολιτικών, η Rei παρέχει δύο καθορισμούς. Τη διαχείριση μέσω περιπτώσεων χρήσης (use-cases) και ανάλυση what-if. Στην πρώτη περίπτωση, ένα σύνολο περιπτώσεων χρήσης μπορεί να περιγραφεί σαν το σύνολο το οποίο μπορεί να επαληθεύεται συνεχώς με βάση μια σειρά πολιτικών. Η ανάλυση what-if χρησιμοποιείται για τον προσδιορισμό προσωρινών αλλαγών στην πολιτική ή στις οντότητες με σκοπό να

εξεταστούν τα αποτελέσματά τους πριν από την ολοκλήρωσή τους.

3.1.3 SOUPA Policy Ontology

Η SOUPA (Standard Ontology for Ubiquitous and Pervasive Applications) είναι ένα σύνολο οντολογιών για την υποστήριξη της αναπαράστασης της γνώσης αλλάκαι τον διαμοιρασμό της, στα συστήματα διάχυτου υπολογισμού. Το πρόγραμμα SOUPA ξεκινά τον Νοέμβριο του 2003 και αποτελεί μέρος του UbiComp Special Interest Groupπου χρησιμοποιεί την γλώσσα OWL και περιλαμβάνει λεξιλόγια για την αναπαράσταση ευφυών πρακτόρων που συνδέονται με πεποιθήσεις, επιθυμίες και προθέσεις, χρόνο, χώρο, γεγονότα, προφίλ χρηστών, ενέργειες και πολιτικές για ασφάλεια και ιδιωτικότητα. Αποτελείται από δύο διαφορετικά, αλλά σχετιζόμενα σύνολα οντολογιών: SOUPA Core και SOUPA Extension. Το πρώτο σύνολο προσπαθεί να ορίσει γενικά λεξιλόγια τα οποία είναι καθολικά για το χτίσιμο εφαρμογών διάχυτου υπολογισμού, ενώ το δεύτερο το οποίο αποτελεί επέκταση του πρώτου, ορίζει επιπρόσθετα λεξιλόγια για την υποστήριξη συγκεκριμένων τύπων εφαρμογών[68].

Συγκεκριμένα το σύνολο Core αποτελείται από εννιά οντολογίες[69]:

1. Person: Η οντολογία αυτή ορίζει τυπικά λεξιλόγια για την περιγραφή τωνπληροφοριών επικοινωνίας και του προφίλ ενός προσώπου. Η κλάση Person ορίζεται γιανα αναπαραστήσει ένα σύνολο όλων των ανθρώπων στο πεδίο της SOUPA. Agent, Action & Bdi: Μερικές φορές όταν χτίζεται ένα ευφυές σύστημα διάχυτου υπολογισμού, είναι χρήσιμο να μοντελοποιούνται οντότητες όπως οι πράκτορες. Στην SOUPA οι πράκτορες χαρακτηρίζονται από ένα σύνολο γνωστικιστικών (mentalistic) εννοιών όπως η γνώση, η πεποίθηση, η πρόθεση και η υποχρέωση. Στην οντολογία αυτή, εξίσου οι υπολογιστικές οντότητες καθώς και οι χρήστες μπορούν να μοντελοποιηθούν σαν πράκτορες.
2. Policy: Η ασφάλεια και η ιδιωτικότητα είναι δύο έννοιες που απασχολούν όλο και περισσότερο στην ανάπτυξη συστημάτων διάχυτου υπολογισμού. Η πολιτική είναι μια τεχνική για τον έλεγχο και την προσαρμογή των συμπεριφορών του χαμηλού επιπέδου του συστήματος, προσδιορίζοντας κανόνες υψηλού επιπέδου. Στην SOUPA, μια πολιτική είναι ένα σύνολο κανόνων. Οι κανόνες ορίζονται από έναν

[68] Wachter, S. (2018), "Internet of Things: Privacy, profiling, discrimination, and the GDPR", Computer Law & Security Review, 34 (3), pp. 436-449

[69] Wachter, S. (2018), "Internet of Things: Privacy, profiling, discrimination, and the GDPR", Computer Law & Security Review, 34 (3), pp. 436-449

δημιουργό πολιτικών (π.χ. ένα χρήστη ή πράκτορα), και οι κανόνες αυτοί επιβάλλονται από κάποιον που εφαρμόζει τις πολιτικές (π.χ. έναν πράκτορα που προστατεύει την ιδιωτικότητα). Ο ορισμός κάθε κανόνα δίνει εξειδικευμένες οδηγίες σε αυτόν που επιβάλλει την πολιτική. Η κλάση Policy αντιπροσωπεύει ένα σύνολο από όλα τα κείμενα πολιτικών. Ένα στιγμιότυπο της κλάσης αυτής αντιπροσωπεύει ένα τέτοιο κείμενο που ρυθμίζει τις παραχωρήσεις για τους πράκτορες να εκτελέσουν διάφορες πράξεις. Οι ιδιότητες creator, policyOf και enforcer περιγράφουν τον πράκτορα που δημιουργεί την πολιτική, τον πράκτορα στον οποίο εφαρμόζεται η πολιτική αυτή και τον πράκτορα που επιβάλλει τους κανόνες της πολιτικής αυτής. Για να περιγραφεί ο χρόνος όπου ένα κείμενο πολιτικής δημιουργήθηκε, η οντολογία ορίζει την ιδιότητα createdOn και εύρος της οποίας είναι η κλάση InstantThing. Για να περιγραφούν οι κανόνες της πολιτικής, η οντολογία ορίζει την ιδιότητα permits για να εκφράσει τις παραχωρήσεις και την ιδιότητα forbids για να εκφράσει τις απαγορεύσεις.

3. Time: Η SOUPA ορίζει ένα σύνολο οντολογιών για την έκφραση του χρόνου καθώς και για σχέσεις που βασίζονται σε χρονικά γεγονότα. Μπορούν να χρησιμοποιηθούν για να περιγράψουν ιδιότητες διαφορετικών γεγονότων που συμβαίνουν στο φυσικό κόσμο. Space: Η οντολογία αυτή είναι σχεδιασμένη για να υποστηρίζει την εξαγωγή συμπερασμάτων σχετικά με τις χωρικές σχέσεις μεταξύ διαφόρων τύπων γεωγραφικών περιοχών, την αντιστοιχία από γεω-χωρικές συντεταγμένες σε συμβολική αναπαράσταση του χώρου και αντίστροφα, καθώς και την αναπαράσταση γεωγραφικών μετρήσεων του χώρου.
4. Event: Τα γεγονότα είναι δραστηριότητες που έχουν χωρικές αλλά και χρονικές προεκτάσεις. Μια οντολογία γεγονότων μπορεί να χρησιμοποιηθεί για την εμφάνιση διαφόρων δραστηριοτήτων και προγραμματισμένων ενεργειών. Μέσα σε αυτή την οντολογία, η κλάση Event αναπαριστά όλα τα γεγονότα του πεδίου. Οι οντολογίες της SOUPA Extension ορίζονται με δύο σκοπούς: 1) τον ορισμό ενός επεκτεταμένου συνόλου λεξιλογίων για την υποστήριξη συγκεκριμένων τύπων εφαρμογών πεδίου διάχυτου υπολογισμού και 2) για να δείξουν πώς ορίζονται νέες οντολογίες επεκτείνοντας της οντολογίες του πυρήνα της SOUPA. Προς το παρόν η προέκταση της SOUPA αποτελείται από πειραματικές οντολογίες για την υποστήριξη εφαρμογών επίγνωσης πλαισίου (context-aware) σε έξυπνα περιβάλλοντα.

Αυτές είναι οι παρακάτω[70]:

- Priority: Η οντολογία αυτή ορίζει πρόσθετα λεξιλόγια για την ανάθεση τιμών προτεραιοτήτων στις επιθυμίες ενός πράκτορα και τις προοριζόμενες ενέργειες. Αν κάποια στιγμή δηλαδή υπάρξει σύγκρουση μεταξύ διαφορετικών επιθυμιών ή ενεργειών, τότε οι τιμές προτεραιότητας μπορούν να χρησιμοποιηθούν για να επιλύσουν τη σύγκρουση αυτή. Conditional & Unconditional Belief: Η οντολογία αυτή ορίζει τα λεξιλόγια για την περιγραφή των υπό συνθήκη πεποιθήσεων. Μια υπό συνθήκη πεποίθηση μπορεί να αποδοθεί με χρονικές τιμές, τιμές ακρίβειας, ή τοπικά ορισμένες συνθήκες. Δηλώσεις που ορίζονται με υπό συνθήκη ιδιότητες θεωρούνται αληθείς αν το σχετιζόμενο χρονόσημο ανάγνωσης (time stamp) είναι έγκυρο, η τιμή ακρίβειας είναι πάνω από κάποιο προκαθορισμένο όριο και όλες οι τοπικά ορισμένες συνθήκες ικανοποιούνται. Σε διαφορετική περίπτωση, οι δηλώσεις θεωρούνται ψευδής.
- Contact Preference: Η οντολογία αυτή ορίζει τα λεξιλόγια που περιγράφουν τις προτιμήσεις επικοινωνίας ενός χρήστη, οι οποίες είναι ένα σύνολο κανόνων που προσδιορίζει το πώς ο χρήστης θέλει να επικοινωνεί το σύστημα μαζί του κάτω από διάφορες συνθήκες (π.χ. σε μια συνάντηση, εκτός πόλης, τα σαββατοκύριακα). Για παράδειγμα, ένας χρήστης μπορεί να ορίσει το σύστημα να επικοινωνεί μαζί του μέσω κινητού τηλεφώνου όταν βρίσκεται εκτός πόλης, και μέσω SMS όταν βρίσκεται σε μια συνάντηση.
- Meeting & Schedule: Αυτές οι δύο οντολογίες ορίζουν τα λεξιλόγια για την περιγραφή ενός γεγονότος συνάντησης (meeting event), προγραμματισμένες ενέργειες και τους αντίστοιχους συμμετέχοντες. Μπορούν να βοηθήσουν έξυπνα συστήματα συναντήσεων να αναπαραστήσουν και να εξάγουν συμπεράσματα σχετικά με το περιεχόμενο της συνάντησης.

3.1.4 Rein Ontology

Η Rein είναι ένα πλαίσιο που στηρίζεται στον Ιστό (web-based) για την αναπαράσταση και εξαγωγή συμπερασμάτων πάνω σε πολιτικές σε πεδία που χρησιμοποιούν διαφορετικές γλώσσες αναπαράστασης πολιτικών. Το σύνολο των πόρων (resources) του συστήματος, οι πολιτικές τους καθώς και οι σχέσεις μεταξύ τους σχηματίζουν δίκτυα (Rein Policy Networks). Η Rein επιτρέπει στις οντότητες των δικτύων αυτών να

[70] Wachter, S. (2018), "Internet of Things: Privacy, profiling, discrimination, and the GDPR", Computer Law & Security Review, 34 (3), pp. 436-449

εντοπιστούν τοπικά ή απομακρυσμένα. Η Rein δεν προτείνει μια απλή γλώσσα για να περιγράψει πολιτικές. Επιτρέπει σε κάθε χρήστη να έχει πιθανώς τη δικιά του γλώσσα πολιτικής ή την επαναχρησιμοποίηση μιας ήδη υπάρχουσας γλώσσας και αν είναι απαραίτητο, μια μεταπολιτική. Το πλαίσιο αυτό λοιπόν αποτελείται από δύο κυρίως μέρη, (i) ένα σύνολο οντολογιών που περιγράφουν τα δίκτυα πολιτικών της Rein καθώς και τις αιτήσεις για πρόσβαση σε κάποιο πόρο, και (ii) μια μηχανή εξαγωγής συμπερασμάτων που δέχεται τις αιτήσεις αυτές και αποφασίζει εάν είναι έγκυρες. Περιλαμβάνει την οντολογία Rein Policy network και την οντολογία Rein Request. Οι οντολογίες αυτές φαίνονται στην παρακάτω εικόνα[71].

