ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (GDPR)»

ΧΟΝΔΡΟΓΙΑΝΝΗ ΛΥΓΕΡΗ

(ΑΜ 14646)

Επιβλέπουσα : Παναγιώτα Βάθη – Σαράβα

Επίκουρη Καθηγήτρια

Μεσολόγγι 2021

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (GDPR)

Χονδρογιάννη Λυγερή

Επιβλέπουσα καθηγήτρια: Παναγιώτα Βάθη-Σαράβα

Επίκουρη καθηγήτρια

Μεσολόγγι 2021

UNIVERSITY OF PATRAS

SCHOOL OF ECONOMICS & BUSINESS

DEPARTMENT OF MANAGEMENT SCIENCE AND TECHNOLOGY

THESIS

GENERAL DATA PROTECTION REGULATION (GDPR)

Xondrogiannh Lygerh

(14646)

Thesis Advisor: Panagiota Vathi – Sarava

Assistant Professor

Messolonghi 2021

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας του Πανεπιστημίου Πατρών δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος.

ΕΥΧΑΡΙΣΤΙΕΣ

Τα βασικά σημεία του GDPR, οι επιπτώσεις που έχει στις επιχειρήσεις αλλά και η επίδραση στην ασφάλεια θα αναλυθούν στην παρούσα πτυχιακή εργασία, στα πλαίσια του προπτυχιακού προγράμματος σπουδών του τμήματος Διοίκησης Επιχειρήσεων της σχολής Διοίκησης & Οικονομίας του Τεχνολογικού Εκπαιδευτικού Ιδρύματος Δυτικής Ελλάδας, η οποία εγγράφηκε από την φοιτήτρια Χονδρογιάννη Λυγερή.

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω όλους τους καθηγητές του τμήματός μου, και ιδιαίτερα τον κ. Τσουραμάνη Χρήστο και την Επιβλέπουσα Καθηγήτρια κα. Παναγιώτα Βάθη – Σαράβα.

Τέλος, ευχαριστώ την οικογένειά μου για την συνεχή στήριξη όλων των χρόνων των σπουδών μου.

Χονδρογιάννη Λυγερή

.

ΠΕΡΙΛΗΨΗ

Το θέμα της παρούσας πτυχιακής εργασίας είναι «Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)» και αρχικά παρουσιάζεται η «ψηφιακή παραβατικότητα», καταγράφοντας γενικά στοιχεία της, και τους τύπους εγκλήματος στον Κυβερνοχώρο. Έπειτα πραγματοποιείται «Επισκόπηση του GDPR», όπου αναλύονται γενικά στοιχεία του GDPR, το πεδίο εφαρμογής, η νόμιμη του βάση και αμφιλεγόμενα θέματα για το GDPR. Εν συνεχεία καταγράφεται η: «Βιβλιογραφική επισκόπηση του γενικού κανονισμού για την προστασία δεδομένων», μελλοντικά ζητήματα, οι κανονιστικές προκλήσεις της αναγνώρισης στο διαδίκτυο και η ασφάλεια στον κυβερνοχώρο ως στρατηγική επιχειρηματική προτεραιότητα. Σημαντικός άξονας είναι τα: «Σημεία κλειδιά του GDPR για την ασφάλεια», όπου παρουσιάζονται η βασική διαφοροποίηση του GDPR και η καινοτομία βασισμένη στο GDPR. Μετά η διατυπώνεται η «Συζήτηση και οι προκλήσεις για το GDPR», η «Επίδραση του GDPR στην ασφάλεια», (ασφάλεια δικτύων και πληροφοριών), και τέλος καταγράφονται τα συμπεράσματα και οι διαπιστώσεις από τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR).

Λέξεις-κλειδιά

- Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR).
- Ψηφιακή παραβατικότητα
- Κυβερνοτρομοκρατία
- Κυβερνοέκθεση
- Κυβερνασφάλεια

ABSTRACT

The topic of this dissertation is «General Data Protection Regulation (GDPR)». At first introduces the «digital delinquency», recording its general data, and the types of cybercrime. A «GDPR Overview» is then conducted, which analyzes general GDPR data, scope, legal basis and controversial GDPR issues. This is followed by «Bibliographic overview of the general data protection regulation», future issues, the regulatory challenges of internet recognition and cyber security as a strategic business priority. An important focus is on the «GDPR Key Points for Security», which outlines key GDPR diversification and GDPR-based innovation. It is followed by the «Discussion and Challenges for the GDPR», the «Impact of the GDPR on Security», (network and information security), and finally the conclusions and findings from the General Data Protection Regulation (GDPR).

Key-words

- General Data Protection Regulation (GDPR).
- Digital delinquency
- Cyber terrorism
- Cyber exposure
- Cybersecurity

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ - ΣΧΗΜΑΤΩΝ

ΕΙΚΟΝΕΣ

ΣΧΗΜΑΤΑ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ - ΑΠΟΔΟΣΗ ΟΡΩΝ

ΑΕΑ: ανεξάρτητη εποπτική αρχή

ΑΕγχΠΠ: Ακαθάριστο Εγχώριο Προϊόν

ΕΕ: Ευρωπαϊκή Ένωση

ΕΚ: Ευρωπαϊκό Κοινοβούλιο

ΕΟΧ: Ευρωπαϊκός Οικονομικός Χώρος

ΚΠΠΔ: Κανονισμός Προστασίας Προσωπικών Δεδομένων

ΣΛΕΕ: Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης

Accountability Principle: Αρχή λογοδοσίας

CERT: Software Engineering Institute (Ινστιτούτο Μηχανικής Λογισμικού)

CSIRT: Computer Security Incident Response Team (Ομάδα αντιμετώπισης περιστατικών ασφαλείας υπολογιστών)

DPIA: Data Protection Impact Assessment (Εκτίμηση αντίκτυπου προστασίας δεδομένων)

DPO: Data Protection Officer (Υπεύθυνος Προστασίας Δεδομένων)

EDPB: European Data Protection Board (Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων)

GDPR: General Data Protection Regulation (Κανονισμός Προστασίας Προσωπικών Δεδομένων)

FUD: Fear, Uncertainty and Doubt (φόβος, αβεβαιότητα και αμφιβολίες)

ICO: Information Commissioner's Office (Γραφείο Επιτρόπου Πληροφοριών)

IoT: Internet of things

NISD: Network and Information Security Directive (Οδηγία για την ασφάλεια δικτύων και πληροφοριών)

ΕΙΣΑΓΩΓΗ

Θεμελιώδες κοινωνικό δικαίωμα αποτελεί η προστασία των φυσικών προσώπων / ατόμων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, το οποίο καταγράφεται στο 8ο άρθρο της 1ης παραγράφου του «Χάρτη των Θεμελιωδών Δικαιωμάτων» της Ευρωπαϊκής Ένωσης αλλά και στο 16ο άρθρο της 1ης παραγράφου της «Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης» (ΣΛΕΕ), όπου ορίζεται ότι κάθε φυσικό πρόσωπο έχει το υπέρτατο δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν. Παρόλο που οι θεμελιακές αρχές της ιδιωτικής ζωής των προσωπικών δεδομένων συνεχίζουν να ισχύουν από την προηγούμενη οδηγία 95/46/ΕΚ, στον νέο κανονισμό GDPR προταθήκαν πολλές αλλαγές στις ρυθμιστικές πολιτικές.

Ο κύριος στόχος του Κανονισμού Προστασίας Προσωπικών Δεδομένων (General Data Protection Regulation / GDPR) είναι η προστασία όλων των πολιτών της ΕΕ από την εισβολή τρίτων στην ιδιωτική τους ζωή αλλά και τις παραβιάσεις των δεδομένων σε μία κοινωνία περισσότερο βασισμένη στην διάδοση πληροφοριών, η οποία μετασχηματίστηκε ραγδαία, από τον χρόνο σύστασης της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου για την «*προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών*» (Ευρωπαϊκό Κοινοβούλιο: 31995L0046-Οδηγία 95/46/ΕΚ, 1995).

Το GDPR, μετά από αρκετά χρόνια προετοιμασίας, εγκρίθηκε στις 14 Απριλίου 2016 από το κοινοβούλιο της ΕΕ. Η ημερομηνία αναγκαστικής εκτέλεσης ήταν η 25η Μαΐου 2018, οπότε οι οργανώσεις που δεν συμμορφώνονται μπορούν να αντιμετωπίσουν μεγάλα πρόστιμα.

Η οδηγία 95/46 / ΕΚ σχετικά με την προστασία των δεδομένων αντικαταστάθηκε από τον γενικό κανονισμό αναφορικά με την προστασία των δεδομένων της ΕΕ (GDPR). Ο στόχος είναι η εναρμόνιση των νομοθεσιών σχετικά με την προστασία της ιδιωτικής ζωής σε όλη την Ευρώπη, για την προστασία και την ενδυνάμωση του ιδιωτικού απορρήτου των πολιτών της ΕΕ και για την αναδόμηση του πώς προσεγγίζονται οι οργανισμοί σε ολόκληρη την περιοχή (Επίσημη Εφημερίδα τον Ευρωπαϊκών Κοινοτήτων, 1995).

Αναμφίβολα η πιο μεγάλη μεταβολή στο ρυθμιστικό περιβάλλον της ιδιωτικότητας των δεδομένων οφείλεται στην εκτεταμένη αρμοδιότητα του GDPR. Είναι ένα γεγονός που ισχύει σε όλες τις εταιρείες οι οποίες εξετάζουν τα προσωπικά δεδομένα των υποκειμένων των

δεδομένων που διαμένουν στην Ένωση, χωρίς να λαμβάνεται υπόψιν η τοποθεσία της εταιρείας. Το GDPR θα ασχολείται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από ελεγκτές και μεταποιητές της ΕΕ, χωρίς να έχει σημασία εάν η επεξεργασία γίνεται στην ΕΕ ή όχι (lawspot.gr/GDPR, 2018).