Η οντολογία Rein Policy network είναι κατασκευασμένη από τρείς βασικές ιδιότητες που χρησιμοποιούνται για να συνδέσουν τις οντότητες του δικτύου των πολιτικών (policy network entities) που βρίσκονται τοπικά ή φιλοξενούνται μέσω HTTP. Η ιδιότητα policy χρησιμοποιείται για να αντιστοιχήσει τους πόρους με τις αντίστοιχες πολιτικές που έχουν οι μηχανισμοί εισόδων των πόρων αυτών. Η ιδιότητα policylanguage χρησιμοποιείται από μια πολιτική για να αναφερθεί στη γλώσσα που χρησιμοποιεί η πολιτική αυτή και η ιδιότητα meta-policy χρησιμοποιείται από μια γλώσσα και αναφέρεται στους κανόνες που μπορούν να χρησιμοποιηθούν για περαιτέρω εξαγωγή συμπερασμάτων. Μια γλώσσα πολιτικής αναπαριστάται σαν μια RDF-S ή OWL οντολογία. Μια πολιτική μπορεί να είναι ένα σύνολο από στιγμιότυπα RDF-S ή OWL ή ακόμα και ένα σύνολο κανόνων σε κάποια από τις γλώσσες αναπαράστασης πολιτικών που υποστηρίζονται από την Rein. Τέλος, η κλάση Request είναι ένας τρόπος για να τίθενται ερωτήματα στο δίκτυο της Rein. Η κλάση αυτή έχει τέσσερις ιδιότητες – η requester ορίζει ποιά οντότητα πραγματοποιεί την αίτηση, resource είναι ο εκάστοτε πόρος, υπηρεσία ή πράξη που ζητείται, η access είναι ένας όρος (κλάση ή ιδιότητα) που ορίζεται στην γλώσσα αναπαράστασης της πολιτικής για τον μηχανισμό πρόσβασης, και ans είναι η απάντηση της μηχανής. Συνήθως η ιδιότητα resource είναι το URI του πόρου που ζητείται, ενώ η ιδιότητα requester είναι ένα σύνολο ιδιοτήτων ή πιστοποιητικών του αιτούντος, γιατί η ταυτότητά του μπορεί να μην έχει πάντα κάποιο νόημα σε ένα ανοιχτό περιβάλλον όπως ο Ιστός. Τέλος, η μηχανή εξαγωγής συμπερασμάτων της Rein μπορεί εύκολα να τροποποιηθεί ώστε να χειρίζεται επιπλέον ιδιότητες για ένα αίτημα, συμπεριλαμβανομένων περιβαλλοντικών συνθηκών και ιδιοτήτων των πόρων[72].

[71] Wachter, S. (2018), "Internet of Things: Privacy, profiling, discrimination, and the GDPR", Computer Law & Security Review, 34 (3), pp. 436-449
[72] Wachter, S. (2018), "Internet of Things: Privacy, profiling, discrimination, and the GDPR", Computer Law & Security Review, 34 (3), pp. 436-449

3.1.5 NRL Security Ontology

Η NRL είναι ένα σύνολο οντολογιών που σχετίζονται με την ασφάλεια (security). Παρέχει την δυνατότητα να περιγραφούν έννοιες που έχουν να κάνουν με την ασφάλεια, σε διάφορα επίπεδα λεπτομέρειας. Οι οντολογίες από τις οποίες αποτελείται μπορούν να σχολιάσουν πόρους (resources) που μπορεί να είναι από απλά κείμενα μέχρι δια-δραστικές υπηρεσίες. Η NRL οντολογία ασφάλειας σχεδιάστηκε με τους εξής σκοπούς: Να περιγράψει πληροφορίες σχετικές με την ασφάλεια οι οποίες εφαρμόζονται σε όλους τους τύπους των πόρων Να δίνει τη δυνατότητα να σχολιαστούν πληροφορίες που σχετίζονται με την ασφάλεια σε διάφορα επίπεδα λεπτομέρειας για διάφορα περιβάλλοντα, τη δημιουργία οντολογιών οι οποίες είναι εύκολο να επεκταθούν και να προσφέρουν επαναχρησιμοποίηση, τη διευκόλυνση της αντιστοιχίας απαιτήσεων ασφαλείας υψηλού επιπέδου σε χαμηλού επιπέδου δυνατότητες. Υπάρχουν επτά ξεχωριστές οντολογίες από τις οποίες αποτελείται η οντολογία NRL[73]:

1) Main Security Ontology: μια οντολογία που περιγράφει έννοιες σχετικές με την ασφάλεια 2)Credentials Ontology: μια οντολογία για να περιγράψει τα πιστοποιητικά ταυτοποίησης 3)Security Algorithms Ontology: μια οντολογία που περιγράφει διάφορους αλγόριθμους ασφάλειας

4)Security Assurance Ontology: μια οντολογία που καθορίζει διάφορα πρότυπα ασφάλειας 5)Service Security Ontology: μια οντολογία που διευκολύνει τον σχολιασμό των υπηρεσιών του σημασιολογικού Ιστού

6) Agent Security Ontology: μια οντολογία που επιτρέπει την ανάπτυξη ερωτημάτων σχετικά με πληροφορίες ασφάλειας. 7)Information Object Ontology: μια οντολογία που περιγράφει τις παραμέτρους εισόδου και εξόδου των υπηρεσιών του Ιστού. Οι οντολογίες Service Security, Agent Security και Information Object βασίζονται σε ήδη υπάρχουσες οντολογίες ενώ οι υπόλοιπες είναι νέες. Οι οντολογίες Credentials, Security Algorithms, και Security Assurance παρέχουν τιμές για τις ιδιότητες των εννοιών της κύριας οντολογίας Main Security Ontology. Αυτές ενεργοποιούν αυτές τις έννοιες να περιγραφούν με περισσότερες λεπτομέρειες σε σχέση με τους τύπους πιστοποιητικών που χρησιμοποιούνται, τους αλγόριθμους που υποστηρίζονται, και τα σχετιζόμενα επίπεδα ασφαλείας. Η οντολογία Service Security παρέχει τα μέσα εκείνα για να χρησιμοποιηθούν έννοιες ασφαλείας από την κύρια οντολογία στο πλαίσιο των υπηρεσιών του Ιστού. Η

[73] Wachter, S. (2018), "Internet of Things: Privacy, profiling, discrimination, and the GDPR", Computer Law & Security Review, 34 (3), pp. 436-449

οντολογία Agent Service επιτρέπει τη δημιουργία ερωτημάτων που σχετίζονται με την ασφάλεια χρησιμοποιώντας έννοιες από την κύρια οντολογία Main Security. Η οντολογία Information Object επιτρέπει το σχολιασμό των εισόδων και εξόδων των υπηρεσιών χρησιμοποιώντας την οντολογία Security Algorithms.

3.1.6 P3P

Η P3P (Platform for Privacy Preferences Project) είναι μια γλώσσα περιγραφής πολιτικών που έχει υλοποιηθεί από την W3C. Επιτρέπει στις ιστοσελίδες να εκφράσουν τις διάφορες πρακτικές ιδιωτικότητάς τους σε ένα συγκεκριμένο τύπο (format) έτσι ώστε να μπορούν να ανακτηθούν αυτόματα και να ερμηνευτούν εύκολα από τους πράκτορες χρηστών (user agents). Οι πράκτορες θα επιτρέπουν στους χρήστες να ενημερώνονται για τις πρακτικές της συγκεκριμένης σελίδας (σε μορφή κατανοητή τόσο από τη μηχανή όσο και από τους ανθρώπους) και να αυτοματοποιούν τη λήψη αποφάσεων βασιζόμενοι στις πρακτικές αυτές, όπου χρειάζεται. Επιπλέον οι χρήστες δε χρειάζεται να διαβάζουν τις πολιτικές ιδιωτικότητας κάθε φορά που επισκέπτονται την σελίδα. Επιπλέον γνωρίζοντας ο χρήστης αυτές τις πληροφορίες (συνήθως μέσω έξυπνων διεπαφών), μπορεί να πάρει συνειδητές αποφάσεις για το αν θα υποβάλει ή όχι προσωπικές πληροφορίες σε μια συγκεκριμένη υπηρεσία[74].

Παρότι η P3P παρέχει ένα τεχνικό μηχανισμό για να εξασφαλίσει ότι οι χρήστες μπορούν να είναι ενημερωμένοι σχετικά με τις πολιτικές ιδιωτικότητας πριν ανακοινώσουν προσωπικές τους πληροφορίες, δεν παρέχει ένα μηχανισμό για να εξασφαλίσει ότι οι ιστοσελίδες συμπεριφέρονται σύμφωνα με τις πολιτικές τους. Παρόλα αυτά η P3P είναι συμπληρωματική σε κανονισμούς και αυτορυθμιζόμενα προγράμματα που παρέχουν μηχανισμούς επιβολής. Οι πολιτικές ιδιωτικότητας προορίζονται για να περιγράψουν τις πρακτικές μιας εταιρίας όσο αφορά τα δεδομένα, δηλαδή τι κάνουν με τις πληροφορίες που συλλέγουν από τα άτομα (συνήθως πελάτες αλλά μερικές φορές εργαζόμενους και άλλους). Οι προδιαγραφές της P3P περιλαμβάνουν ένα τυποποιημένο λεξιλόγιο για την περιγραφή των πρακτικών αυτών και ένα σχήμα βάσης δεδομένων για να περιγράψουν το είδος των πληροφοριών που συλλέγονται. Μια πολιτική P3P είναι μια συλλογή στοιχείων λεξιλογίου και δεδομένων που περιγράφουν τις παραπάνω πρακτικές μιας συγκεκριμένης ιστοσελίδας. Μια P3P πολιτική αποτελείται ουσιαστικά από τις απαντήσεις σε μια σειρά πολλαπλών ερωτήσεων και επομένως δεν περιέχει πάντα τόσο λεπτομερείς πληροφορίες

[74] Baer, W. S. and Parkinson, A. (2007), "Cyberinsurance in IT Security Management," IEEE Security and Privacy, 5 (3), pp. 50–56

όσο μια πολιτική ιδιωτικότητας που είναι αναγνώσιμη από τους ανθρώπους[75].

Η τυποποιημένη μορφή μιας P3P πολιτικής της επιτρέπει την αυτόματη επεξεργασία. Οι προδιαγραφές της P3P περιλαμβάνουν ακόμα ένα πρωτόκολλο για την αίτηση και μετάδοση πολιτικών. Το πρωτόκολλο αυτό είναι χτισμένο στο ίδιο πρωτόκολλο μεταφοράς υπερκειμένου (HTTP protocol), το οποίο χρησιμοποιούν οι περιηγητές για την επικοινωνία με τους εξυπηρετητές. Όπως φαίνεται και στην παρακάτω εικόνα οι πράκτορες χρησιμοποιούν τυποποιημένα HTTP αιτήματα ενός αρχείου αναφοράς πολιτικών (policy referencefile) από μια γνωστή τοποθεσία της ιστοσελίδας στην οποία ο χρήστης κάνει το αίτημα. Το αρχείο αναφοράς της πολιτικής προσδιορίζει την τοποθεσία του αρχείου της πολιτικής που εφαρμόζεται σε κάθε κομμάτι της ιστοσελίδας. Μπορεί να υπάρχει μια πολιτική για ολόκληρη την ιστοσελίδα, ή διάφορες πολιτικές που καλύπτουν ένα διαφορετικό κομμάτι της σελίδας. Ο πράκτορας τότε μπορεί να βρει την κατάλληλη πολιτική, να την αναλύσει και στη συνέχεια να δράσει ανάλογα με τις προτιμήσεις του χρήστη. Η P3P επίσης επιτρέπει στις ιστοσελίδες να τοποθετούν τα αρχεία αναφοράς των πολιτικών σε άλλες τοποθεσίες πέρα των γνωστών. Σε αυτές τις περιπτώσεις η ιστοσελίδα πρέπει να υποδεικνύει την τοποθεσία αυτή χρησιμοποιώντας μια ειδική HTTP επικεφαλίδα. Οι ειδικές επικεφαλίδες επιπλέον χρησιμοποιούνται ώστε να μεταφέρουν μια προαιρετική συνοπτική πολιτική. Οι πολιτικές αυτές αποτελούν περιλήψεις ολόκληρων των P3P πολιτικών και περιγράφουν μόνο τις πρακτικές όσο αφορά τα δεδομένα, χωρίς να έχουν τις πλήρεις δυνατότητες έκφρασης των P3P πολιτικών[76].

3.1.7 Trust Ontology in Service-Oriented Environments

Η εμπιστοσύνη (trust) πραγματοποιείται μέσω της έννοιας μιας σχέσης εμπιστοσύνης (trustrelationship) και ενός βαθμού εμπιστοσύνης (trust value). Η σχέση εμπιστοσύνης δηλώνει ένα βαθμό εμπιστοσύνης από το μέρος που εμπιστεύεται (trusting party) στο εμπιστευμένο μέρος (trusted party). Σε ένα περιβάλλον προσανατολισμένο στις υπηρεσίες (service-oriented environment) η εμπιστοσύνη μπορεί να επικυρωθεί σε τρεις τουλάχιστον περιοχές, όπως πράκτορας (agent), υπηρεσία (service) και προϊόν (product[77]).

[75] Baer, W. S. and Parkinson, A. (2007), "Cyberinsurance in IT Security Management," IEEE Security and Privacy, 5 (3), pp. 50–56
[76] Baer, W. S. and Parkinson, A. (2007), "Cyberinsurance in IT Security Management," IEEE Security and Privacy, 5 (3), pp. 50–56
[77] Baer, W. S. and Parkinson, A. (2007), "Cyberinsurance in IT Security Management," IEEE Security and Privacy, 5 (3), pp. 50–56

Στο ανώτερο επίπεδο υπάρχει η έννοια ‘εμπιστοσύνη’. Στο μεσαίο επίπεδο υπάρχει μια λίστα γενικότερων εννοιών όπως η εμπιστοσύνη του πράκτορα (agent trust), η εμπιστοσύνη της υπηρεσίας (service trust) και η εμπιστοσύνη του προϊόντος (product trust). Στο χαμηλότερο επίπεδο υπάρχει μια λίστα από συγκεκριμένες έννοιες, οι οποίες αποτελούν η κάθε μία και μια συγκεκριμένη οντολογία. Πιο ειδικά, η οντολογία service trust ορίζεται σαν την εννοιολογική μορφοποίηση ότι ο πελάτης (customer) εμπιστεύεται την υπηρεσία ανάλογα με την ποιότητα της υπηρεσίας (Quality of Service) που διαθέτει ο παροχέας της συγκεκριμένης υπηρεσίας. Οι υπόλοιπες έννοιες έχουν ως εξής[78]:

- Service Requester: πράκτορας που έχει το βαθμό εμπιστευτικότητας της QoS της υπηρεσίας που παρέχεται
- Service: μια εμπιστευόμενη οντότητα της οποίας η QoS εξετάζεται από τον service requester
- Context: αναφέρεται στη φύση της υπηρεσίας
- Quality Aspects: ορίζουν την QoS
- QoS criteria: είναι μετρικές που χρησιμοποιούνται για την ποιοτική αξιολόγηση της εμπιστευτικότητας των υπηρεσιών
- Time slot: είναι το χρονικό πλαίσιο για το οποίο ο βαθμός εμπιστοσύνης ισχύει (παραμένει σταθερός)
- Trustworthiness: είναι ένα μέτρο εμπιστοσύνης σε μια κλίμακα εμπιστευτικότητας.

[78] Westby, J., R. (2010), “Governance of enterprise security: CyLab 2010 report”, Pittsburgh, PA: Carnegie Mellon

Κεφάλαιο 4. Ανάλυση της οντολογίας που αντιστοιχεί στην προστασία προσωπικών δεδομένων

4.1 Ανάπτυξη οντολογίας Privacy Policy

Η οντολογία ως μια τυποποιημένη περιγραφή ενός συγκεκριμένου τομέα γνώσης η οποία πρέπει να είναι αποδεκτή από μια ομάδα ατόμων, για να έχει νόημα η ύπαρξή της, έρχεται να καλύψει το πρόβλημα της πολυσημίας (πολλές λέξεις περιγράφουν το ίδιο αντικείμενο) και της αμφισημίας (ο ίδιος όρος περιγράφει διαφορετικά αντικείμενα). Μια οντολογία περιγράφει με ακρίβεια τις έννοιες που αποφασίζει η ομάδα να περιγράψει. Η κατασκευή της απαιτεί να αποφασιστούν[79]:

- οι "παραδοχές" που πρέπει να λάβουν υπόψη οι κατασκευαστές της για το περιεχόμενο της οντολογίας (ποιες έννοιες θα περιγραφούν και ποιες όχι, αφού δεν μπορούν να περιγραφούν τα πάντα)
- ο σκοπός δημιουργίας της (ποιοί θα είναι οι χρήστες της και που θα τη χρησιμοποιήσουν) το είδος της οντολογίας που θα αναπτυχθεί (μια οντολογία που θα περιγράφει γενικούς όρους, όπως ο χρόνος και ο χώρος ή μια οντολογία που θα περιγράφει όρους μιας εξειδικευμένης περιοχής ενδιαφέροντος όπως η βιολογία)
- η γλώσσα στην οποία θα υλοποιηθεί
- η μεθοδολογία υλοποίησης της οντολογίας

4.1.1 Είδος Οντολογίας

Έχουν αναπτυχθεί διάφορα είδη οντολογιών για διάφορους τύπους εφαρμογών και οι οποίες διαφέρουν ως προς το επίπεδο λεπτομέρειας περιγραφής του πεδίου ενδιαφέροντος το οποίο αναπαριστούν. ως προς το επίπεδο γενίκευσης, μπορούν να διακριθούν σε[80]:

1) Οντολογίες "γενικού επιπέδου" (*top-level ontologies*), οι οποίες περιγράφουν γενικές έννοιες, ανεξάρτητες συγκεκριμένου πεδίου ενδιαφέροντος

2) Οντολογίες πεδίου ενδιαφέροντος και οντολογίες εργασίας (*domain and taskontologies*), οι οποίες αντίστοιχα, περιγράφουν έννοιες μιας συγκεκριμένης περιοχής ενδιαφέροντος,

[79] Westby, J., R. (2010), "Governance of enterprise security: CyLab 2010 report", Pittsburgh, PA: Carnegie Mellon
[80] Tikkinen-Piri, C., Rohunen, A. and Markulla, J. (2018), "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", Computer Law & Security Review, 34 (1), pp. 134-153

(όπως η βιολογία, η φυσική) και μια γενική εργασία ή δραστηριότητα (όπως η διάγνωση, ή οι πωλήσεις), εξειδικεύοντας τις έννοιες της οντολογίας του γενικού επιπέδου
3) Οντολογίες εφαρμογής (*application ontologies*), οι οποίες περιγράφουν τις απαραίτητες για μια συγκεκριμένη εφαρμογή έννοιες.

4.1.2 Γλώσσα υλοποίησης της οντολογίας

Οι γλώσσες αναπαράστασης οντολογιών διακρίνονται σε παραδοσιακές γλώσσες (Κατηγορηματική Λογική Πρώτης Τάξης, Λογική Πλαισίων, Περιγραφική Λογική), σε γλώσσες που βασίζονται στο δίκτυο και η σύνταξή τους βασίζεται στην XML, όπως SHOE (Simple HTML ontology extensions) , XOL (Ontology exchange language), OML (Ontology Markup Language), RDFS (Resource Description Framework Schema), DAML (DARPA Agent Markup Language) , OIL (Ontology Interchange Language), OWL (Ontology Web Language), και σε γλώσσες που αναπτύχθηκαν για να αναπαραστήσουν συγκεκριμένες οντολογίες και να χρησιμοποιηθούν σε συγκεκριμένες εφαρμογές, όπως η CycL[81].

Πιο συγκεκριμένα, είναι μια σημασιολογική γλώσσα με επισημειώσεις για την έκδοση και διαμοιρασμό οντολογιών στον Παγκόσμιο Ιστό. Επιτρέπει την περιγραφή της σημασιολογίας της γνώσης με τρόπο προσπελάσιμο από μηχανές. Ενώ παλαιότερες γλώσσες χρησιμοποιήθηκαν για την ανάπτυξη εργαλείων και οντολογιών για εξειδικευμένες κοινότητες χρηστών (ειδικά στις επιστήμες και για εταιρικές εφαρμογές ηλεκτρονικού εμπορίου), δεν ήταν συμβατές με την αρχιτεκτονική του Παγκόσμιου Ιστού γενικά και του σημασιολογικού Ιστού ειδικότερα. Η OWL χρησιμοποιεί URIs για ονοματοδοσία καθώς και το πλαίσιο περιγραφής για τον Ιστό, το οποίο παρέχεται από την RDF, προσθέτοντας τις παρακάτω δυνατότητες στις οντολογίες[82]:
1. Δυνατότητα να κατανέμονται μεταξύ πολλαπλών συστημάτων,
2. Κλιμάκωση σύμφωνη με τις ανάγκες του Ιστού,
3. Συμβατότητα με πρότυπα του Ιστού για προσπελασιμότητα και διεθνοποίηση,
4. Ανοικτότητα και επεκτασιμότητα.

[81] Tikkinen-Piri, C., Rohunen, A. and Markulla, J. (2018), "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", Computer Law & Security Review, 34 (1), pp. 134-153
[82] Tikkinen-Piri, C., Rohunen, A. and Markulla, J. (2018), "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", Computer Law & Security Review, 34 (1), pp. 134-153

Η OWL είναι χτισμένη πάνω από τις RDF και RDF Schema και προσθέτει επιπλέον λεξιλόγιο για την περιγραφή ιδιοτήτων και κλάσεων: μεταξύ άλλων, σχέσεις ανάμεσα σε κλάσεις (π.χ. ξένες μεταξύ τους), πληθάριθμος (π.χ. "ακριβώς ένα"), ισότητα, περισσότεροι τύποι ιδιοτήτων, (χαρακτηριστικά ιδιοτήτων (π.χ. συμμετρία) και απαριθμημένες κλάσεις.

Παρέχει μηχανισμούς για τη δημιουργία όλων των συστατικών μιας οντολογίας: έννοιες, στιγμιότυπα, ιδιότητες (ή σχέσεις), και αξιώματα. Μπορεί να οριστούν δυο είδη ιδιοτήτων: ιδιότητες αντικειμένων και ιδιότητες τύπων δεδομένων. Οι ιδιότητες αντικειμένων συσχετίζουν στιγμιότυπα με άλλα στιγμιότυπα. Οι ιδιότητες τύπων δεδομένων συσχετίζουν στιγμιότυπα με τιμές τύπων δεδομένων, για παράδειγμα συμβολοσειρές κειμένου, ή αριθμούς. Οι έννοιες μπορεί να έχουν υπέρ- και υπό-έννοιες, παρέχοντας έτσι ένα μηχανισμό για συλλογιστική υπαγωγής και κληρονομικότητα ιδιοτήτων. Αξιώματα χρησιμοποιούνται για να παρέχουν πληροφορίες σχετικά με κλάσεις και ιδιότητες, για παράδειγμα για τον καθορισμό της ισοδυναμίας μεταξύ δυο κλάσεων ή την περιοχή τιμών μιας ιδιότητας. Υπάρχουν τρεις εκδόσεις της OWL[83]:

1) Η OWL Lite προσφέρει ένα περιορισμένο σύνολο χαρακτηριστικών, επαρκή για πολλές εφαρμογές και συγχρόνως σχετικά αποτελεσματικά υπολογιστικά,
2) Η OWL DL είναι ένα υπερσύνολο της OWL Lite και βασίζεται σε μια μορφή λογικής πρώτης τάξης που καλείται περιγραφική λογική,
3) Η OWL Full είναι ένα υπερσύνολο της OWL DL και εξαλείφει κάποιους περιορισμούς της OWL DL με το τίμημα της εισαγωγής προβλημάτων υπολογιστικής διαχειρισιμότητας.

Στη συγκεκριμένη εργασία χρησιμοποιείται η έκδοση OWL-DL. Η έκδοση αυτή προσφέρει τη μέγιστη εκφραστικότητα, διατηρώντας παράλληλα υπολογιστική πληρότητα (όλα τα συμπεράσματα είναι υπολογίσιμα) και αποδοχή (όλοι οι υπολογισμοί τερματίζονται σε πεπερασμένο χρονικό διάστημα). Επιπλέον οι οντολογίες που βασίζονται στην περιγραφική λογική, αποτελούν μια καλή επιλογή για την περιγραφή της πληροφορίας που τροφοδοτεί τις εφαρμογές περιρρέουσας νοημοσύνης.

4.1.3 Εργαλείο υλοποίησης της οντολογίας

Μεταξύ όλων των εργαλείων το Protégé είναι το πιο διαδεδομένο. Τα πιο ισχυρά του πλεονεκτήματα σε σχέση με τα υπόλοιπα εργαλεία είναι: ανώτερη διεπαφή χρήστη (user

[83] Anderson, R. and Moore, T. (2006), "The Economics of Information Security", Science, 314 (5799), pp. 610-613

interface), επεκτασιμότητα μέσω plug-ins, ευρεία λειτουργικότητα που παρέχεται είτε με την χρήση των plug-ins ή όχι, και το ευρύ σύνολο διαφορετικών μορφών (formats) που μπορούν να εισαχθούν ή να εξαχθούν. Πιο συγκεκριμένα, το Protégé είναι ένα εργαλείο διαχείρισης γνώσης. Χιλιάδες χρήστες το χρησιμοποιούν σε έργα που ποικίλουν από τη μοντελοποίηση της νόσου του καρκίνου έως τη μοντελοποίηση πυρηνικών σταθμών παραγωγής ενέργειας. Το Protégé είναι ελεύθερο λογισμικό[84].