Στην παρούσα πτυχιακή εργασία πραγματοποιήθηκε διεξαγωγή βιβλιογραφικής έρευνας με αποτελεσματικό και συστηματικό τρόπο. Η συνάφεια αυτής της μεθόδου καθίσταται προφανής μέσω εμπειρικής έρευνας σχετικά με το GDPR σε πλήθος επιστημονικών περιοδικών. Υπάρχει μια συναίνεση μεταξύ των επιστημονικών ερευνητών ότι για να προχωρήσει η επιστημονική γνώση είναι απαραίτητο να διεξαχθεί αυστηρή βιβλιογραφική έρευνα για να προσδιοριστεί η κατάσταση της γνώσης, πιθανά κενά έρευνας που μπορεί να υπάρχουν και ευκαιρίες για νέες συνεισφορές στο υπό μελέτη θέμα (Villas, Macedo-Soares, & Russo, 2008).

Τα επιστημονικά περιοδικά είναι τα κύρια μέσα της βιβλιογραφικής έρευνας και δημοσίευσης της επιστημονικής έρευνας, επειδή παρουσιάζουν τα κύρια αποτελέσματα των ερευνών και αποτελούν εισροές για νέες.

Η βιβλιογραφική έρευνα είναι μια επίπονη και χρονοβόρα εργασία. Παρόλο που η τεχνολογία πληροφοριών, παρέχοντας ισχυρά εργαλεία αναζήτησης, έχει συμβάλει πράγματι στον εντοπισμό πιθανών πηγών διαβούλευσης, η εκθετική αύξηση του διαθέσιμου αριθμού πληροφοριών έχει κάνει τις αναζητήσεις και τις αποφάσεις σχετικά με τις καλύτερες πηγές που πρέπει να υιοθετηθούν, όλο και πιο περίπλοκο έργο.

Η δομή της παρούσης πτυχιακής εργασίας είναι η εξής:

Στο 1ο κεφάλαιο η: «ψηφιακή παραβατικότητα», καταγράφονται γενικά στοιχεία, τα οικονομικά εγκλήματα, η κυβερνοτρομοκρατία, η κυβερνοέκθεση, το cybersex, το ηλεκτρονικό «ψάρεμα» (Phishing, Pharming) και το κακόβουλο λογισμικό.

Στο 2ο κεφάλαιο η: «Επισκόπηση του GDPR», αναλύονται γενικά στοιχεία του GDPR, το πεδίο εφαρμογής του GDPR, η νόμιμη του βάση, έπειτα πραγματοποιείται σύνοψη των άρθρων που περιέχονται στο GDPR, η επισκόπηση βασικών συμβάντων του GDPR, και τέλος παρατίθενται αμφιλεγόμενα θέματα για το GDPR.

Στο 3ο κεφάλαιο η: «Βιβλιογραφική επισκόπηση του γενικού κανονισμού για την προστασία δεδομένων», καταγράφονται μελλοντικά ζητήματα, οι κανονιστικές προκλήσεις της αναγνώρισης στο διαδίκτυο, η προετοιμασία με το GDPR, η σχέση του ICO και η τεχνητή

νοημοσύνη, το GDPR για τις επιχειρήσεις, το δικαίωμα μεταφοράς δεδομένων στο GDPR, η κατανόηση της εννοίας του κινδύνου στον κανονισμό γενικής προστασίας δεδομένων, η βιομηχανική ασφάλεια και FUD, και τέλος η ασφάλεια στον κυβερνοχώρο ως στρατηγική επιχειρηματική προτεραιότητα.

Στο 4ο κεφάλαιο τα: «Σημεία κλειδιά του GDPR για την ασφάλεια», παρουσιάζονται γενικά στοιχεία, η βασική διαφοροποίηση του GDPR, οι προϋποθέσεις νόμιμης επεξεργασίας των προσωπικών δεδομένων, το πεδίο εφαρμογής του κανονισμού (κατάργηση της γενικής υποχρέωσης γνωστοποίησης προς την εποπτική αρχή, διενέργεια εκτίμησης αντίκτυπου, ορισμός υπεύθυνου προστασίας δεδομένων, σύνταξη κωδικών δεοντολογίας), η αυστηρή επιβολή νομού, η αυξημένη υποχρέωση λογοδοσίας, η προστασία της ιδιωτικότητας, η ατομική ελευθερία / εξουσία, και τέλος η καινοτομία βασισμένη στο GDPR.

Το θέμα του 5ου κεφαλαίου είναι η: «Συζήτηση και οι προκλήσεις για το GDPR» και παρατίθενται γενικά στοιχεία, ο επηρεασμός των επιχειρήσεων (email marketing, GDPR και πολίτες, GDPR και παραβιάσεις δεδομένων, πρόστιμα και κυρώσεις), και τέλος το GDPR ως ευκαιρία.

Στο 6ο κεφάλαιο η «Επίδραση του GDPR στην ασφάλεια», αναλύονται γενικά στοιχεία, η ασφάλεια δικτύων και πληροφοριών, η ασφάλεια δεδομένων προσωπικού χαρακτήρα, οι τρόποι ασφάλειας δεδομένων (κρυπτογράφηση), και τέλος τα πιο κοινά ζητήματα στο internet security.

Στο 7ο και τελευταίο κεφάλαιο καταγράφονται τα συμπεράσματα και οι διαπιστώσεις από τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR).

1 ΚΕΦΑΛΑΙΟ: «ΨΗΦΙΑΚΗ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑ»

1.1 ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ

Το έγκλημα στον κυβερνοχώρο είναι ένα έγκλημα που περιλαμβάνει υπολογιστές σε δίκτυο. Ο υπολογιστής μπορεί να έχει χρησιμοποιηθεί στη διάπραξη ενός εγκλήματος, ή μπορεί να είναι ο στόχος. Επίσης, το έγκλημα στον κυβερνοχώρο μπορεί να απειλήσει ένα άτομο, μια εταιρεία ή την ασφάλεια και την οικονομική υγεία ενός έθνους (Lewis, 2018).

Υπάρχουν πολλές ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής σχετικά με το έγκλημα στον κυβερνοχώρο όταν οι εμπιστευτικές πληροφορίες υποκλέπτονται ή αποκαλύπτονται, νόμιμα ή με άλλο τρόπο. Σε διεθνές επίπεδο, τόσο κυβερνητικοί όσο και μη κρατικοί παράγοντες εμπλέκονται σε εγκλήματα στον κυβερνοχώρο, συμπεριλαμβανομένης της κατασκοπείας, της οικονομικής κλοπής και άλλων διασυνοριακών εγκλημάτων. Τα εγκλήματα στον κυβερνοχώρο που περνούν τα διεθνή σύνορα και περιλαμβάνουν τις ενέργειες τουλάχιστον ενός έθνους-κράτους αναφέρονται μερικές φορές ως κυβερνοπόλεμος.

Μια έκθεση (που χρηματοδοτείται από την McAfee), που δημοσιεύθηκε το 2014, υπολόγισε ότι η ετήσια ζημιά στην παγκόσμια οικονομία ήταν 445 δισεκατομμύρια δολάρια. Περίπου 1,5 δισεκατομμύρια δολάρια χάθηκαν το 2012 λόγω διαδικτυακής απάτης με πιστωτικές και χρεωστικές κάρτες στις ΗΠΑ. Το 2018, μια μελέτη του Κέντρου Στρατηγικών και Διεθνών Σπουδών (Center for Strategic and International Studies / CSIS), σε συνεργασία με την McAfee, καταλήγει στο συμπέρασμα ότι σχεδόν 600 δισεκατομμύρια δολάρια, σχεδόν το 1% του παγκόσμιου ΑΕΠ, χάνονται από το έγκλημα στον κυβερνοχώρο κάθε χρόνο (Lewis, 2018).

Τέλος, το ηλεκτρονικό έγκλημα περιλαμβάνει ένα ευρύ φάσμα δραστηριοτήτων.

1.2 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΩΝ ΕΓΚΛΗΜΑΤΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Οι νέες τεχνολογίες δημιουργούν νέες ευκαιρίες για εγκλήματα, αλλά λίγα νέα είδη εγκλήματος. Το ερώτημα που προκύπτει είναι τι διακρίνει το έγκλημα στον κυβερνοχώρο από την παραδοσιακή εγκληματική δραστηριότητα. Προφανώς, η μεγαλύτερη διαφορά είναι η χρήση του υπολογιστή, αν και η τεχνολογία από μόνη της δεν επαρκεί για οποιαδήποτε

διάκριση που μπορεί να υπάρχει μεταξύ διαφορετικών ειδών εγκληματικής δραστηριότητας. Οι εγκληματίες δεν χρειάζονται υπολογιστή για να διαπράξουν διάφορα είδη απάτης, όπως κυκλοφορία παιδικής πορνογραφίας και πνευματική ιδιοκτησίας, κλοπή μιας ταυτότητας ή παραβίαση του απόρρητου κάποιου. Όλες αυτές οι δραστηριότητες υπήρχαν και πριν τον «κυβερνοχώρο». Το έγκλημα στον κυβερνοχώρο, ιδίως με το Διαδίκτυο, αποτελεί επέκταση της υπάρχουσας εγκληματικής συμπεριφοράς παράλληλα με ορισμένες νέες παράνομες δραστηριότητες (Dennis, 2021).

Εικόνα 1.1: Απεικόνιση του εγκλήματος στον Κυβερνοχώρο.

Πηγή: (CyberCrime-ΚΕΔΙΒΙΜ, 2020).

Τα περισσότερα εγκλήματα στον κυβερνοχώρο είναι μια επίθεση σε πληροφορίες σχετικά με άτομα, εταιρείες ή κυβερνήσεις. Αν και οι επιθέσεις δεν πραγματοποιούνται σε ένα φυσικό σώμα, ωστόσο πραγματοποιούνται σε ένα προσωπικό ή εταιρικό εικονικό σώμα, το οποίο είναι το σύνολο των πληροφοριακών χαρακτηριστικών που ορίζουν άτομα και ιδρύματα στο Διαδίκτυο. Με άλλα λόγια, στην ψηφιακή εποχή οι εικονικές ταυτότητες είναι βασικά στοιχεία της καθημερινής ζωής. Όλοι οι άνθρωποι είναι μια δέσμη αριθμών και αναγνωριστικών σε πολλές βάσεις δεδομένων υπολογιστών που ανήκουν σε κυβερνήσεις και εταιρείες. Το έγκλημα στον κυβερνοχώρο επισημαίνει την κεντρική θέση των δικτυωμένων υπολογιστών στη ζωή του σύγχρονου ανθρώπου, καθώς και την ευθραυστότητα τέτοιων φαινομενικά στερεών γεγονότων όπως η ατομική ταυτότητα (Lotha, 2019).