Παρέχει ένα γραφικό δια-δραστικό περιβάλλον για σχεδιασμό και ανάπτυξη βάσεων γνώσης. Επιτρέπει στους μηχανικούς και τους ειδικούς εμπειρογνώμονες να εκτελούν με ευκολία εργασίες διαχείρισης γνώσης. Όσοι αναπτύσσουν οντολογίες μπορούν να προσπελαύνουν τις σχετικές πληροφορίες γρήγορα όταν τις χρειάζονται και να διαμορφώνουν και να χειρίζονται οντολογίες. Η ιεραρχική δομή της οντολογίας αναπαρίσταται με τη μορφή δέντρου δίνοντας στο χρήστη γρήγορη και εύκολη πρόσβαση στις κλάσεις και υπό-κλάσεις. Για την εισαγωγή τιμών στις ιδιότητες, το Protégé χρησιμοποιεί ειδικές φόρμες[85],

Το γνωστικό μοντέλο του Protégé είναι συμβατό με το πρωτόκολλο OKBC (Open Knowledge Base Connectivity). Υποστηρίζει κλάσεις και ιεραρχίες κλάσεων με πολλαπλή κληρονομικότητα, templates και slots, ορισμό προκαθορισμένων και αυθαίρετων facet για τα slots με σύνολα επιτρεπόμενων τιμών, περιορισμούς πλήθους, εξ ορισμού τιμές, και αντίστροφα slots, μετα-κλάσεις και ιεραρχία μετα-κλάσεων. Εκτός από την ευχρηστία του, το Protégé διακρίνεται από τα υπόλοιπα ολοκληρωμένα περιβάλλοντα μηχανικής οντολογιών για τις δυνατότητες εξέλιξης και επέκτασης που προσφέρει[86].

Το Protégé έχει με επιτυχία χρησιμοποιηθεί για την κατασκευή και τη χρήση οντολογιών αποτελούμενων από 150.000 πλαίσια (frames). Η δυνατότητα υποστήριξης βάσεων γνώσης αποτελούμενων από εκατοντάδες χιλιάδες πλαίσια απαιτεί την παρουσία δύο βασικών υποσυστημάτων: μιας βάσης δεδομένων για την αποθήκευση και προσπέλαση των δεδομένων και ενός μηχανισμού αποθηκευτικής μνήμης έτσι ώστε να είναι δυνατός ο χειρισμός νέων πλαισίων όταν ο αριθμός τους στη βασική μνήμη έχει ξεπεράσει το μέγιστο όριο.

Ένα από τα βασικότερα πλεονεκτήματα της αρχιτεκτονικής του Protégé είναι ότι το σύστημα είναι κατασκευασμένο με ανοικτό και αρθρωτό σχεδιασμό. Η βασισμένη σε υπό-

[84] Anderson, R. and Moore, T. (2006), "The Economics of Information Security", Science, 314 (5799), pp. 610-613
[85] Anderson, R. and Moore, T. (2006), "The Economics of Information Security", Science, 314 (5799), pp. 610-613
[86] Westby, J., R. (2010), "Governance of enterprise security: CyLab 2010 report", Pittsburgh, PA: Carnegie Mellon

συστήματα αρχιτεκτονική του δίνει τη δυνατότητα προσθήκης νέων λειτουργιών με τη δημιουργία αντίστοιχων πρόσθετων υπό-μονάδων (plug-ins). Κάποιες από τις διαθέσιμες προσθήκες παρέχουν λειτουργίες, όπως[87]:

1)Εμφάνιση εικόνων μορφής gif, βίντεο και ήχου, καθώς και έναν επεξεργαστή διαγραμμάτων που επιτρέπει στο χρήστη να κατασκευάσει μια βάση γνώσης σχεδιάζοντας ένα διάγραμμα του οποίου οι κόμβοι και οι ακμές απεικονίζουν πλαίσια διαφορετικού είδους, ανάλογα με το σχήμα και το χρώμα,
2)Υποστήριξη για αποθήκευση και εισαγωγή οντολογιών γραμμένων σε RDF Schema, αρχεία XML με DTD, αρχεία XML Schema και DAML+OIL,
3)Οπτική αναπαράσταση οντολογιών με το OntoViz plug-in,
4)Συγχώνευση οντολογιών με το PROMPT plug-in,
5)Μηχανές εξαγωγής συμπερασμάτων (Flora, PAL plug-ins),
6)Εισαγωγή στοιχείων από πηγές του διαδικτύου (UMLS, WordNet plug-ins),
7)Αυτόματο υπολογισμό δομικών διαφορών μεταξύ των διαφορετικών εκδόσεων μιας οντολογίας (PROMPTDiff plug-in),
8)Σχολιασμός RTF εγγράφων (ONTO-H plug-in),
9)Αυτόματη εξαγωγή κλάσεων και ιδιοτήτων από συλλογές κειμένων (OntoLT plug-in).

4.1.4 Μεθοδολογίες υλοποίησης οντολογιών

Η μεθοδολογία που χρησιμοποιήσαμε για την κατασκευή της δικιάς μας οντολογίας, αναπτύσσεται αναλυτικά στην επόμενη παράγραφο. Ενδεικτικά στο σημείο αυτό αναφέρονται κάποιες υπάρχουσες μεθοδολογίες[88].

Η μεθοδολογία METHONTOLOGY είναι μια μεθοδολογία για την κατασκευή οντολογιών είτε από την αρχή, με την επαναχρησιμοποίηση άλλων οντολογιών όπως είναι ή μέσω μιας διαδικασίας επανα-κατασκευής τους. Η μεθοδολογία DILIGENT (Distributed, Loosely-controlled and evolving Engineering of oNTologies) είναι μια συνεργατική και κατανεμημένη μεθοδολογία κατασκευής οντολογιών, όπου εμπλέκονται συμμετέχοντες με διαφορετικούς στόχους και ανάγκες και οι οποίοι δεν βρίσκονται συνήθως στην ίδια τοποθεσία, οπότε απαιτείται υποστήριξη άμεσης επικοινωνίας (online). Τέλος, η μεθοδολογία On-To-Knowledge είναι μια μη-συνεργατική, εξαρτώμενη από την εφαρμογή μεθοδολογία κατασκευής οντολογιών που εστιάζει σε διαδικασίες γνώσης (knowledge

[87] Westby, J., R. (2010), "Governance of enterprise security: CyLab 2010 report", Pittsburgh, PA: Carnegie Mellon
[88] Antonucci, D. (2017), "The Cyber Risk Handbook, Creating and Measuring Effective Cybersecurity Capabilities", Published by John Wiley & Sons, Inc. Hoboken, New Jersey

processes), οι οποίες αφορούν στη χρήση των οντολογιών και μετα-διαδικασίες γνώσης (knowledge meta-processes), οι οποίες αφορούν στην καθοδήγηση για την κατασκευή τους[89].

4.2 Μεθοδολογία ανάπτυξης της οντολογίας Privacy Policy

Η μεθοδολογία που έχει χρησιμοποιηθεί ακολουθεί την φιλοσοφία της κατασκευής οντολογιών από την αρχή, η οποία βασίζεται στις ερωτήσεις επάρκειας (competency questions).

Στο σημείο αυτό θα περιγράψουμε τη μεθοδολογία που χρησιμοποιήσαμε για την κατασκευή της παρούσας οντολογίας. Η μεθοδολογία περιλαμβάνει τέσσερις κύριες φάσεις: *καθορισμός (specification)*, *εννοιολογική μορφοποίηση (conceptualization)*, *υλοποίηση (implementation)* και *αξιολόγηση (evaluation)*, κάθε μία από αυτές συνοψίζοντας διαφορετικά βήματα. Η συγκεκριμένη μεθοδολογία προκύπτει από την επεξεργασία μεθοδολογιών που ήδη υπάρχουν, όπως αυτές που είδαμε παραπάνω, οι οποίες έχουν προσαρμοστεί στις απαιτήσεις της συγκεκριμένης εργασίας. Στη συνέχεια, περιγράφουμε τα βήματα της επαναληπτικής διαδικασίας της κατασκευής της οντολογίας[90]:

Φάση του καθορισμού (Specification Phase): ασχολείται με την συλλογή των απαιτήσεων που πρέπει να πληροί η οντολογία, π.χ. λόγοι δημιουργίας, που στοχεύει, προβλεπόμενες χρήσεις.

• Βήμα 1 : Προσδιορισμός του πεδίου και του τομέα της οντολογίας

Αυτό σημαίνει τον περιορισμό των ορίων του πεδίου που καλύπτει η οντολογία.
Είναι σημαντικό βήμα για την ελαχιστοποίηση των δεδομένων και των εννοιών που θα αναλυθούν. Στο βήμα αυτό πραγματοποιήσαμε συναντήσεις με ειδικούς του συγκεκριμένου πεδίου. Οι ειδικοί αυτοί υποστηρίζουν την απόκτηση γνώσης κατά την διάρκεια ανάπτυξης της οντολογίας. Ένας άλλος τρόπος προσδιορισμού του πεδίου της οντολογίας και των βασικών της εννοιών, είναι ο σχεδιασμός μιας λίστας ερωτήσεων επάρκειας (competency questions) τις οποίες η οντολογία θα είναι σε θέση να απαντήσει. Οι ερωτήσεις αυτές στο τέλος, θα αποτελέσουν κριτήριο για την επάρκεια της οντολογίας. Στο παράρτημα

[89] Antonucci, D. (2017), "The Cyber Risk Handbook, Creating and Measuring Effective Cybersecurity Capabilities", Published by John Wiley & Sons, Inc. Hoboken, New Jersey
[90] Antonucci, D. (2017), "The Cyber Risk Handbook, Creating and Measuring Effective Cybersecurity Capabilities", Published by John Wiley & Sons, Inc. Hoboken, New Jersey

παραθέτουμε το ερωτηματολόγιο που χρησιμοποιήσαμε στις συναντήσεις με τους ειδικούς και ενδειτκτικά κάποιες από τις απαντήσεις τις οποίες λάβαμε.

• Βήμα 2 : Εξέταση επαναχρησιμοποίησης οντολογιών που ήδη υπάρχουν

Είναι σχεδόν πάντα αναγκαίο να εξεταστεί κάτι το οποίο έχει δημιουργήσει κάποιος άλλος και να ελεγχθεί αν μπορούμε να βελτιώσουμε και να επεκτείνουμε υπάρχουσες πηγές για την δική μας συγκεκριμένη εργασία. Μια διαδικασία λιγότερο χρονοβόρα και πιο βολική για τους δημιουργούς να χτίσουν μια οντολογία, είναι να ψάξουν και να επαναχρησιμοποιήσουν ήδη υπάρχουσες οντολογίες που βρίσκονται στον Ιστό, όταν κατασκευάζουν καινούργιες. Πολλές οντολογίες είναι πλέον διαθέσιμες σε ψηφιακή μορφή και μπορούν να εισαχθούν σε περιβάλλοντα μηχανικής οντολογιών που χρησιμοποιούνται για την κατασκευή νέων οντολογιών. Υπάρχουν βιβλιοθήκες επαναχρησιμοποιημένων οντολογιών στον Ιστό, όπως η βιβλιοθήκη Ontolingua (http://www.ksl.stanford.edu/software/ontolingua/), η βιβλιοθήκη DAML (http://www.daml.org/ontologies), και η βιβλιοθήκη Protégé (http://www.protege.stanford.edu/plugins/owl/owl-library/).

Η διαδικασία αυτή αποτελείται από δύο υπό-βήματα. Το πρώτο είναι η εύρεση σχετικών οντολογιών για επαναχρησιμοποίηση. Αυτό μπορεί να γίνει με την αναζήτηση συγκεκριμένων λέξεων- κλειδιών (όπως στο Swoogle), ή χρησιμοποιώντας ένα πιο σύνθετο μηχανισμό ερωτημάτων. Η διαδικασία αυτή παράγει μια λίστα από URIs οντολογιών σχετικές με τις ανάγκες του χρήστη. Παρόλα αυτά οι υπηρεσίες που προσφέρουν τέτοια εργαλεία αναζήτησης οντολογιών με βάση λέξεις-κλειδιά, όπως το Swoogle και το OntoSearch, περιορίζονται μόνο στην εύρεση και δεν υποστηρίζουν πιθανή επαναχρησιμοποίηση των οντολογιών[91].

Φάση εννοιολογικής μορφοποίησης (Conceptualization Phase): αναφέρεται στις δραστηριότητες που πραγματοποιούνται με σκοπό την οργάνωση και τη δόμηση των πληροφοριών που λαμβάνεται στην φάση του καθορισμού, σε μοντέλα που έχουν νόημα. Η φάση αυτή είναι ανεξάρτητη από τον τρόπο που θα υλοποιηθεί η οντολογία και αποτελείται από τα δύο ακόλουθα υπό-βήματα :

• Βήμα 3 : Ανάλυση της επιλεγμένης οντολογίας

[91] Antonucci, D. (2017), "The Cyber Risk Handbook, Creating and Measuring Effective Cybersecurity Capabilities", Published by John Wiley & Sons, Inc. Hoboken, New Jersey

Στο βήμα αυτό αναλύεται η επιλεγμένη οντολογία, αν υπάρχει αυτή, εξετάζοντας τις κλάσεις και τις ιδιότητές της, με σκοπό να βρεθεί τρόπος ώστε να επεκταθεί.
Όπως θα δούμε και παρακάτω στην ανάλυση των όρων της οντολογίας μας, υπάρχουν κάποιες βασικές έννοιες τις οποίες έχουμε δανειστεί από τις ήδη υπάρχουσες οντολογίες που είδαμε παραπάνω. Έτσι λοιπόν η οντολογία μας θα περιλαμβάνει την έννοια της πολιτικής (policy) που ορίζουν οι χρήστες ανάλογα με τις δικές τους ανάγκες. Επιπλέον για την περιγραφή του πλαισίου απαραίτητες είναι οι έννοιες των οντοτήτων (entity) όπου αυτές μπορεί να είναι πράκτορες (agents) ή συσκευές (devices), ενώ στην περιγραφή αυτή περιλαμβάνονται και οι ενέργειες που είναι δυνατό να λάβουν χώρα. Στην οντολογία μας οι ενέργειες αυτές αναφέρονται σαν μηχανισμοί (mechanisms).

Ακόμα στο παραπάνω πλαίσιο σημαντικό ρόλο παίζουν οι υπηρεσίες (services) που παρέχονται από τους διάφορους πόρους (resources) του συστήματος, όρους τους οποίους έχουμε δανειστεί και εμείς. Τέλος, στην οντολογίας μας περιλαμβάνονται οι έννοιες της παροχής δικαιωμάτων (authorization) και πιστοποίησης των πόρων του συστήματος (authentication).

• Βήμα 4 : Απαρίθμηση των βασικών όρων της οντολογίας

Αρχικά, είναι σημαντικό να συγκεντρωθούν διάφοροι όροι σε μια λίστα, τους οποίους θέλουμε να δηλώσουμε. Σε πρώτη φάση δημιουργούμε ορισμούς των εννοιών, χωρίζοντάς τους σε μια ιεραρχία και στη συνέχεια περιγράφουμε τις ιδιότητες των εννοιών αυτών, οι οποίες παρέχουν και τους βασικούς περιορισμούς και τις σχέσεις μεταξύ των εννοιών. Το βήμα αυτό είναι το πιο σημαντικό στην διαδικασία σχεδιασμού της οντολογίας γιατί περιλαμβάνει μηχανισμούς αποφάσεων σχετικά με τη γενική δομή της οντολογίας και κατά πόσο αυτή θα είναι λεπτομερής όσο αφορά το πεδίο που περιγράφει. Χωρίζεται σε τρία υπό-βήματα: (1) ορισμός και ιεραρχία των κλάσεων, (2) ορισμός σχέσεων και ιδιοτήτων των κλάσεων και (3) ορισμός των στιγμιότυπων. Στο πρώτο υπό-βήμα, για τον ορισμό της ιεραρχίας των κλάσεων, υπάρχουν τρείς προσεγγίσεις: ανάπτυξη από πάνω προς τα κάτω (top-down), που ξεκινά με τον ορισμό των πιο γενικών εννοιών του πεδίου και μετέπειτα εξειδίκευση των εννοιών, ανάπτυξη από κάτω προς τα πάνω (bottom-up), που ξεκινά με τον ορισμό των πιο εξειδικευμένων κλάσεων και μετέπειτα ομαδοποίηση αυτών σε πιο γενικές έννοιες και την από μέσα προς τα έξω ανάπτυξη (middle-out), όπου ορίζουμε τις πιο προεξέχουσες έννοιες και έπειτα τις γενικεύουμε και εξειδικεύουμε κατάλληλα. Η επιλογή της προσέγγισης εξαρτάται άμεσα από την προσωπική άποψη του ειδικού του πεδίου, καθώς

δεν υπάρχει κανένας σωστός τρόπος για τον ορισμό της ιεραρχίας για κάποιο πεδίο. Στη δική μας περίπτωση ακολουθήσαμε τη δεύτερη προσέγγιση[92].

Υποβολή 1 : Ορισμός και Ιεραρχία κλάσεων

Στο πρώτο επίπεδο η οντολογία μας αποτελείται από τις κλάσεις:

- *Mechanism*: Το σύνολο των μηχανισμών (ενεργειών) που είναι δυνατό να πραγματοποιηθούν μέσα στο πλαίσιο του διάχυτου υπολογισμού και αφορούν κυρίως τα δεδομένα
- *PolicyMechanisms*: Οι μηχανισμοί (ενέργειες) που είναι απαραίτητοι για την υλοποίηση μιας πολιτικής
- *Resource*: Το σύνολο των πόρων ενός συστήματος διάχυτου υπολογισμού
- *User*: Οι χρήστες του πλαισίου
- *ID*: Το σύνολο των ταυτοτήτων των οντοτήτων του συστήματος. Μια ταυτότητα αποτελείται από ένα σύνολο τιμών που κατέχει μια οντότητα ή χρήστης και της επιτρέπει να διαχωρίζεται από κάποια άλλη οντότητα/χρήστη και από τις οντότητες:
- *Policy*: Το σύνολο των πολιτικών που ορίζουν οι χρήστες του συστήματος με βάση τις ανάγκες τους.
- *Time*: Η έννοια του χρόνου, όπου θα μας χρειαστεί για να απαντήσουμε σε ερωτήματα π.χ. πόσο διαρκεί η αποθήκευση κάποιων δεδομένων ή μια πολιτική.
- *TrustLevel*: Το επίπεδο εμπιστοσύνης που διαθέτει ένας χρήστης ή ένα σύνολο χρηστών

Πιο αναλυτικά[93]:

Η κλάση Mechanism

[92] Antonucci, D. (2017), "The Cyber Risk Handbook, Creating and Measuring Effective Cybersecurity Capabilities", Published by John Wiley & Sons, Inc. Hoboken, New Jersey
[93] Westby, J., R. (2010), "Governance of enterprise security: CyLab 2010 report", Pittsburgh, PA: Carnegie Mellon

- *DataProcessing*: Η επεξεργασία των δεδομένων που αποτελεί ουσιαστικά και το σύνολο των ενεργειών που μπορούν να πραγματοποιηθούν στο σύστημα και αφορούν τα δεδομένα.
- *DataCollection*: Συλλογή των δεδομένων. διάφορες οντότητες ή υπηρεσίες συλλέγουν πληροφορίες από ένα άτομο. Οι πληροφορίες που συλλέγονται θα πρέπει να καταγράφονται σα να είναι συνδεδεμένες με το άτομο προκειμένου να διασφαλιστεί ότι οι πληροφορίες ανήκουν σε αυτά τα άτομα.
- *DataTransfer*: Μεταφορά των δεδομένων. Κατά τη μεταφορά των δεδομένων πρέπει να διασφαλιστεί η υπευθυνότητα από κάθε μέρος που συμμετέχει στη μεταφορά. Επιπλέον η μεταφορά ευαίσθητων δεδομένων πρέπει να αποφεύγεται εκτός αν είναι αναγκαία για μια υπηρεσία που έχει ζητήσει ένα άτομο.,
- *DataStorage*: Αποθήκευση δεδομένων. Τα δεδομένα αποθηκεύονται σε διαφορετικές μορφές και σε πολλά διαφορετικά μέρη. Η αποθήκευση ευαίσθητων προσωπικών δεδομένων θα πρέπει να αποφεύγεται όταν δεν είναι απολύτως απαραίτητη και θα πρέπει να αποθηκεύεται με τέτοιο τρόπο ώστε να αναγνωρίζονται σαν ευαίσθητα προσωπικά δεδομένα.
- *DataArchive*: Η αρχειοθέτηση των δεδομένων απαιτεί μεγάλη προσοχή κυρίως όταν αφορά προσωπικά δεδομένα. Οι αρχές της ιδιωτικότητας ορίζουν ότι τα προσωπικά δεδομένα πρέπει να διατηρούνται μόνο τόσο όσο χρειάζεται για να εξυπηρετήσουν ένα συγκεκριμένο σκοπό.
- *DataUse*: Η χρήση των δεδομένων μπορεί να σημαίνει πολλά πράγματα. Η πρόσβαση σε δεδομένα (*DataAccess*), η αποκάλυψη δεδομένων (*DataDisclosure*), και η τροποποίηση των δεδομένων (*DataModification*). Ειδικά η τροποποίηση των δεδομένων μπορεί να αφορά την προσθήκη νέων δεδομένων (*DataAdd*) ή τη διαγραφή κάποιων δεδομένων (*DataDelete*). Επιπλέον η τροποποίηση μπορεί να αφορά τη διόρθωση κάποιων δεδομένων (*DataCorrect*) ή την ανωνυμοποίηση δεδομένων προσωπικού χαρακτήρα (*DataAnonymization*).
- *DataDispose*: Στη φάση αυτή τα δεδομένα διαγράφονται, μετατρέπονται σε ανώνυμα, να αρχειοθετηθούν ή να τα ξεφορτωθούμε με κάποιο τρόπο. Εδώ σημειώνεται ότι η διαγραφή των δεδομένων δε σημαίνει απαραίτητα ότι ξεφορτωνόμαστε οριστικά τα δεδομένα αφού σε συστήματα πληροφοριών τα διαγραμμένα δεδομένα μπορούν να ανακτηθούν.

Η κλάση PolicyMechanisms

- *PolicyMechanisms*: Οι μηχανισμοί (ενέργειες) που απαιτούνται για την υλοποίηση της πολιτικής που ορίζει ένας χρήστης.
- *Identification*: Αναγνώριση κάποιας οντότητας ή χρήστη με βάση κάποιες μοναδικές αναφορές ταυτότητας και/ή πρόσθετες πληροφορίες που χαρακτηρίζουν την οντότητα αυτή.
- *Authorization*: Είναι το δικαίωμα που δίνει ο κάτοχος ενός πόρου σε κάποιο άλλο χρήστη ώστε να μπορέσει να τον χρησιμοποιήσει.
- *Encryption*: Η χρήση κρυπτογράφησης κατά την αποθήκευση ή μεταφορά των δεδομένων.
- *Authentication*: Η επαλήθευση της ταυτότητας κάποιας οντότητας ή χρήστη με βάση κάποια ταυτότητα ή άλλο πιστοποιητικό. Η επαλήθευση αυτή ανάλογα με το αποτέλεσμά της διακρίνεται σε θετική (*PositiveAuthentication*) ή αρνητική (*NegativeAuthentication*)[94].

Η κλάση Resource

- *Entity*: Κάτι που έχει μια ξεχωριστή και διακριτή ύπαρξη. Για παράδειγμα ένας πράκτορας (*Agent*) ή μια συσκευή (*Device*).
- *Data*: Είναι το σύνολο των δεδομένων τα οποία βρίσκονται αποθηκευμένα μέσα σε κάποιο πλαίσιο. Συνήθως αποθηκεύονται μέσα σε κάποια οντότητα. _ιακρίνονται σε προσωπικά δεδομένα (*PersonalData*) ή δημόσια (*PublicData*). Επιπλέον τα προσωπικά δεδομένα ενός χρήστη ανάλογα με το πόσο σημαντικά θεωρούνται γι΄αυτόν, διακρίνονται σε ευαίσθητα (*SensitiveData*) ή μη-ευαίσθητα (*NonSensitiveData*).
- *Service*: Είναι το σύνολο των υπηρεσιών που παρέχονται από κάποιες συσκευές μέσα σε κάποιο πλαίσιο. Ανάλογα με το αν κάποια οντότητα λαμβάνει ή παρέχει κάποια υπηρεσία, διακρίνονται σε παρεχόμενες υπηρεσίες (*ServiceProvided*) ή ληφθείσες (*ServiceReceived*)[95].