Μια σημαντική πτυχή του εγκλήματος στον κυβερνοχώρο είναι ο μη τοπικός χαρακτήρας του, δηλαδή οι ενέργειες μπορούν να γίνουν σε δικαιοδοσίες που χωρίζονται από μεγάλες αποστάσεις. Αυτό δημιουργεί σοβαρά προβλήματα για την επιβολή του νόμου, καθώς προηγουμένως τοπικά ή ακόμη και εθνικά εγκλήματα απαιτούν πλέον διεθνή συνεργασία. Για παράδειγμα, εάν ένα άτομο έχει πρόσβαση σε παιδική πορνογραφία μέσω υπολογιστή σε μια χώρα που δεν απαγορεύει την παιδική πορνογραφία, τότε μπορεί να ισχυριστεί κάποιος ότι διαπράττει έγκλημα σε ένα έθνος όπου αυτά τα υλικά είναι παράνομα; Πού ακριβώς συμβαίνει το έγκλημα στον κυβερνοχώρο; Ως ένα πλανητικό δίκτυο, το Διαδίκτυο προσφέρει σε εγκληματίες πολλές κρυψώνες στον πραγματικό κόσμο, καθώς και στο ίδιο το δίκτυο. Ωστόσο, ακριβώς όπως οι άνθρωποι αφήνουν ίχνη όταν περπατούν τα οποία μπορεί να ακολουθήσει ένας εξειδικευμένος ιχνηλάτης, αντίστοιχα και οι εγκληματίες του κυβερνοχώρου αφήνουν ενδείξεις για την ταυτότητα και την τοποθεσία τους, παρά τις προσπάθειές τους να καλύψουν τα ίχνη τους. Ωστόσο, για να ακολουθηθούν τέτοιες ενδείξεις πέρα από τα εθνικά σύνορα, πρέπει να επικυρωθούν οι διεθνείς συνθήκες εγκλήματος στον κυβερνοχώρο (Ray, 2018).

Το 1996, το Συμβούλιο της Ευρώπης, μαζί με κυβερνητικούς εκπροσώπους από τις Ηνωμένες Πολιτείες, τον Καναδά και την Ιαπωνία, συνέταξαν μια προκαταρκτική διεθνή συνθήκη που καλύπτει το έγκλημα των υπολογιστών. Σε όλο τον κόσμο, πολιτικές ελεύθερες ομάδες διαμαρτυρήθηκαν αμέσως για τις διατάξεις της συνθήκης που απαιτούν οι πάροχοι υπηρεσιών Διαδικτύου (ISP) να αποθηκεύουν πληροφορίες σχετικά με τις συναλλαγές των πελατών τους και να μετατρέπουν αυτές τις πληροφορίες κατά παραγγελία. Ωστόσο, οι εργασίες για τη συνθήκη συνεχίστηκαν, και στις 23 Νοεμβρίου 2001, η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο υπεγράφη από 30 κράτη. Η σύμβαση τέθηκε σε ισχύ το 2004. Πρόσθετα πρωτόκολλα, που καλύπτουν τρομοκρατικές δραστηριότητες, ρατσιστικά και ξενοφοβικά εγκλήματα στον κυβερνοχώρο, προτάθηκαν το 2002 και τέθηκαν σε ισχύ το 2006. (Dennis, 2021).

1.3 Τύποι Εγκλήματος Στον Κυβερνοχώρο

Το έγκλημα στον κυβερνοχώρο κυμαίνεται σε ένα φάσμα δραστηριοτήτων. Στο ένα άκρο είναι εγκλήματα που συνεπάγονται θεμελιώδεις παραβιάσεις προσωπικού ή εταιρικού απορρήτου, όπως επιθέσεις σχετικά με την ακεραιότητα των πληροφοριών που διατηρούνται σε ψηφιακά αποθετήρια και τη χρήση παράνομα ληφθέντων ψηφιακών πληροφοριών για

εκβιασμό μιας εταιρείας ή ενός ατόμου. Επίσης, σε αυτό το τέλος του φάσματος βρίσκεται το αυξανόμενο έγκλημα της κλοπής ταυτότητας. Στη μέση του φάσματος βρίσκονται τα εγκλήματα που βασίζονται σε συναλλαγές, όπως απάτη, εμπορία παιδικής πορνογραφίας, ψηφιακή πειρατεία, ξέπλυμα χρήματος και παραποίηση. Πρόκειται για συγκεκριμένα εγκλήματα με συγκεκριμένα θύματα, ενώ ο εγκληματίας κρύβεται στη σχετική ανωνυμία που παρέχει το Διαδίκτυο. Ένα άλλο μέρος αυτού του είδους του εγκλήματος περιλαμβάνει άτομα εντός εταιρειών ή κυβερνητικών γραφειοκρατών που τροποποιούν σκόπιμα δεδομένα είτε για κέρδη είτε για πολιτικούς στόχους. Στο άλλο άκρο του φάσματος είναι εκείνα τα εγκλήματα που συνεπάγονται προσπάθειες να διαταράξουν την πραγματική λειτουργία του Διαδικτύου. Αυτά κυμαίνονται από ανεπιθύμητα μηνύματα, εισβολές και επιθέσεις άρνησης υπηρεσίας σε συγκεκριμένους ιστότοπους έως πράξεις κυβερνο-τρομοκρατίας – δηλαδή η χρήση του Διαδικτύου για την πρόκληση δημόσιων ενοχλήσεων, ακόμη και θανάτου. Η κυβερνοτρομοκρατία εστιάζει στη χρήση του Διαδικτύου από μη κρατικούς φορείς για να επηρεάσει την οικονομική και τεχνολογική υποδομή ενός έθνους. Από τις επιθέσεις της 11ης Σεπτεμβρίου του 2001 και μετά έχει αυξηθεί δραματικά η ευαισθητοποίηση του κοινού για την απειλή της κυβερνο-τρομοκρατίας (Dennis, 2021).

1.3.1 Κλοπή ταυτότητας και παραβίαση της ιδιωτικής ζωής

Το έγκλημα στον κυβερνοχώρο επηρεάζει τόσο ένα εικονικό πρόσωπο όσο και ένα πραγματικό, αλλά τα αποτελέσματα σε κάθε ένα είναι διαφορετικά. Αυτό το φαινόμενο είναι σαφέστερο στην περίπτωση κλοπής ταυτότητας. Στις Ηνωμένες Πολιτείες, για παράδειγμα, τα άτομα δεν διαθέτουν επίσημη ταυτότητα, καθώς υπάρχει ο αριθμός κοινωνικής ασφάλισης που χρησιμεύει ως αναγνωριστικός αριθμός. Οι φόροι εισπράττονται βάσει του αριθμού κοινωνικής ασφάλισης κάθε πολίτη, και πολλά ιδιωτικά ιδρύματα χρησιμοποιούν τον αριθμό για να παρακολουθούν τους υπαλλήλους, τους μαθητές και τους ασθενείς τους. Η πρόσβαση στον αριθμό κοινωνικής ασφάλισης ενός ατόμου παρέχει την ευκαιρία συγκέντρωσης όλων των εγγράφων που σχετίζονται με την ιθαγένεια αυτού του ατόμου. Οι πληροφορίες μπορούν να χρησιμοποιηθούν για την ανακατασκευή της ταυτότητας ενός ατόμου. Όταν οι εγκληματίες κλέβουν τα αρχεία πιστωτικών καρτών μιας εταιρείας, παράγουν δύο ξεχωριστά «πρότυπα». Πρώτον, δημιουργούν ψηφιακές πληροφορίες που είναι χρήσιμες με πολλούς τρόπους. Για παράδειγμα, ενδέχεται να χρησιμοποιήσουν τα στοιχεία της πιστωτικής κάρτας για να εξοικονομήσουν τεράστιους λογαριασμούς, αναγκάζοντας τις εταιρείες πιστωτικών καρτών να

υποστούν μεγάλες απώλειες ή μπορεί να πουλήσουν τις πληροφορίες σε άλλους που μπορούν να τις χρησιμοποιήσουν με παρόμοιο τρόπο. Δεύτερον, ενδέχεται να χρησιμοποιήσουν μεμονωμένα ονόματα και αριθμούς πιστωτικών καρτών για να δημιουργήσουν νέες ταυτότητες για άλλους εγκληματίες. Για παράδειγμα, ένας εγκληματίας μπορεί να επικοινωνήσει με την τράπεζα έκδοσης μιας κλεμμένης πιστωτικής κάρτας και να αλλάξει τη διεύθυνση αλληλογραφίας του λογαριασμού. Στη συνέχεια, ο εγκληματίας μπορεί να πάρει διαβατήριο ή άδεια οδήγησης με τη δική του φωτογραφία, αλλά με το όνομα του θύματος. Επίσης, με άδεια οδήγησης ο εγκληματίας μπορεί εύκολα να αποκτήσει μια νέα κάρτα κοινωνικής ασφάλισης. Είναι τότε δυνατό να ανοίξει τραπεζικούς λογαριασμούς και να λάβει δάνεια - όλα με το πιστωτικό αρχείο και το ιστορικό του θύματος. Ο αρχικός κάτοχος της κάρτας μπορεί να μην το γνωρίζει μέχρι που το χρέος να γίνει τόσο μεγάλο και να επικοινωνήσει η τράπεζα με τον κάτοχο του λογαριασμού. Μόνο τότε θα γίνει ορατή η κλοπή ταυτότητας. Αν και η κλοπή ταυτότητας λαμβάνει χώρα σε πολλές χώρες, ωστόσο οι ερευνητές και οι αξιωματούχοι επιβολής του νόμου μαστίζονται από την έλλειψη πληροφοριών και στατιστικών σχετικά με το έγκλημα παγκοσμίως. Το έγκλημα στον κυβερνοχώρο είναι σαφώς ένα διεθνές πρόβλημα (Dennis, 2021), (Lotha, 2019).