Η κλάση User

[94] Westby, J., R. (2010), "Governance of enterprise security: CyLab 2010 report", Pittsburgh, PA: Carnegie Mellon
[95] Westby, J., R. (2010), "Governance of enterprise security: CyLab 2010 report", Pittsburgh, PA: Carnegie Mellon

- *User*: Το σύνολο όλων των χρηστών μέσα σε κάποιο πλαίσιο. Οι χρήστες διακρίνονται σε πελάτες (*Client*) και είναι αυτοί που ζητούν πρόσβαση σε δεδομένα και γενικότερα τη χρήση κάποιου πόρου ή υπηρεσίας. διακρίνονται σε άτομα (*Individual*) ή ομάδες ατόμων (*Group*).
- *ResourceOwner*: Το σύνολο των χρηστών που κατέχουν κάποιο πόρο[96].

Η κλάση ID

- *IdentifiedID*: Η ταυτότητα ενός χρήστη η οποία είναι εγγεγραμμένη και αναγνωρίζεται από τον πόρο στον οποίο θέλει να έχει πρόσβαση ο χρήστης.
- *NonIdentifiedID*: Η ταυτότητα ενός χρήστη η οποία δεν ταυτοποιείται από το συγκεκριμένο πόρο στον οποίο επιθυμεί πρόσβαση ο χρήστης.
- *AnonymousID*: Η ταυτότητα ενός χρήστη που δεν έχει κάποια τιμή. Μπορεί να χρησιμοποιηθεί σε περιπτώσεις όπου ο χρήστης δε θέλει να αναγνωριστεί (π.χ. σαν guest σε κάποια υπηρεσία).
- *AuthenticatedID*: Η ταυτότητα του χρήστη η οποία επαληθεύεται μετά την αναγνώρισή της. Δηλαδή ο πόρος επαληθεύει την ταυτότητα του χρήστη που έχει τη συγκεκριμένη ταυτότητα και επομένως αποκτά πρόσβαση στον πόρο αυτό.
- *NonAuthenticatedID*: Η ταυτότητα ενός χρήστη η οποία ενώ έχει πρώτα αναγνωριστεί από τον πόρο, δε μπορεί στη συνέχεια να πιστοποιηθεί ότι πράγματι πρόκειται για τον χρήστη που τη χρησιμοποιεί. Έτσι ο χρήστης δεν αποκτά πρόσβαση στον πόρο.
- *AuthorizedID*: Η ταυτότητα του χρήστη, όπου αφού αναγνωρισθεί και πιστοποιηθεί από τον πόρο έχει δικαιώματα σε κάποιο μηχανισμό για το συγκεκριμένο πόρο.
- *NonAuthorizedID*: Η ταυτότητα του χρήστη, όπου αφού αναγνωρισθεί και πιστοποιηθεί από τον πόρο δεν έχει δικαιώματα σε κάποιο συγκεκριμένο μηχανισμό για το συγκεκριμένο πόρο[97].

Υποβολή 2 : Ορισμός σχέσεων και ιδιοτήτων των κλάσεων

Το δεύτερο υπό-βήμα αφορά τον ορισμό των ιδιοτήτων των κλάσεων, καθώς επίσης και τους περιορισμούς πάνω στις ιδιότητες αυτές. Οι κλάσεις από μόνες τους δεν παρέχουν αρκετές πληροφορίες για να απαντηθούν οι ερωτήσεις επάρκειας της πρώτης φάσης, οι

[96] Westby, J., R. (2010), "Governance of enterprise security: CyLab 2010 report", Pittsburgh, PA: Carnegie Mellon
[97] Westby, J., R. (2010), "Governance of enterprise security: CyLab 2010 report", Pittsburgh, PA: Carnegie Mellon

οποίες αναφέρονται στο Παράρτημα. Αφού έχουμε ορίσει μερικές από τις κλάσεις, πρέπει πρώτα να περιγράψουμε την εσωτερική δομή των εννοιών, ορίζοντας δηλαδή ιδιότητες για κάθε έννοια και επίσης περιορισμούς στις ιδιότητες αυτές (data properties), και μετά πρέπει να ορίσουμε σχέσεις μεταξύ των διαφορετικών κλάσεων (object properties). Παρακάτω βλέπουμε τον πίνακα των σχέσεων (ιδιοτήτων) που συνδέουν τις κλάσεις (Domain και Range) καθώς και η περιγραφή τους (description)[98]:

Παράδειγμα κλάσεων με τα στιγμιότυπά τους στο Protégé[99]:

Φάση της υλοποίησης (Implementation Phase): αναφέρεται στις δραστηριότητες που αφορούν την παραγωγή υπολογίσιμων μοντέλων, σύμφωνα με το συντακτικό μιας τυπικής γλώσσας αναπαράστασης (π.χ. OWL), μετά την επιλογή του περιβάλλοντος ανάπτυξης της οντολογίας (π.χ. Protégé), στο οποίο θα αναπτυχθεί η οντολογία μας. Παρακάτω θα δούμε κάποιες εικόνες με τις κλάσεις, υποκλάσεις και τις ιδιότητες των κλάσεων όπως αυτές αναπαριστώνται στο εργαλείο Protégé.

Φάση της αξιολόγησης (Evaluation Phase): αναφέρεται στις δραστηριότητες ελέγχου της γενικής και τεχνικής ποιότητας της οντολογίας σύμφωνα με κάποια προκαθορισμένα κριτήρια. Η γενική ποιότητα μιας οντολογίας βασίζεται στην αξιολόγηση απέναντι σε κριτήρια όπως: η κάλυψη ενός συγκεκριμένου πεδίου, η πολυπλοκότητα και η πληρότητα αυτής της κάλυψης, συγκεκριμένες περιπτώσεις χρήσεων, σενάρια, απαιτήσεις, και εφαρμογές για τις οποίες αναπτύχθηκε. Η τεχνική ποιότητα επικεντρώνεται στη συνέπεια, τη σαφήνεια, ακρίβεια κλπ. Πρακτικά, αφού ορίσουμε μια αρχική έκδοση της οντολογίας, μπορούμε να την αξιολογήσουμε χρησιμοποιώντας την σε εφαρμογές, ή συζητώντας την με κάποιους ειδικούς του χώρου. Η αξιολόγηση της οντολογίας πρέπει να γίνει σε δύο στάδια: στο στάδιο της μοντελοποίησης, όπου ο σχεδιαστής της οντολογίας, σε τακτά διαστήματα, αποφασίζει να ελέγξει την ποιότητα της δουλειάς που έχει γίνει μέχρι τώρα, και μετά την έκδοση της οντολογίας. δηλαδή η αξιολόγηση είναι μια διάχυτη διαδικασία στην διάρκεια ανάπτυξης της οντολογίας[100].

[98] Westby, J., R. (2010), "Governance of enterprise security: CyLab 2010 report", Pittsburgh, PA: Carnegie Mellon
[99] Zerlang, J. (2017), "GDPR: a milestone in convergence for cybersecurity and compliance", Network Security, 17 (6), pp. 8-11
[100] Zerlang, J. (2017), "GDPR: a milestone in convergence for cybersecurity and compliance", Network Security, 17 (6), pp. 8-11

Η συνολική ποιότητα μιας οντολογίας μπορεί να προσδιοριστεί συγκρίνοντας την οντολογία με ένα "χρυσό πρότυπο" (golden standard) που μπορεί να είναι το ίδιο μια οντολογία, στη χρήση της οντολογίας σε μια εφαρμογή και την αξιολόγηση των αποτελεσμάτων, κάνοντας συγκρίσεις με μια πηγή δεδομένων (π.χ. μια συλλογή κειμένων) σχετικά με το πεδίο που καλύπτει η οντολογία, ζητώντας από ανθρώπους να αξιολογήσουν πόσο καλά η οντολογία πληροί μια σειρά από προκαθορισμένα κριτήρια, προδιαγραφές και απαιτήσεις [62]. Επιπλέον η τεχνική ποιότητα της οντολογίας εξαρτάται από τη συνοχή (πόσες έννοιες της οντολογίας εμπλέκονται σε αντιφάσεις), τη σαφήνεια (αν οι όροι που χρησιμοποιούνται στην οντολογία έχουν πολλές σημασίες), την ακρίβεια (ποσοστό των ψευδών δηλώσεων στην οντολογία), τον έλεγχο της σχετικότητας (ο αριθμός των δηλώσεων που περιέχουν συντακτικά χαρακτηριστικά τα οποία χαρακτηρίζονται σαν χρήσιμα ή αποδεκτά από το χρήστη), δηλαδή, τις σχεδιαστικές παραμέτρους που πρέπει να καλυφθούν κατά την ανάπτυξη μιας οντολογίας καλής ποιότητας . Στην πράξη κάποιος σχεδόν βέβαια θα πρέπει να αναθεωρήσει την αρχική οντολογία.

Ειδικότερα, εμείς έχουμε αξιολογήσει την τεχνική ποιότητα της οντολογίας μας,χρησιμοποιώντας τη μηχανή συλλογιστικής ανάλυσης Pellet (Pellet reasoner), κατά τη διάρκεια του σταδίου της μοντελοποίησης, και την συνολική ποιότητα της οντολογίας με τη χρήση των ερωτήσεων επάρκειας[101].

Επιπλέον από τη χρήση των ερωτήσεων επάρκειας και τη μηχανή συλλογιστικής ανάλυσης η οποία εξασφαλίζει τη συνέπεια της οντολογίας, η σαφήνεια και η αντικειμενικότητα της οντολογίας εξασφαλίζεται από τις συναντήσεις με τους ειδικούς του πεδίου, οι οποίες πραγματοποιήθηκαν στο στάδιο κατασκευής της οντολογίας. Ταυτόχρονα με τη σαφήνεια, οι παρατηρήσεις των ειδικών του πεδίου εξασφαλίζουν και την επάρκεια αλλά και πληρότητα των εννοιών που έχουν χρησιμοποιηθεί στην οντολογία με τη μορφή των κλάσεων. Δηλαδή, οι έννοιες της οντολογίας μπορούν να περιγράψουν επαρκώς ένα περιβάλλον περιρρέουσας νοημοσύνης καθώς και πολιτικές ιδιωτικότητας μέσα σε ένα τέτοιο περιβάλλον. Αντίστροφα, ένα περιβάλλον περιρρέουσας νοημοσύνης και μια πολιτική ιδιωτικότητας για μια εφαρμογή σε ένα τέτοιο περιβάλλον μπορεί να περιγραφεί πλήρως από τις έννοιες που περιλαμβάνονται στην οντολογία.

[101] Zerlang, J. (2017), "GDPR: a milestone in convergence for cybersecurity and compliance", Network Security, 17 (6), pp. 8-11

Εκτός από τις συναντήσεις που πραγματοποιήθηκαν με τους ειδικούς του πεδίου, για τη συνολική ποιότητα της οντολογίας έγινε σύγκριση με την οντολογία SOUPA, την οποία είδαμε σε προηγούμενο κεφάλαιο, σαν το "χρυσό πρότυπο". Έτσι, τόσο στην προτεινόμενη οντολογία όσο και στην SOUPA υπάρχουν έννοιες που αφορούν τους χρήστες ή το σύνολο των ανθρώπων (User και Person αντίστοιχα). Επιπλέον και στις δύο οντολογίες περιλαμβάνονται έννοιες που αφορούν το σύνολο των ενεργειών (Mechanism και Action), τις πολιτικές (Policy) και το χρόνο (Time)[102].

Η συγκεκριμένη οντολογία έχει ακόμη χρησιμοποιηθεί ως μέρος του προγράμματος ATRACO Project, για την περιγραφή πολιτικών ιδιωτικότητας που μπορούν να εφαρμοστούν σε εφαρμογές διάχυτου υπολογισμού που υποστηρίζουν δραστηριότητες των χρηστών, με ικανοποιητικά αποτελέσματα. Ένα από τα μεγαλύτερα πλεονεκτήματα της οντολογίας είναι ότι έχει κατασκευαστεί με τέτοιο τρόπο ώστε να είναι δυνατή η επέκταση αλλά και εξειδίκευσή της ως προς τα στιγμιότυπα και τις έννοιες που εμπεριέχονται σε αυτή. Ακόμη μπορεί εύκολα να συγχωνευτεί με άλλες οντολογίες που αφορούν πόρους ενός περιβάλλοντος περιρρέουσας νοημοσύνης απαντώντας με αυτό τον τρόπο σε περισσότερα και πιο σύνθετα ερωτήματα που αφορούν το συγκεκριμένο πεδίο[103].