Το 2015, το Γραφείο Στατιστικών της Δικαιοσύνης των ΗΠΑ (Bureau of Justice Statistics / BJS) δημοσίευσε μια έκθεση σχετικά με την κλοπή ταυτότητας. Τον προηγούμενο χρόνο σχεδόν 1,1 εκατομμύρια Αμερικανοί χρησιμοποίησαν τις ταυτότητές τους για να ανοίξουν τραπεζικούς λογαριασμούς, πιστωτικές κάρτες ή λογαριασμούς κοινής ωφέλειας. Η έκθεση ανέφερε επίσης ότι άλλα 16,4 εκατομμύρια Αμερικανοί υπέστησαν θύματα κλοπής λογαριασμού, όπως η χρήση κλεμμένων πιστωτικών καρτών και αυτόματων ταμειολογιστικών (automatic teller machine / ATM) καρτών. Η έκθεση BJS έδειξε ότι ενώ ο συνολικός αριθμός θυμάτων κλοπής ταυτότητας στις Ηνωμένες Πολιτείες είχε αυξηθεί κατά περίπου 1 εκατομμύριο από το 2012, η συνολική απώλεια που υπέστησαν άτομα αυξήθηκε από το 2012 από περίπου 10 δισεκατομμύρια δολάρια σε 15,4 δισεκατομμύρια δολάρια. Το μεγαλύτερο μέρος αυτής της μείωσης οφείλεται στην απότομη πτώση του αριθμού των ατόμων που έχασαν περισσότερα από 2.000 $. Οι περισσότερες κλοπές ταυτότητας αφορούσαν μικρά ποσά, με απώλειες μικρότερες από 300 $ που αντιπροσωπεύουν το 54% του συνόλου (Dennis, 2021).

1.3.2 Απάτη στο Διαδίκτυο

Σχέδια για την εξαπάτηση των καταναλωτών αφθονούν στο Διαδίκτυο. Μεταξύ των πιο διάσημων είναι η Νιγηριανή απάτη ή απάτη «419», ο αριθμός είναι μια αναφορά στο τμήμα του νιγηριανού νόμου που παραβίασε η απάτη. Αν και αυτή η απάτη έχει χρησιμοποιηθεί τόσο με φαξ όσο και με το παραδοσιακό ταχυδρομείο, έχει δοθεί νέα ώθηση από το Διαδίκτυο. Σύμφωνα με το σχέδιο της απάτης, ένα άτομο λαμβάνει ένα e-mail που δηλώνει ότι ο αποστολέας χρειάζεται βοήθεια για τη μεταφορά ενός μεγάλου ποσού χρημάτων από τη Νιγηρία ή άλλη μακρινή χώρα. Συνήθως, αυτά τα χρήματα έχουν τη μορφή ενός περιουσιακού στοιχείου που πρόκειται να πωληθεί, όπως πετρέλαιο ή ένα μεγάλο χρηματικό ποσό που απαιτεί «ξέπλυμα» για να αποκρύψει την πηγή του. Οι παραλλαγές είναι ατελείωτες και αναπτύσσονται συνεχώς νέες ιδιαιτερότητες. Το μήνυμα ζητά από τον παραλήπτη να καλύψει κάποιο κόστος μεταφοράς χρημάτων από τη χώρα σε αντάλλαγμα για τη λήψη πολύ μεγαλύτερου ποσού χρημάτων στο εγγύς μέλλον. Εάν ο παραλήπτης απαντήσει με επιταγή ή εντολή πληρωμής, του λένε ότι έχουν αναπτυχθεί επιπλοκές και απαιτούνται περισσότερα χρήματα. Με την πάροδο του χρόνου, τα θύματα μπορούν να χάσουν χιλιάδες δολάρια που είναι εντελώς ανακτήσιμα (Dennis, 2021), (Ray, 2018).

Το 2002 το νεοσύστατο Internet Crime Complaint Center (IC3) των ΗΠΑ ανέφερε ότι περισσότερα από 54 εκατομμύρια δολάρια είχαν χαθεί από διάφορα είδη απάτης. Αυτό αντιπροσώπευε μια τριπλή αύξηση σε σχέση με τις εκτιμώμενες απώλειες ύψους 17 εκατομμυρίων δολαρίων το 2001. Οι ετήσιες απώλειες αυξήθηκαν τα επόμενα χρόνια, φθάνοντας τα 125 εκατομμύρια δολάρια το 2003, περίπου 200 εκατομμύρια δολάρια το 2006, περίπου 250 εκατομμύρια δολάρια το 2008 και πάνω από 1 δισεκατομμύριο δολάρια το 2015. Το IC3 των ΗΠΑ τη μεγαλύτερη πηγή απάτης αποκαλεί «μη πληρωμή / μη παράδοση», καθώς αγαθά και υπηρεσίες είτε παραδίδονται αλλά δεν πληρώνονται ή πληρώνονται αλλά δεν παραδίδονται. Σε αντίθεση με την κλοπή ταυτότητας, όπου η κλοπή συμβαίνει χωρίς να το γνωρίζει το θύμα, αυτές οι πιο παραδοσιακές μορφές απάτης εμφανίζονται με απλό τρόπο. Το θύμα παρέχει πρόθυμα προσωπικές πληροφορίες που επιτρέπουν το έγκλημα. Ως εκ τούτου, αυτά είναι εγκλήματα συναλλαγών. Αν και λίγοι άνθρωποι θα πίστευαν κάποιον που συναντούν τυχαία στον δρόμο και τους υπόσχεται εύκολα πλούτη, παρόλα αυτά εύκολα πιστεύουν σε ένα ανεπιθύμητο e-mail ή στην επίσκεψη μιας τυχαίας ιστοσελίδας. Παρά την εκπαίδευση των καταναλωτών, η απάτη στο Διαδίκτυο παραμένει μια βιομηχανία για εγκληματίες. Η Ευρώπη και οι Ηνωμένες Πολιτείες απέχουν πολύ από τους αποκλειστικούς

ιστότοπους εγκλήματος στον κυβερνοχώρο. Η Νότια Κορέα είναι μια από τις χώρες στον κόσμο και οι στατιστικές της για την απάτη στον κυβερνοχώρο αυξάνονται με ανησυχητικό ρυθμό. Η Ιαπωνία γνώρισε επίσης ραγδαία ανάπτυξη σε παρόμοια εγκλήματα (Dennis, 2021).

1.3.3 Απάτη ATM

Στο αυτοματοποιημένο ταμείο (automated teller machine / ATM) μέσω του οποίου πολλοί άνθρωποι παίρνουν μετρητά, για να αποκτήσει ένας χρήστης πρόσβαση σε έναν λογαριασμό παρέχει μια κάρτα και έναν προσωπικό αριθμό αναγνώρισης (personal identification number / PIN). Οι εγκληματίες έχουν αναπτύξει μέσα για να παρακολουθούν τόσο τα δεδομένα στη μαγνητική ταινία όσο και το PIN του χρήστη. Με τη σειρά τους, οι πληροφορίες χρησιμοποιούνται για τη δημιουργία πλαστών καρτών που στη συνέχεια χρησιμοποιούνται για την ανάληψη χρημάτων από τον ανυποψίαστο λογαριασμό του ατόμου.

Εικόνα 1.2: Personal Identification Number / PIN.

Πηγή: (Personal Identification Number (PIN), 2021).

Για παράδειγμα, το 2002 οι New York Times ανέφεραν ότι υπήρχαν περισσότεροι από 21.000 αμερικανικοί τραπεζικοί λογαριασμοί με τους οποίους ασχολήθηκε μια μόνο ομάδα που ασχολείται με την παράνομη απόκτηση πληροφοριών ATM. Μια ιδιαίτερα αποτελεσματική μορφή απάτης αφορούσε τη χρήση ATM σε εμπορικά κέντρα και καταστήματα. Αυτές οι μηχανές είναι ανεξάρτητες και δεν είναι μέρος μιας τράπεζας. Οι εγκληματίες μπορούν εύκολα να δημιουργήσουν μια μηχανή που μοιάζει με μια νόμιμη μηχανή. Αντί, ωστόσο, το μηχάνημα να διανέμει χρήματα, συλλέγει πληροφορίες για τους χρήστες και τους λέει μόνο ότι το μηχάνημα είναι εκτός λειτουργίας αφού πληκτρολογήσουν

τα PIN τους. Δεδομένου ότι τα ATM είναι η προτιμώμενη μέθοδος για τη διανομή νομισμάτων σε όλο τον κόσμο, η απάτη ATM έχει γίνει διεθνές πρόβλημα (Ray, 2018).

1.3.4 «Κανάλι» απάτης

Ο διεθνής χαρακτήρας του εγκλήματος στον κυβερνοχώρο είναι ιδιαίτερα εμφανής με την απάτη μέσω καναλιών (δίαυλος συνεχόμενων κόμβων). Ένα από τα μεγαλύτερα και καλύτερα οργανωμένα προγράμματα απάτης μέσω καναλιού ενορχηστρώθηκε από τον Vladimir Levin, Ρώσος προγραμματιστής με εταιρεία λογισμικού στην Αγία Πετρούπολη. Το 1994, με τη βοήθεια δεκάδων ομοσπονδιών, ο Levin άρχισε να μεταφέρει περίπου 10 εκατομμύρια δολάρια από θυγατρικές της Citibank στην Αργεντινή και την Ινδονησία σε τραπεζικούς λογαριασμούς στο Σαν Φρανσίσκο, το Τελ Αβίβ, το Άμστερνταμ, τη Γερμανία και τη Φινλανδία. Σύμφωνα με την Citibank όλα τα χρήματα, εκτός από 400.000 $, ανακτήθηκαν τελικά καθώς οι συνεργοί του Levin προσπάθησαν να αποσύρουν τα χρήματα. Ο ίδιος ο Levin συνελήφθη το 1995 ενώ ήταν σε διέλευση μέσω του αεροδρομίου Heathrow του Λονδίνου (τότε, η Ρωσία δεν είχε συνθήκη έκδοσης για το έγκλημα στον κυβερνοχώρο). Το 1998, ο Levin εκδόθηκε τελικά στις Ηνωμένες Πολιτείες, όπου καταδικάστηκε σε φυλάκιση τριών ετών και διατάχθηκε να επιστρέψει στην Citibank 240.015 $. Ο ακριβής τρόπος με τον οποίο ο Levin έλαβε τα απαραίτητα ονόματα λογαριασμών και κωδικούς πρόσβασης δεν αποκαλύφθηκε ποτέ, ενώ κανένας υπάλληλος της Citibank δεν κατηγορήθηκε ποτέ σε σχέση με την υπόθεση. Επειδή η αίσθηση της ασφάλειας και της ιδιωτικής ζωής είναι υψίστης σημασίας για τα χρηματοπιστωτικά ιδρύματα, είναι δύσκολο να εξακριβωθεί η ακριβής έκταση της απάτης. Στις αρχές του 21^{ου} αιώνα, η απάτη μέσω καλωδίων ήταν παγκόσμιο πρόβλημα (Lewis, 2018).

1.3.5 Κοινή χρήση αρχείων και πειρατεία

Μέχρι τη δεκαετία του 1990, οι πωλήσεις δίσκων (compact discs / CD) ήταν η κύρια πηγή εσόδων για τις εταιρείες εγγραφής. Αν και η πειρατεία - δηλαδή η παράνομη επανάληψη υλικού που προστατεύεται από πνευματικά δικαιώματα - ήταν πάντα ένα πρόβλημα, ειδικά στην Άπω Ανατολή, παρόλα αυτά ο πολλαπλασιασμός στις πανεπιστημιουπόλεις των φθηνών προσωπικών υπολογιστών που ήταν σε θέση να ηχογραφήσουν μουσική από CD και να τις μοιραστούν μέσω συνδέσεων διαδικτύου υψηλής ταχύτητας («ευρυζωνική») έγινε ο

μεγαλύτερος εφιάλτης της βιομηχανίας ηχογραφήσεων. Στις Ηνωμένες Πολιτείες, η βιομηχανία ηχογραφήσεων, εκπροσωπούμενη από τον Σύνδεσμο Βιομηχανίας Ηχογραφήσεων της Αμερικής (Recording Industry Association of America / RIAA), επιτέθηκε σε μία υπηρεσία κοινής χρήσης αρχείων, το Napster , το οποίο από το 1999 έως το 2001 επέτρεπε στους χρήστες του Διαδικτύου να έχουν πρόσβαση σε αρχεία μουσικής, αποθηκευμένα σε μορφή συμπίεσης δεδομένων, γνωστή ως MP3, σε υπολογιστές άλλων χρηστών μέσω του κεντρικού υπολογιστή του Napster. Σύμφωνα με το RIAA, οι χρήστες του Napster παραβίαζαν τακτικά τα πνευματικά δικαιώματα των καλλιτεχνών και η υπηρεσία έπρεπε να σταματήσει. Για τους χρήστες, τα ζητήματα δεν ήταν τόσο ξεκάθαρα. Στο επίκεντρο της υπόθεσης Napster ήταν το ζήτημα της ορθής χρήσης. Τα άτομα που είχαν αγοράσει ένα CD είχαν σαφώς τη δυνατότητα να ακούσουν τη μουσική, είτε στο στερεοφωνικό τους στο σπίτι, στο σύστημα ήχου του αυτοκινήτου είτε στον προσωπικό υπολογιστή. Αυτό που δεν είχαν το δικαίωμα να κάνουν, υποστήριξε το RIAA, ήταν να διαθέσουν το CD σε χιλιάδες άλλους που θα μπορούσαν να κάνουν ένα τέλειο ψηφιακό αντίγραφο της μουσικής και να δημιουργήσουν τα δικά τους CD. Οι χρήστες επανήλθαν στο ότι η κοινή χρήση των αρχείων τους ήταν ορθή χρήση υλικού που προστατεύεται από πνευματικά δικαιώματα για το οποίο είχαν πληρώσει μια δίκαιη τιμή. Στο τέλος, η RIAA υποστήριξε ότι με αυτόν τον τρόπο δημιουργήθηκε μια νέα τάξη εγκληματιώμ στον κυβερνοχώρο - ο ψηφιακός πειρατής - που περιελάμβανε σχεδόν οποιονδήποτε είχε μοιραστεί ή κατεβάσει ένα αρχείο MP3. Παρόλο που η RIAA έκλεισε με επιτυχία το Napster, ένας νέος τύπος υπηρεσίας κοινής χρήσης αρχείων, γνωστός ως δίκτυα peer-to-peer / ομότιμος σε ομότιμο (peer-to-peer / P2P), εμφανίστηκε. Αυτά τα αποκεντρωμένα συστήματα δεν βασίζονται σε έναν κεντρικό υπολογιστή διευκόλυνσης. Αντ' αυτού, αποτελούνται από εκατομμύρια χρήστες που ανοίγουν οικειοθελώς τους δικούς τους υπολογιστές σε άλλους για κοινή χρήση αρχείων (Dennis, 2021).

Η RIAA συνέχισε να καταπολεμά αυτά τα δίκτυα κοινής χρήσης αρχείων, απαιτώντας από τους Πάροχους Υπηρεσιών Διαδικτύου (Internet Service Provider, ISP) να ανατρέψουν αρχεία των πελατών τους που μετακινούσαν μεγάλες ποσότητες δεδομένων μέσω των δικτύων τους. Η άλλη τακτική της RIAA ήταν να πιέσει για την ανάπτυξη τεχνολογιών για την επιβολή των ψηφιακών δικαιωμάτων των κατόχων πνευματικών δικαιωμάτων. Η τεχνολογία ψηφιακής διαχείρισης δικαιωμάτων (digital rights management / DRM) είναι μια προσπάθεια πρόληψης της πειρατείας μέσω τεχνολογιών που δεν επιτρέπουν στους καταναλωτές να μοιράζονται αρχεία ή να διαθέτουν πολλά αντίγραφα ενός έργου που προστατεύεται από πνευματικά δικαιώματα (Ray, 2018).

Στις αρχές του 21ου αιώνα, οι κάτοχοι πνευματικών δικαιωμάτων άρχισαν να προσαρμόζονται στην ιδέα της εμπορικής ψηφιακής διανομής. Παραδείγματα αποτελούν οι διαδικτυακές πωλήσεις μουσικής, τηλεοπτικών εκπομπών και ταινιών σε μορφές με δυνατότητα λήψης, με και χωρίς περιορισμούς DRM από το iTunes Store (που διαχειρίζεται η Apple Inc.) και από το Amazon.com. Επιπλέον, αρκετοί πάροχοι καλωδιακής και δορυφορικής τηλεόρασης, πολλά ηλεκτρονικά συστήματα παιχνιδιών (το PlayStation 3 της Sony Corporation και το Xbox 360 της Microsoft Corporation) και υπηρεσίες ροής όπως το Netflix ανέπτυξαν «βίντεο κατ' απαίτηση» και υπηρεσίες που επιτρέπουν στους πελάτες να κατεβάζουν ταινίες και εκπομπές για άμεση (συνεχούς ροής) ή νεότερη αναπαραγωγή.

Η κοινή χρήση αρχείων επέφερε μια θεμελιώδη ανακατασκευή της σχέσης μεταξύ παραγωγών, διανομέων και καταναλωτών καλλιτεχνικού υλικού. Στην Αμερική, οι πωλήσεις CD μειώθηκαν από σχεδόν 800 εκατομμύρια άλμπουμ το 2000 σε λιγότερο από 150 εκατομμύρια άλμπουμ το 2014. Αν και η μουσική βιομηχανία πούλησε περισσότερα άλμπουμ ψηφιακά, τα έσοδα μειώθηκαν περισσότερο από το ήμισυ από το 2000. Καθώς οι ευρυζωνικές συνδέσεις στο Διαδίκτυο πολλαπλασιάζονται, η βιομηχανία κινηματογραφικών ταινιών αντιμετωπίζει παρόμοιο πρόβλημα, αν και η ψηφιακή βιντεοκάμερα (digital videodisc / DVD) κυκλοφόρησε στην αγορά με κρυπτογράφηση και διάφορες ενσωματωμένες προσπάθειες αποφυγής των προβλημάτων ενός βίντεο Napster. Ωστόσο, ιστότοποι όπως το The Pirate Bay εμφανίστηκαν εξειδικευμένοι στην κοινή χρήση τόσο μεγάλων αρχείων όπως εκείνων των ταινιών και των ηλεκτρονικών παιχνιδιών (Lewis, 2018).

1.3.6 Παραποίηση και πλαστογράφηση

Η κοινή χρήση αρχείων πνευματικής ιδιοκτησίας είναι μόνο μία πτυχή του προβλήματος με αντίγραφα. Μια άλλη πιο απλή πτυχή έγκειται στην ικανότητα των ψηφιακών συσκευών να αποδίδουν σχεδόν τέλεια αντίγραφα υλικών αντικειμένων. Μέχρι πρόσφατα, η δημιουργία παθητικού νομίσματος απαιτούσε σημαντική δεξιότητα και πρόσβαση σε τεχνολογίες που συνήθως δεν κατέχουν άτομα, όπως πρέσες, χαρακτικά και ειδικά μελάνια. Η έλευση φθηνών, υψηλής ποιότητας έγχρωμων φωτοαντιγραφικών και εκτυπωτών έκανε το έγκλημα της παραχάραξη πιο ευρύ. Οι εκτυπωτές Ink-jet αντιπροσωπεύουν τώρα ένα αυξανόμενο ποσοστό του πλαστού νόμισμα που κατασχέθηκε από τη Μυστική Υπηρεσία των ΗΠΑ. Το 1995, το νόμισμα ink-jet αντιπροσώπευε το 0,5 τοις εκατό του πλαστού νομίσματος των ΗΠΑ και το 1997 οι εκτυπωτές μελάνης παρήγαγαν το 19% των παράνομων μετρητών.