[102] Ulsch, M. (2014), "Cyber Threat! How to manage the growing risk of cyber attacks", Published by John Wiley & Sons, Ltd.
[103] Ulsch, M. (2014), "Cyber Threat! How to manage the growing risk of cyber attacks", Published by John Wiley & Sons, Ltd.

Κεφάλαιο 5. Συμπεράσματα-προτάσεις για το μέλλον

Όσον αφορά το Γενικό Κανονισμό Προστασίας Δεδομένων, διαφαίνεται ότι, σε γενικές γραμμές, η επιστημονική κοινότητα συντάσσεται με την άποψη ότι πρόκειται περί ενός γόνιμου μέτρου και μιας προσπάθειας της Ευρωπαϊκής Ένωσης, προς την θετική κατεύθυνση, για την αποτελεσματικότερη και πιο αυστηρή προστασία της αξίας των προσωπικών δεδομένων των Ευρωπαίων χρηστών του διαδικτύου. Παρόλα αυτά, η υποχρεωτική εφαρμογή του Κανονισμού, αρχής γενομένης τον Μάιο του 2018, φανέρωσε τα οργανικά προβλήματα και την έλλειψη της απαραίτητης οργάνωσης ορισμένων επιχειρήσεων, πολλές εκ των οποίων είτε δεν αντιλήφθηκαν εγκαίρως τη βαρύτητά του, είτε θεώρησαν ότι πρόκειται για ακόμα μια πηγή επιπρόσθετου κόστους (δίχως κάποιο επιπρόσθετο όφελος για τις ίδιες) και κατά συνέπεια προσπάθησαν απλώς να τον αγνοήσουν (κάτι το οποίο φυσικά δεν καθίσταται εύκολο). Το μόνο βέβαιο είναι ότι απαιτείται επιπρόσθετος χρόνος και περισσότερα στοιχεία προκειμένου να αξιολογηθούν πληρέστερα οι επιπτώσεις του GDPR, καθώς και η ευεργετική του (ή μη) συνδρομή προς την προστασία των προσωπικών δεδομένων, ενώ είναι δεδομένο ότι στα επόμενα χρόνια, η επιστημονική έρευνα θα εστιάσει ακόμα πιο πολύ προς αυτή τη κατεύθυνση.

Σχετικά με τους κινδύνους του κυβερνοχώρου, θα μπορούσαμε να πούμε ότι η τρέχουσα εικόνα μαρτυράει μόνο δυσοίωνα στοιχεία για το μέλλον και τις επιπτώσεις τους. Πρόκειται για μια μορφή κινδύνων που έχει εξελιχθεί ραγδαία, κατά τη τελευταία 15ετία, σκαρφαλώνοντας πλέον στην κορυφή της λίστας μεταξύ των πιο σημαντικών κινδύνων που απειλούν, τόσο τις επιχειρήσεις, όσο και τους μεμονωμένους ιδιώτες, στο σύνολο της παγκόσμιας οικονομίας. Η ραγδαία ανάπτυξη της τεχνολογίας και των πολύπλοκων πληροφοριακών συστημάτων, έχει οδηγήσει σε μια παράλληλη αύξηση, όχι μόνο των κρουσμάτων επιθέσεων στον παγκόσμιο κυβερνοχώρο, αλλά και της σοβαρότητας των κινδύνων αυτών, καθώς και των δυνητικών ευπαθειών των πληροφοριακών συστημάτων απέναντι στους κινδύνους αυτούς. Σύμφωνα μάλιστα με ορισμένες πρόσφατες εκτιμήσεις, το κόστος που συνεπάγονται οι κίνδυνοι του κυβερνοχώρου ανέρχεται έως και τα 600 δις. δολάρια, παγκοσμίως. Ενδιαφέρον ωστόσο έχει η παρατήρηση ότι ενώ η πλειοψηφία των επιχειρήσεων, έως και πριν μια δεκαετία, δεν απέδιδε στους κινδύνους του κυβερνοχώρου την απαιτούμενη αναγνώριση, ως προς τις δυνητικές τους συνέπειες και τις επιπτώσεις τους, σήμερα η κατάσταση έχει αντιστραφεί σε πολύ μεγάλο βαθμό. Πλέον, οι προσπάθειες

στρέφονται προς την πιο αποτελεσματική και επαγγελματική διαχείριση των κινδύνων αυτών, ενώ τα δεκάδες ηχηρά παραδείγματα παραβιάσεων εταιρικών πληροφοριακών συστημάτων έχουν ευαισθητοποιήσει την παγκόσμια επιχειρηματική κοινότητα προς την ανάληψη των ευθυνών της για την βελτίωση των εταιρικών δομών και τη θωράκισή τους έναντι αυτής της μορφής των κινδύνων.

Η ραγδαία αύξηση των κινδύνων του κυβερνοχώρου (τόσο σε απόλυτα μεγέθη, όσο και σε βαρύτητα των καταγεγραμμένων περιστατικών παραβιάσεων), έχει οδηγήσει στην άνθιση του επαγγέλματος της ασφάλισης έναντι των κινδύνων αυτών. Για τις επιχειρήσεις, αυτό αποτελεί μια επιπρόσθετη επιλογή για τον σχεδιασμό του βέλτιστου προγράμματος διαχείρισης των εταιρικών κινδύνων. Τα κύρια ζητήματα που αντιμετωπίζουν οι ασφαλιστικές εταιρίες επικεντρώνονται στην έλλειψη ιστορικών δεδομένων και στη δυσκολία μοντελοποίησης των υφιστάμενων δεδομένων λόγω της εξελισσόμενης φύσης των κινδύνων στον κυβερνοχώρο. Επιπρόσθετα ζητήματα όπως η ασυμμετρία της πληροφόρησης και ο ηθικός κίνδυνος που συνεπάγεται το κάθε ασφαλιστικό εγχείρημα, φαίνεται ότι δυσχεραίνουν ακόμα περισσότερο, την ήδη περίπλοκη εικόνα που παρουσιάζει αυτή η αγορά. Παρόλα αυτά, η εικόνα για το μέλλον της ασφάλισης έναντι των κινδύνων του κυβερνοχώρου φαίνεται ιδιαίτερα ενθαρρυντική, δεδομένου ότι αποτελεί κοινή γνώμη ότι υπάρχει τεράστιο περιθώριο ανάπτυξης.

Μια εκ των βασικών διαπιστώσεών μας κατά την επισκόπηση των πηγών που χρησιμοποιήθηκαν για την συγγραφή της παρούσας εργασίας ήταν ότι η υφιστάμενη έρευνα στον τομέα των κινδύνων του κυβερνοχώρου και της ασφάλισης έναντι αυτών επικεντρώνεται κυρίως στην πλευρά της προσφοράς, δηλαδή εξετάζει το θέμα δυσανάλογα περισσότερο από την οπτική των ασφαλιστικών εταιριών. Η πλευρά της ζήτησης – δηλαδή των επιχειρήσεων που καλούνται να αντιμετωπίσουν τους κινδύνους που απειλούν τα πληροφοριακά τους συστήματα, καθώς και να αποφασίσουν το εάν θα αναζητήσουν την συνδρομή της ασφαλιστικής κάλυψης έναντι των κινδύνων αυτών - ωστόσο, μπορεί να προσελκύσει εξίσου σημαντικό ερευνητικό ενδιαφέρον στο μέλλον.

Πιο συγκεκριμένα, προτείνουμε την εξέταση του αντιληπτού επιπέδου της σοβαρότητας των κινδύνων του κυβερνοχώρου. Μια τέτοια έρευνα θα μπορούσε να αναδείξει τα όποια προβλήματα και τις γνωστικές ελλείψεις του επιχειρηματικού κόσμου αναφορικά με την έκταση και την βαρύτητα των κινδύνων του κυβερνοχώρου, καθώς επίσης και να αναδείξει τη σημασία της ασφάλισης έναντι των κινδύνων αυτών.

Επιπρόσθετα ζητήματα όπως η διερεύνηση των συνθηκών που δημιουργούν ένα ευνοϊκότερο κλίμα προς την αναζήτηση των ασφαλιστικών υπηρεσιών για την κάλυψη των κινδύνων του κυβερνοχώρου, η εξέταση των πιθανών τρόπων και μέσων βελτίωσης της αυτοπροστασίας έναντι των κινδύνων αυτών, καθώς και η εύρεση της ισορροπίας μεταξύ των ποικίλων τεχνικών διαχείρισης των εταιρικών κινδύνων προκειμένου να προταθεί ένα βέλτιστο μίγμα πολιτικής, θα μπορούσαν να αποτελέσουν έμπνευση για μελλοντική έρευνα.

Η εξέταση των υπαρχόντων μεθόδων μοντελοποίησης του ρίσκου που εγκυμονεί η ανάληψη της ασφαλιστικής κάλυψης έναντι συγκεκριμένων κινδύνων του κυβερνοχώρου, καθώς και η διασύνδεσή τους με τις τελευταίες εξελίξεις της τεχνολογίας, είναι ένα ακόμα θέμα που μπορεί να διερευνηθεί μελλοντικά. Παραδείγματος χάριν, ποια θα μπορούσε να είναι η ευθύνη της ασφαλιστικής εταιρίας απέναντι σε κρούσματα παραβίασης των πληροφοριακών συστημάτων των νέων «έξυπνων αυτοκινήτων» τα οποία καθοδηγούνται από προγράμματα τεχνητής νοημοσύνης (Artificial Intelligence – AI).

Βιβλιογραφία

Ελληνική

- Γαμπά, Δ., (2018). Σημειώσεις: Παραβίαση της Ασφάλειας των Προσωπικών Δεδομένων
- Αλεξανδροπούλου-Αιγυπτιάδου, Ε., (2016). Προσωπικά Δεδομένα, Νομική Βιβλιοθήκη
- Κοτσαλής, Λ., (2016). Προσωπικά Δεδομένα, Ανάλυση-Σχόλια-Εφαρμογή, Νομική Βιβλιοθήκη
- Κοτσαλής, Λ., Μενουδάκος, Κ., (2018). Γενικός Κανονισμός για την Προστασία Προσωπικών Δεδομένων GDPR, Νομική Βιβλιοθήκη
- Μυρτίδης, Δ., (2008). Μέσα Τραπεζικής Εργασίας, Τραπεζική Πληροφορική, τόμος Β, ΕΑΠ, Πάτρα

Ξένη

- Allianz Global Corporate Specialty. (2015), "A Guide to Cyber Risk"
- Anderson, R. and Moore, T. (2006), "The Economics of Information Security", Science, 314 (5799), pp. 610-613
- Antonucci, D. (2017), "The Cyber Risk Handbook, Creating and Measuring Effective Cybersecurity Capabilities", Published by John Wiley & Sons, Inc. Hoboken, New Jersey
- Baer, W. S. and Parkinson, A. (2007), "Cyberinsurance in IT Security Management," IEEE Security and Privacy, 5 (3), pp. 50–56
- Tikkinen-Piri, C., Rohunen, A. and Markulla, J. (2018), "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", Computer Law & Security Review, 34 (1), pp. 134-153
- Ulsch, M. (2014), "Cyber Threat! How to manage the growing risk of cyber attacks", Published by John Wiley & Sons, Ltd.
- Wachter, S. (2018), "Internet of Things: Privacy, profiling, discrimination, and the GDPR", Computer Law & Security Review, 34 (3), pp. 436-449
- Westby, J., R. (2010), "Governance of enterprise security: CyLab 2010 report", Pittsburgh, PA: Carnegie Mellon
- Zerlang, J. (2017), "GDPR: a milestone in convergence for cybersecurity and compliance", Network Security, 17 (6), pp. 8-11

Ηλεκτρονική

- Ανακοινώσεις Τραπεζών Μελών https://www.hba.gr/Media/Details/358
- ΑΠΔΠΧ, Χρηματοπιστωτικά, Σημαντικά αρχεία http://www.dpa.gr/portal/page?_pageid=33,124336&_dad=portal&_schema=PORTAL
- Απόρρητο και το Ψηφιακό Μέλλον, 2018, http://oecdobserver.org/news/fullstory.php/aid/6040/Privacy_and_your_digital_future
- Ασφάλεια Πληροφοριακών Συστημάτων https://el.wikipedia.org/wiki
- Ασφάλεια πληροφοριών και Κυβερνοέγκλημα https://lawandtech.eu/sectors/cybercrime_infosec/
- Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) https://pofee.gr/images/books/GDPR-pofee-april2018.pdf
- Εθνική Τράπεζα της Ελλάδος, Δήλωση προστασίας δεδομένων προσωπικού χαρακτήρα nbg-privacy_statement.pdf
- Ένας χρόνος εφαρμογής του GDPR. Τι έγινε, τι θα γίνει, τι πρέπει να γίνει, 2019 http://www.epixeiro.gr/article/126595
- Ένα έτος GDPR – Απογραφή https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en
- Ενημέρωση των πελατών της Attica Bank για την επεξεργασία των προσωπικών τους δεδομένων σύμφωνα με τον Κανονισμό (ΕΕ) 2016/679 και τη συναφή Ελληνική Νομοθεσία GDPR_ATTICA-BANK_gr.pdf
- Έντυπο ενημέρωσης για την επεξεργασία προσωπικών δεδομένων σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 και τη σχετική Ελληνική Νομοθεσία gdpr_A.indd=EUROBANK
- ΕΕΔΑ, Κατάλογος Διεθνών και Ευρωπαϊκών Συμβάσεων για τα Δικαιώματα του Ανθρώπουhttp://www.antigone.gr/files/gr/library/educationalmaterial/katalogos%20diethnon%20kai%20evropaikon%20symvaseon.pdf

Παράρτημα

ΕΛΛΗΝΙΚΗ ΝΟΜΟΛΟΓΙΑ

1)Απόφαση μονομελούς πρωτοδικείου Αθηνών

Στην απόφαση αυτή το μονομελές πρωτοδικείο Αθηνών δέχθηκε ότι:

1. Σύμφωνα με το άρθρο 4 του Ν.2472/1997 τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει:

α) Να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών β) Να είναι συναφή, πρόσφορα και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας.