Μέχρι το 2014 σχεδόν το 60% των παραποιημένων χρημάτων που ανακτήθηκαν στις ΗΠΑ προέρχονταν από εκτυπωτές μελάνης. Η ευρεία ανάπτυξη και χρήση της τεχνολογίας των υπολογιστών ώθησε το Υπουργείο Οικονομικών των ΗΠΑ να επανασχεδιάσει το αμερικανικό νόμισμα χαρτιού για να συμπεριλάβει μια ποικιλία τεχνολογιών παραποίησης / απομίμησης. Το νόμισμα της Ευρωπαϊκής Ένωσης είχε σχεδιαστεί με ασφάλεια από την αρχή. Ειδικά χαρακτηριστικά, όπως ολόγραμμα ανάγλυφου φύλλου και ειδικές κορδέλες και χαρτί, σχεδιάστηκαν για να κάνουν την παραχάραξη δύσκολη. Πράγματι, η μετάβαση στο ευρώ παρουσίασε μια άνευ προηγουμένου ευκαιρία για παραχαράκτες προϋπάρχοντων εθνικών νομισμάτων. Ο μεγάλος φόβος ήταν ότι το πλαστό νόμισμα θα «ξεπλυθεί» σε νόμιμα ευρώ (Lewis, 2018).

Ούτε το νόμισμα είναι το μόνο έγγραφο που αντιγράφεται. Τα έγγραφα μετανάστευσης είναι, επίσης, από τα πιο πολύτιμα και είναι πολύ πιο εύκολο να αντιγραφούν από το νόμισμα. Μετά τις επιθέσεις της 11ης Σεπτεμβρίου, αυτό το πρόβλημα τέθηκε υπό αυξανόμενο έλεγχο στις Ηνωμένες Πολιτείες. Συγκεκριμένα, το Γενικό Λογιστήριο (U.S. Government Accountability Office / GAO) των ΗΠΑ εξέδωσε αρκετές εκθέσεις στα τέλη της δεκαετίας του 1990 και στις αρχές της δεκαετίας του 2000 σχετικά με την έκταση της απάτης σε έγγραφα που είχε χάσει η Υπηρεσία μετανάστευσης και πολιτογράφησης (Immigration and Naturalization Service / INS). Τέλος, μια έκθεση του GAO του 2002 ανέφερε ότι πάνω από το 90 τοις εκατό ορισμένων τύπων αιτήσεων παροχών ήταν δόλια και ανέφερε περαιτέρω ότι η απάτη μετανάστευσης ήταν «εκτός ελέγχου» (Lewis, 2018).

1.3.7 Παιδική πορνογραφία

Με την έλευση σχεδόν κάθε νέας τεχνολογίας μέσων μαζικής ενημέρωσης, η πορνογραφία ήταν η «δολοφονική εφαρμογή» ή η εφαρμογή που οδήγησε στην έγκαιρη ανάπτυξη τεχνικών καινοτομιών στην αναζήτηση του κέρδους. Το Διαδίκτυο δεν αποτελούσε εξαίρεση, αλλά υπάρχει ένα εγκληματικό στοιχείο σε αυτήν την επιχείρηση bonanza - παιδική πορνογραφία, η οποία δεν σχετίζεται με την προσοδοφόρα επιχείρηση της νόμιμης πορνογραφίας που απευθύνεται σε ενήλικες. Η κατοχή παιδικής πορνογραφίας, που ορίζεται ως εικόνες παιδιών κάτω των 18 ετών που έχουν σεξουαλική συμπεριφορά, είναι παράνομη στις Ηνωμένες Πολιτείες, στην Ευρωπαϊκή Ένωση και σε πολλές άλλες χώρες, αλλά παραμένει ένα πρόβλημα που δεν έχει εύκολη λύση. Το πρόβλημα επιδεινώνεται από την ικανότητα των ιστότοπων «kiddie porn» να διαδίδουν το υλικό τους από τοποθεσίες, όπως κράτη της πρώην

Σοβιετικής Ένωσης, καθώς και από τη Νοτιοανατολική Ασία, που δεν διαθέτουν νόμους για το έγκλημα στον κυβερνοχώρο. Ορισμένοι οργανισμοί επιβολής του νόμου πιστεύουν ότι η παιδική πορνογραφία αντιπροσωπεύει μια βιομηχανία 3 δισεκατομμυρίων δολαρίων ετησίως και ότι περισσότερες από 10.000 τοποθεσίες στο Διαδίκτυο παρέχουν πρόσβαση σε αυτά τα υλικά (Dennis, 2021).

Το Διαδίκτυο παρέχει επίσης παιδεραστές με άνευ προηγουμένου ευκαιρία να διαπράξουν εγκληματικές πράξεις μέσω της χρήσης «αίθουσες συνομιλίας» για να εντοπίσουν και να δελεάσουν θύματα. Εδώ οι εικονικοί και υλικοί κόσμοι τέμνονται με έναν ιδιαίτερα επικίνδυνο τρόπο. Σε πολλές χώρες, οι κρατικές αρχές θέτουν αστυνομικούς ως «παιδιά» σε αίθουσες συνομιλίας. Παρά την ευρεία γνώση αυτής της πρακτικής, οι παιδεραστές συνεχίζουν να έρχονται σε επαφή με αυτά τα «παιδιά» για να τα γνωρίσουν «εκτός σύνδεσης». Ότι μια τέτοια συνάντηση προκαλεί υψηλό κίνδυνο άμεσης σύλληψης δεν φαίνεται να αποτρέπει τους παιδεραστές (Dennis, 2021).

1.3.8 Παραβίαση / Hacking

Η παραβίαση του απορρήτου για τον εντοπισμό του εγκλήματος στον κυβερνοχώρο λειτουργεί καλά όταν τα εγκλήματα περιλαμβάνουν κλοπή και κατάχρηση πληροφοριών, από αριθμούς πιστωτικών καρτών και προσωπικά δεδομένα έως την κοινή χρήση αρχείων διαφόρων προϊόντων - μουσική, βίντεο ή παιδική πορνογραφία. Η ιστορία του hacking ξεκινά από τη δεκαετία του 1950, όταν μια ομάδα phreaks (συντομογραφία του όρου «phone freaks») άρχισε να εισβάλλει στα τμήματα των τηλεφωνικών δικτύων, πραγματοποιώντας μη εξουσιοδοτημένες υπεραστικές κλήσεις. Με τον πολλαπλασιασμό των συστημάτων πινάκων ανακοινώσεων υπολογιστών (bulletin board systems / BBS) στα τέλη της δεκαετίας του 1970, η κουλτούρα του phreaking άρχισε να συγκεντρώνεται σε σχεδόν οργανωμένες ομάδες ατόμων, σε «hacking» εταιρικών και κυβερνητικών συστήματων δικτύου υπολογιστών (Dennis, 2021).

Παρόλο που ο όρος χάκερ προηγείται των υπολογιστών και χρησιμοποιήθηκε ήδη από τα μέσα της δεκαετίας του 1950 σε σχέση με ερασιτέχνες ηλεκτρονικούς, η πρώτη καταγεγραμμένη παρουσία της χρήσης του σε σχέση με προγραμματιστές υπολογιστών που ήταν έμπειροι στην «πειρατεία», διαπιστώθηκε σε άρθρο του 1963 σε φοιτητική εφημερίδα στο Massachusetts Institute of Technology (MIT). Αφού τα πρώτα συστήματα υπολογιστών

συνδέθηκαν με πολλούς χρήστες μέσω τηλεφωνικών γραμμών στις αρχές της δεκαετίας του 1960, ο όρος χάκερ αναφέρεται σε άτομα που απέκτησαν μη εξουσιοδοτημένη πρόσβαση σε δίκτυα υπολογιστών, είτε από άλλο δίκτυο υπολογιστών είτε από τα δικά τους συστήματα υπολογιστών. Αξίζει να αναφερθεί στο σημείο αυτό ότι οι περισσότεροι χάκερ δεν είναι εγκληματίες με την έννοια ότι είναι βανδαλιστές ή ότι αναζητούν παράνομες οικονομικές ανταμοιβές. Αντ' αυτού, οι περισσότεροι είναι νέοι που οδηγούνται από την περιέργεια, ενώ πολλοί από αυτούς έχουν γίνει αρχιτέκτονες ασφάλειας υπολογιστών. Ωστόσο, καθώς ορισμένοι χάκερ αναζητούσαν τη φήμη μεταξύ των συνομηλίκων τους οδηγήθηκαν σε ξεκάθαρα εγκλήματα. Συγκεκριμένα, οι χάκερ άρχισαν να εισβάλλουν σε συστήματα υπολογιστών και στη συνέχεια καυχιόταν ο ένας στον άλλο για τα κατορθώματά τους, μοιράζοντας τα κλεμμένα έγγραφα ως τρόπαια για να αποδείξουν τις επιτυχίες τους. Αυτά τα κατορθώματα δημιουργήθηκαν καθώς οι χάκερ όχι μόνο εισέβαλαν, αλλά μερικές φορές ανέλαβαν τον έλεγχο των κυβερνητικών και εταιρικών δικτύων υπολογιστών (Dennis, 2021).

Ένας τέτοιος εγκληματίας ήταν ο Kevin Mitnick, ο πρώτος χάκερ που έκανε τη «πιο επιθυμητή λίστα» του Ομοσπονδιακού Γραφείου Ερευνών των ΗΠΑ (Federal Bureau of Investigation / FBI). Υποτίθεται ότι εισέβαλε στον υπολογιστή της Διοίκησης Αεροναυπηγικής Βόρειας Αμερικής (North American Aerospace Defense Command / NORAD) το 1981, όταν ήταν 17 ετών. Επρόκειτο για ένα επίτευγμα που έφερε στο προσκήνιο τη σοβαρότητα της απειλής που δημιουργούν τέτοιες παραβιάσεις ασφαλείας. Η ανησυχία με το hacking συνέβαλε πρώτα σε μια αναθεώρηση των ομοσπονδιακών καταδικαστικών αποφάσεων στις Ηνωμένες Πολιτείες, με τον νόμο περί ολοκληρωμένου ελέγχου εγκλημάτων του 1984 και στη συνέχεια με τον νόμο περί απάτης και κατάχρησης υπολογιστών του 1986 (Ray, 2018).

Η κλίμακα των εγκλημάτων πειρατείας είναι από τις πιο δύσκολες στην αξιολόγηση, επειδή τα θύματα συχνά προτιμούν να μην αναφέρουν τα εγκλήματα - μερικές φορές λόγω αμηχανίας ή φόβου για περαιτέρω παραβιάσεις της ασφάλειας. Αξιωματούχοι εκτιμούν, ωστόσο, ότι η πειρατεία κοστίζει δισεκατομμύρια δολάρια στην παγκόσμια οικονομία ετησίως. Η πειρατεία δεν είναι πάντα μια εξωτερική δουλειά - μια σχετική εγκληματική προσπάθεια περιλαμβάνει άτομα εντός εταιρειών ή κυβερνητικών γραφείων να τροποποιούν σκόπιμα αρχεία βάσεων δεδομένων είτε για κέρδος είτε για πολιτικούς σκοπούς. Οι μεγαλύτερες απώλειες προέρχονται από την κλοπή ιδιοκτησιακών πληροφοριών, μερικές φορές ακολουθούνται από εκβιασμό χρημάτων από τον αρχικό κάτοχο για την επιστροφή των

δεδομένων. Υπό αυτήν την έννοια, το hacking είναι παλιομοδίτικη βιομηχανική κατασκοπεία με άλλα μέσα.

Μία από τις μεγαλύτερες γνωστές περιπτώσεις πειρατείας υπολογιστών ανακαλύφθηκε στα τέλη Μαρτίου 2009. Περιλάμβανε κυβερνητικούς και ιδιωτικούς υπολογιστές σε τουλάχιστον 103 χώρες. Το παγκόσμιο δίκτυο κατασκοπείας γνωστό ως GhostNet ανακαλύφθηκε από ερευνητές του Πανεπιστημίου του Τορόντο, στους οποίους είχε ζητηθεί από εκπροσώπους του Δαλάι Λάμα να διερευνήσουν τους υπολογιστές του εξόριστου θιβετιανού ηγέτη για πιθανό κακόβουλο λογισμικό. Εκτός από το να ανακαλύψουν ότι οι υπολογιστές του Δαλάι Λάμα ήταν σε κίνδυνο, οι ερευνητές ανακάλυψαν ότι το GhostNet είχε διεισδύσει σε περισσότερους από χίλιους υπολογιστές σε όλο τον κόσμο. Η υψηλότερη συγκέντρωση «συμβιβασμένων» συστημάτων ήταν σε γραφεία πρεσβειών και εξωτερικών υποθέσεων ή βρίσκονταν σε χώρες της Νότιας Ασίας και της Νοτιοανατολικής Ασίας. Σύμφωνα με πληροφορίες, οι υπολογιστές μολύνθηκαν από χρήστες που άνοιξαν συνημμένα e-mail ή έκαναν κλικ σε συνδέσμους ιστοσελίδων. Μόλις μολύνθηκαν από το κακόβουλο λογισμικό GhostNet, οι υπολογιστές άρχισαν να «ψαρεύουν» αρχεία σε όλο το τοπικό δίκτυο - ακόμη και να ενεργοποιούν κάμερες και συσκευές εγγραφής βίντεο για απομακρυσμένη παρακολούθηση. Τρεις διακομιστές ελέγχου που εκτελούσαν το κακόβουλο λογισμικό εντοπίστηκαν στο Hainan, στις επαρχίες Γκουανγκντόνγκ και Σιτσουάν στην Κίνα και ένας τέταρτος διακομιστής βρισκόταν στην Καλιφόρνια (Dennis, 2021).

1.3.9 Ιοί υπολογιστών

Η σκόπιμη απελευθέρωση καταστροφικών ιών υπολογιστών είναι ένας ακόμη τύπος εγκλήματος στον κυβερνοχώρο. Στην πραγματικότητα, αυτό ήταν το έγκλημα του πρώτου ατόμου που καταδικάστηκε στις Ηνωμένες Πολιτείες βάσει του Νόμου περί απάτης και κατάχρησης υπολογιστών το 1986. Στις 2 Νοεμβρίου 1988, ένας φοιτητής της επιστήμης των υπολογιστών στο Πανεπιστήμιο Cornell με την ονομασία Robert Morris κυκλοφόρησε ένα λογισμικό «worm» στο Διαδίκτυο από το MIT (ως επισκέπτης στην πανεπιστημιούπολη, ήλπιζε να παραμείνει ανώνυμος). Το worm ήταν ένα πειραματικό πρόγραμμα αυτο-πολλαπλασιασμού και αναπαραγωγής υπολογιστών που εκμεταλλεύτηκε τις ατέλειες σε ορισμένα πρωτόκολλα ηλεκτρονικού ταχυδρομείου. Λόγω λάθους στον προγραμματισμό του, αντί να στέλνει αντίγραφα του εαυτού του σε άλλους υπολογιστές, αυτό το λογισμικό συνέχισε να επαναλαμβάνεται σε κάθε μολυσμένο σύστημα, γεμίζοντας όλη τη διαθέσιμη μνήμη του υπολογιστή. Πριν βρεθεί μια επιδιόρθωση, το «σκουλήκι» είχε αναγκάσει περίπου 6.000 υπολογιστές (το ένα δέκατο του Διαδικτύου) να σταματήσει. Αν και το «σκουλήκι» του Μόρις κόστισε χρόνο και εκατομμύρια δολάρια για να διορθωθεί, το γεγονός είχε λίγες εμπορικές συνέπειες, γιατί το Διαδίκτυο δεν είχε γίνει ακόμη ένα στοιχείο οικονομικών υποθέσεων. Έκτοτε, ολοένα και περισσότεροι επιβλαβείς ιοί έχουν δημιουργηθεί από αναρχικούς και λανθασμένες τοποθεσίες από διαφορετικές περιοχές, όπως οι Ηνωμένες Πολιτείες, η Βουλγαρία, το Πακιστάν και οι Φιλιππίνες (Dennis, 2021), (Ray, 2018).

1.3.10 Επιθέσεις άρνησης υπηρεσίας / Denial of service attacks

Την 7η Φεβρουαρίου 2000, ο «mafiaboy», ένας 15χρονος Καναδός χάκερ με την βοήθεια του «σκουληκιού» (worm) Morris, ενορχήστρωσε μια σειρά επιθέσεων άρνησης υπηρεσίας (denial of service attacks / DoS) σε αρκετούς ιστότοπους ηλεκτρονικού εμπορίου, συμπεριλαμβανομένου του Amazon.com και eBay.com. Αυτές οι επιθέσεις χρησιμοποιούν υπολογιστές σε πολλαπλές τοποθεσίες για να καταστρέψουν τους υπολογιστές του προμηθευτή και να κλείσουν τους World Wide Web sites (WWW) με νόμιμη εμπορική κυκλοφορία. Οι επιθέσεις κατέστρεψαν το εμπόριο Διαδικτύου, με το FBI να εκτιμά ότι οι πληγείσες ιστοσελίδες υπέστησαν ζημιές 1,7 δισεκατομμυρίων δολαρίων. Το 1988 το Διαδίκτυο διαδραμάτιζε σημαντικό ρόλο μόνο στη ζωή ερευνητών και ακαδημαϊκών, ενώ μέχρι το 2000 είχε καταστεί απαραίτητο για τη λειτουργία της κυβέρνησης και της οικονομίας

των ΗΠΑ. Το έγκλημα στον κυβερνοχώρο είχε μετατραπεί από ζήτημα των ατομικών αδικημάτων σε θέμα εθνικής ασφάλειας (Dennis, 2021).

Οι κατανεμημένες επιθέσεις DoS είναι ένα ιδιαίτερο είδος hacking. Ένας εγκληματίας προσβάλλει μια σειρά υπολογιστών με προγράμματα υπολογιστών που μπορούν να ενεργοποιηθούν από έναν εξωτερικό χρήστη υπολογιστή. Αυτά τα προγράμματα είναι γνωστά ως Δούρειοι ίπποι αφού εισέρχονται στους υπολογιστές των άγνωστων χρηστών ως κάτι καλόηθες, όπως μια φωτογραφία ή ένα έγγραφο που επισυνάπτεται σε ένα ηλεκτρονικό ταχυδρομείο. Σε προκαθορισμένο χρόνο, αυτό το πρόγραμμα Trojan horse αρχίζει να στέλνει μηνύματα σε μια προκαθορισμένη τοποθεσία. Εάν έχουν παραβιαστεί αρκετοί υπολογιστές, είναι πιθανό ο επιλεγμένος ιστότοπος να μπορεί να συνδεθεί τόσο αποτελεσματικά, ώστε να μην μπορεί να φτάσει σε καμία νόμιμη κίνηση. Μια σημαντική διαπίστωση από αυτά τα γεγονότα ήταν ότι πολλά λογισμικά δεν είναι ασφαλή, καθιστώντας εύκολο ακόμη και σε έναν ανειδίκευτο χάκερ να θέσει σε κίνδυνο έναν τεράστιο αριθμό μηχανημάτων. Αν και οι εταιρείες λογισμικού προσφέρουν τακτικά patches ενημέρωσης κώδικα για τα τρωτά σημεία λογισμικού, δεν μπορούν όλοι οι χρήστες να εφαρμόσουν τις ενημερωμένες εκδόσεις, και οι υπολογιστές τους παραμένουν ευάλωτοι σε εγκληματίες που θέλουν να ξεκινήσουν επιθέσεις DoS. Το 2003 ο πάροχος υπηρεσιών Διαδικτύου PSINet Europe συνέδεσε έναν μη προστατευμένο διακομιστή στο Διαδίκτυο. Μέσα σε 24 ώρες ο διακομιστής δέχθηκε επίθεση 467 φορές και μετά από τρεις εβδομάδες καταγράφηκαν περισσότερες από 600 επιθέσεις (Ray, 2018).