2. Σύμφωνα με το άρθρο 7 § 2 περ. α΄ του Ν.2472/1997. Κατ' εξαίρεση επιτρέπεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων, καθώς και η ίδρυση και λειτουργία σχετικού αρχείου, ύστερα από άδεια της Αρχής, όταν το υποκείμενο έδωσε τη γραπτή συγκατάθεσή του.

3.Σύμφωνα με το άρθρο 7Α § 1 περ. α΄ του Ν.2472/1997 Ο υπεύθυνος επεξεργασίας απαλλάσσεται από την υποχρέωση γνωστοποίησης του άρθρου 6 και από την υποχρέωση λήψης άδειας του άρθρου 7 του παρόντος νόμου όταν η επεξεργασία πραγματοποιείται αποκλειστικά για σκοπούς που συνδέονται άμεσα με σχέση εργασίας ή έργου ή με παροχή υπηρεσιών στο δημόσιο τομέα και είναι αναγκαία για την εκπλήρωση υποχρέωσης που επιβάλλει ο νόμος ή για την εκτέλεση των υποχρεώσεων από τις παραπάνω σχέσεις και το υποκείμενο έχει προηγουμένως ενημερωθεί.

4. Σύμφωνα με το άρθρο 13 § 1 του Ν.2472/1997 Το υποκείμενο των δεδομένων έχει δικαίωμα να προβάλλει οποτεδήποτε αντιρρήσεις για την επεξεργασία δεδομένων που το αφορούν. Οι αντιρρήσεις απευθύνονται εγγράφως στον υπεύθυνο επεξεργασίας και πρέπει να περιέχουν αίτημα για συγκεκριμένη ενέργεια, όπως διόρθωση, προσωρινή μη χρησιμοποίηση, δέσμευση, μη διαβίβαση ή δια- γραφή. Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να απαντήσει εγγράφως επί των αντιρρήσεων μέσα σε αποκλειστική προθεσμία δεκαπέντε (15) ημερών. Στην απάντησή του οφείλει να ενημερώσει το υποκείμενο για τις ενέργειες στις οποίες προέβη ή, ενδεχομένως, για τους λόγους που δεν ικανοποίησε το αίτημα.

5. Σύμφωνα με το άρθρο 13 § 2 του Ν.2472/1997 Εάν ο υπεύθυνος επεξεργασίας δεν απαντήσει εμπροθέσμως ή η απάντησή του δεν είναι ικανοποιητική, το υποκείμενο των δεδομένων έχει δικαίωμα να προσφύγει στην Αρχή και να ζητήσει την εξέταση των αντιρρήσεών του. Εάν η Αρχή πιθανολογήσει ότι οι αντιρρήσεις είναι εύλογες και ότι συντρέχει κίνδυνος σοβαρής βλάβης του υποκειμένου από την συνέχιση της επεξεργασίας, μπορεί να επιβάλλει την άμεση αναστολή της επεξεργασίας έως ότου εκδώσει οριστική απόφαση επί των αντιρρήσεων.

Η Αρχή έχει αρμοδιότητα μόνο να κρίνει τυχόν παραβίαση προσωπικών δεδομένων και όχι άλλα ανακύπτοντα θέματα, π.χ. τη νομιμότητα κρίσεων Υπηρεσιακού Συμβουλίου, τοποθέτησης ή μη υπαλλήλων σε θέσεις Προϊσταμένων.

Από τα στοιχεία της υπό εξέταση υπόθεσης το μονομελές πρωτοδικείο Αθηνών :

Η συλλογή και τήρηση της επίμαχης ιατρικής γνωμάτευσης στον ατομικό υπηρεσιακό φάκελο της προσφεύγουσας ήταν νόμιμη, και συνεπώς δεν κωλυόταν ο Δήμος *** από τον Ν.2472/1997 να χρησιμοποιήσει το στοιχείο αυτό με έγγραφό του προς το Υπηρεσιακό Συμβούλιο προς ανάκληση της επιλογής της προσφεύγουσας σε θέση προϊσταμένης και διατηρείται νομίμως για όσο χρονικό διάστημα είναι αναγκαίο, όπως για όσο διάστημα δύναται να προσβληθούν οι πράξεις που βασίζονται στο στοιχείο αυτό, π.χ. η μη τοποθέτηση της προσφεύγουσας σε θέση προϊσταμένης. Επειδή η προσφεύγουσα δεν εκφράζει αντιρρήσεις προς την ορθότητα της εν λόγω ιατρικής γνωμάτευσης, δεδομένου ότι δεν προσκομίζει νεότερη ιατρική γνωμάτευση που να είναι σε αντίθεση με την υπάρχουσα στο φάκελό της, ώστε να δημιουργούνται αμφιβολίες για την ορθότητα της πρώτης, και ως εκ τούτου, να διαταχθεί δέσμευση της επίμαχης γνωμάτευσης μέχρι να λυθεί η αμφιβολία. Επειδή, κατά συνέπεια, οι αντιρρήσεις της προσφεύγουσας, που υποβλήθηκαν κατά το άρθρο 13 του Ν.2472/1997, με αίτημα να μη χρησιμοποιηθεί, να μη διαβιβαστεί (δέσμευση) και να διαγραφεί η επίμαχη ιατρική γνωμάτευση είναι αβάσιμες και απορριπτέες.

Για τους λόγους αυτούς το μονομελές πρωτοδικείο Αθηνών αποφάνθηκε ότι:

Ο Δήμος μπορούσε να χρησιμοποιήσει για κάθε νόμιμο σκοπό την από 13.1.2003 ιατρική γνωμάτευση του γιατρού , την οποία δημοσιοποίησε γενικά προς ενημέρωση της Υπηρεσίας της η ίδια η προσφεύγουσα, και κατά συνέπεια καθόσον η προαναφερόμενη ιατρική γνωμάτευση τηρούνταν νομίμως στον ατομικό υπηρεσιακό φάκελο της προσφεύγουσας, η προαναφερόμενη χρήση της από τον Δήμο δεν προσκρούει στις διατάξεις του Ν.2472/1997.[3]

2)Απόφαση μονομελούς πρωτοδικείου Θεσσαλονίκης

Στην απόφαση αυτή το μονομελές πρωτοδικείο Θεσσαλονίκης λαμβάνοντας υπόψη τις διατάξεις του ν.2472/1997: Και ιδίως, το άρθρο 2 σύμφωνα με το οποίο

«Για τους σκοπούς του παρόντος νόμου νοούνται ως:

α) "Δεδομένα προσωπικού χαρακτήρα", κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. ....

γ) "Υποκείμενο των δεδομένων", το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα....

δ) "Επεξεργασία δεδομένων προσωπικού χαρακτήρα" ("επεξεργασία"), κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοή- θεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή

ε) "Αρχείο δεδομένων προσωπικού χαρακτήρα" ("αρχείο"), σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία αποτελούν ή μπορεί να αποτελέσουν αντικείμενο επεξεργασίας, και τα οποία τηρούνται είτε από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου, ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο.

ζ) "Υπεύθυνος επεξεργασίας", οποιοσδήποτε καθορίζει το σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός. Όταν ο σκοπός και ο τρόπος της επεξεργασίας καθορίζονται με δια- τάξεις νόμου ή κανονιστικές διατάξεις εθνικού ή κοινοτικού δικαίου, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια βάσει των οποίων γίνεται η επιλογή του καθορίζονται αντίστοιχα από το εθνικό ή το κοινοτικό δίκαιο».

Το άρθρο 5 § 1 του ν. 2472/1997, όπου ορίζεται ότι «Επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνον όταν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του». Ενώ, κατά το άρθρο 5 § 2 ν. 2472/1997 «Κατ' εξαίρεση επιτρέπεται η επεξεργασία και χωρίς τη συγκατάθεση, όταν: .... β) Η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρεώσεως του υπευθύνου επεξεργασίας, η οποία επιβάλλεται από το νόμο [βλ. σχετικές διατάξεις αρθρ. 5 του Κ.Δ.Διαδ.].

3)Μονομελές Πρωτόδικο Αθηνών

Στην απόφαση αυτή το μονομελές πρωτοδικείο Αθηνών δέχτηκε ότι ο χρήστης δεν επιτρέπεται να διενεργεί πράξεις που είχαν σαν αποτέλεσμα την πρόκληση βλάβης ή δυσλειτουργίας στο δίκτυο (π.χ. μαζική αποστολή μηνυμάτων, spamming κ.λπ.), να συλλέγει και συγκεντρώνει προσωπικά δεδομένα που αφορούν άλλους χρήστες. Στην προκειμένη περίπτωση ο αιτών, προκειμένου να εξεύρει τις ηλεκτρονικές διευθύνσεις των συνδρομητών της καθής, δεδομένου ότι η τελευταία δεν τηρεί δημόσιο κατάλογο ηλεκτρονικών διευθύνσεων των συνδρομητών της κατά την έννοια του άρθρου 8 του Ν 2774/1999 αλλά αλφαβητικό ευρετήριο ονομάτων πρόσβασης των συνδρομητών της που είχαν επιλέξει να κατασκευάσουν δική τους σελίδα χρήστη και αποτελούν ονόματα πρόσβασης, χωρίς την συγκατάθεση των συνδρομητών προέβη σε συλλογή των ονομάτων πρόσβασης αυτών από τον πιο πάνω αλφαβητικό κατάλογο της καθής, πρόσθεσε σ'αυτά "otenet.gr" και απέκτησε την ηλεκτρονική διεύθυνση των συνδρομητών, της καθής, στους οποίους απέστειλε μαζικώς, χωρίς να ζητηθεί, αλληλογραφία από την ιστοσελίδα www.e.....Gr, παραβιάζοντας τους όρους χρήσης που προαναφέρθηκαν.

Για το ζήτημα που ανέκυψε από την πιο πάνω συμπεριφορά του αιτούντος, η καθής με το από 25.9.2001 έγγραφο της απευθυνόμενο προς την Αρχή Προστασίας Δεδομένων ζήτησε να κριθεί αν συντρέχει περίπτωση παράνομης επεξεργασίας προσωπικών δεδομένων λόγω της κατά τα άνω συλλογής και επεξεργασίας ηλεκτρονικών διευθύνσεων συνδρομητών της από τον αιτούντα για μαζική αποστολή μη ζητηθείσας αλληλογραφίας και η Αρχή με την υπ'αριθμό 19/2001 απόφαση της έκρινε ότι η συλλογή των κωδικών πρόσβασης των συνδρομητών της otenet χωρίς την συγκατάθεση των τελευταίων από τον αιτούντα παραβιάζουν τις διατάξεις των άρθρων 4 και 5 Ν 2472/1997, όπως και ότι η αποστολή ηλεκτρονικών μηνυμάτων από το site e…gr με περιεχόμενο ανακοίνωση των θεμάτων της και την πρόσκληση επίσκεψης της συγκεκριμένης ιστοσελίδας μέσω ηλεκτρονικού ταχυδρομείου συνιστά παράνομη επεξεργασία κατά το άρθρο 9 παρ. 1 Ν 2774/1999, εφόσον οι συνδρομητές δεν είχαν δώσει προηγουμένως τη ρητή συγκατάθεση τους.