1.3.11 Ανεπιθύμητη αλληλογραφία και ηλεκτρονική εισβολή

Το ηλεκτρονικό ταχυδρομείο έχει δημιουργήσει μία από τις πιο σοβαρές μορφές εγκλήματος στον κυβερνοχώρο, τις ανεπιθύμητες διαφημίσεις για προϊόντα και υπηρεσίες, οι οποίες οι ειδικοί εκτιμούν ότι αποτελούν περίπου το 50% του ηλεκτρονικού ταχυδρομείου που κυκλοφορεί στο Διαδίκτυο. Το Spam είναι έγκλημα εναντίον όλων των χρηστών του Διαδικτύου, δεδομένου ότι σπαταλά τόσο την ικανότητα αποθήκευσης όσο και τις δυνατότητες δικτύου των ISP. Ωστόσο, παρά τις διάφορες προσπάθειες να νομοθετηθεί εκτός λειτουργίας, παραμένει ασαφές πώς μπορεί να εξαλειφθεί το spam χωρίς να παραβιάζεται η ελευθερία του λόγου σε μια φιλελεύθερη δημοκρατική πολιτεία. Σε αντίθεση με το ανεπιθύμητο ταχυδρομείο, το οποίο έχει σχέση με τα ταχυδρομικά έξοδα, το spam είναι σχεδόν δωρεάν για τους δράστες

- συνήθως κοστίζει το ίδιο για την αποστολή 10 μηνυμάτων όπως και για την αποστολή 10 εκατομμυρίων (Lewis, 2018).

Ένα από τα πιο σημαντικά προβλήματα στο κλείσιμο των spammers αφορά τη χρήση προσωπικών υπολογιστών άλλων ατόμων. Συνήθως, πολλά μηχανήματα που είναι συνδεδεμένα στο Διαδίκτυο μολύνονται πρώτα με ιό ή μέσω του Δούρειου ίππου που δίνει στον spammer μυστικό έλεγχο. Τέτοια μηχανήματα είναι γνωστά ως υπολογιστές «ζόμπι», και δίκτυα αυτών, που συχνά περιλαμβάνουν χιλιάδες μολυσμένους υπολογιστές, μπορούν να ενεργοποιηθούν για να πλημμυρίσουν το Διαδίκτυο με ανεπιθύμητα μηνύματα ή για να προκαλέσουν επιθέσεις DoS. Ενώ το πρώτο μπορεί να είναι σχεδόν καλόηθες, συμπεριλαμβανομένων αιτημάτων για αγορά νόμιμων αγαθών, οι επιθέσεις DoS έχουν αναπτυχθεί σε προσπάθειες εκβιασμού απειλώντας να τους κλείσουν. Οι Cyberexperts εκτιμούν ότι οι Ηνωμένες Πολιτείες αντιπροσωπεύουν περίπου το ένα τέταρτο των 4-8 εκατομμυρίων υπολογιστών ζόμπι στον κόσμο και είναι η προέλευση σχεδόν του ενός τρίτου όλων των ανεπιθύμητων μηνυμάτων (Lewis, 2018).

Το ηλεκτρονικό ταχυδρομείο χρησιμεύει επίσης ως μέσο τόσο για τους παραδοσιακούς εγκληματίες όσο και για τους τρομοκράτες. Ενώ πολλοί επαινούν τη χρήση της κρυπτογραφίας για τη διασφάλιση της ιδιωτικής ζωής στις επικοινωνίες, οι εγκληματίες και οι τρομοκράτες μπορούν επίσης να χρησιμοποιούν κρυπτογραφικά μέσα για να αποκρύψουν τα σχέδιά τους. Αξιωματούχοι επιβολής του νόμου αναφέρουν ότι ορισμένες τρομοκρατικές ομάδες ενσωματώνουν οδηγίες και πληροφορίες σε εικόνες μέσω μιας διαδικασίας γνωστής ως steganography, μια εξελιγμένη μέθοδος απόκρυψης πληροφοριών. Ακόμη και η αναγνώριση ότι κάτι κρύβεται με αυτόν τον τρόπο απαιτεί συχνά σημαντικές ποσότητες υπολογιστικής ισχύος. Στην πραγματικότητα η αποκωδικοποίηση των πληροφοριών είναι σχεδόν αδύνατη εάν δεν έχει το κλειδί για τον διαχωρισμό των κρυφών δεδομένων.

Σε έναν τύπο απάτης που ονομάζεται business e-mail συμβιβασμός (business e-mail compromise / BEC), ένα e-mail που αποστέλλεται σε μια επιχείρηση φαίνεται να προέρχεται από ένα στέλεχος άλλης εταιρείας με την οποία λειτουργεί η επιχείρηση. Στο e-mail, ο «χάκερ» ζητά να μεταφερθούν χρήματα σε έναν συγκεκριμένο λογαριασμό. Το FBI εκτιμά ότι οι απάτες BEC έχουν κοστίσει σε αμερικανικές επιχειρήσεις περίπου 750 εκατομμύρια δολάρια.

Μερικές φορές λαμβάνεται και κυκλοφορεί μήνυμα ηλεκτρονικού ταχυδρομείου που ένας οργανισμός επιθυμεί να κρατήσει μυστικό. Το 2014 οι χάκερ που αποκαλούνταν «Guardians of Peace» κυκλοφόρησαν e-mail από στελέχη της εταιρείας κινηματογραφικών

ταινιών Sony Pictures Entertainment, καθώς και άλλες εμπιστευτικές πληροφορίες της εταιρείας. Οι χάκερ ζήτησαν να μην κυκλοφορήσει η Sony Pictures μια συνέντευξη για συνωμοσία της CIA για δολοφονία του ηγέτη της Βόρειας Κορέας Kim Jong-Un, και απείλησε να επιτεθεί σε θέατρα που έδειχναν την ταινία. Αφού οι αμερικανικές αλυσίδες κινηματογράφου ακύρωσαν τις προβολές, η Sony κυκλοφόρησε την ταινία online και σε περιορισμένη κυκλοφορία. Η ηλεκτρονική εισβολή έχει επηρεάσει ακόμη και την πολιτική. Το 2016 ελήφθησαν e-mail στη Δημοκρατική Εθνική Επιτροπή (Democratic National Committee / DNC) από χάκερ που πιστεύεται ότι ήταν στη Ρωσία. Λίγο πριν από τη Δημοκρατική Εθνική Επιτροπή, ο οργανισμός μέσων ενημέρωσης WikiLeaks κυκλοφόρησε το e-mail, το οποίο έδειξε μια έντονη προτίμηση των αξιωματούχων του DNC για την προεδρική εκστρατεία της Χίλαρι Κλίντον από εκείνη του αμφισβητή της Bernie Sanders. Ο πρόεδρος του DNCH Debbie Wasserman Schultz παραιτήθηκε και ορισμένοι Αμερικανοί σχολιαστές εικάζουν ότι η κυκλοφορία του e-mail έδειξε την προτίμηση της ρωσικής κυβέρνησης για τον Ρεπουμπλικανικό υποψήφιο Donald Trump (Dennis, 2021).

1.3.12 Σαμποτάζ

Ένας άλλος τύπος πειρατείας περιλαμβάνει την πειρατεία ενός ιστότοπου κυβέρνησης ή εταιρίας. Μερικές φορές αυτά τα εγκλήματα έχουν διαπραχθεί ως διαμαρτυρία για την φυλάκιση άλλων χάκερ. Το 1996 ο ιστότοπος της Κεντρικής Υπηρεσίας Πληροφοριών (CIA) άλλαξε από Σουηδούς χάκερ για να κερδίσουν τη διεθνή υποστήριξη για τη διαμαρτυρία τους για τη δίωξη τοπικών χάκερ από τη σουηδική κυβέρνηση ενώ το 1998 η ιστοσελίδα των New York Times παραβιάστηκε από υποστηρικτές του φυλακισμένου χάκερ Kevin Mitnick. Ακόμα άλλοι χάκερ έχουν χρησιμοποιήσει τις δεξιότητές τους για να συμμετάσχουν σε πολιτικές διαμαρτυρίες: το 1998 μια ομάδα που ονομαζόταν «Λεγεώνα του Μετρό» δήλωσε «cyberwar» στην Κίνα και το Ιράκ σε ένδειξη διαμαρτυρίας για φερόμενες παραβιάσεις των ανθρωπίνων δικαιωμάτων και ένα πρόγραμμα κατασκευής όπλων μαζικής καταστροφής, αντίστοιχα. Το 2007, οι ιστότοποι της εσθονικής κυβέρνησης, καθώς και εκείνοι για τις τράπεζες και τα μέσα ενημέρωσης, επίσης, δέχθηκαν επίθεση. Υποψιάστηκαν Ρώσους χάκερ επειδή η Εσθονία ήταν τότε σε διαμάχη με τη Ρωσία σχετικά με την απομάκρυνση ενός σοβιετικού μνημείου πολέμου στο Ταλίν (Ray, 2018).

Η καταστροφή των ιστοτόπων είναι ένα ασήμαντο ζήτημα, ωστόσο, σε σύγκριση με το πρόβλημα των κυβερνο-τρομοκρατών που χρησιμοποιούν το Διαδίκτυο για να επιτεθούν στην

υποδομή ενός έθνους, με εκτροπή της κυκλοφορίας των αεροπορικών εταιρειών, μόλυνση της παροχής νερού ή απενεργοποίηση των διασφαλίσεων πυρηνικών εγκαταστάσεων. Μια από τις συνέπειες των επιθέσεων της 11ης Σεπτεμβρίου στην πόλη της Νέας Υόρκης ήταν η καταστροφή ενός μεγάλου κέντρου εναλλαγής τηλεφώνου και Διαδικτύου. Το Λόουερ Μανχάταν είχε αποκοπεί αποτελεσματικά από τον υπόλοιπο κόσμο, εκτός από τα ραδιόφωνα και τα κινητά τηλέφωνα (Ray, 2018).

Στα τέλη Μαρτίου 2007, το Εθνικό Εργαστήριο του Αϊντάχο κυκλοφόρησε ένα βίντεο που δείχνει ποιες καταστροφικές ζημιές θα μπορούσαν να προκύψουν από βοηθητικά συστήματα που διακυβεύονται από χάκερ Αρκετές επιχειρήσεις κοινής ωφέλειας απάντησαν δίνοντας στην κυβέρνηση των ΗΠΑ άδεια να διενεργήσει έλεγχο στα συστήματά τους. Τον Μάρτιο του 2009 τα αποτελέσματα άρχισαν να διαρρέουν από την έκθεση στην The Wall Street Journal. Συγκεκριμένα, η έκθεση ανέφερε ότι οι χάκερ είχαν εγκαταστήσει λογισμικό σε ορισμένους υπολογιστές που θα τους επέτρεπαν να διακόψουν τις ηλεκτρικές υπηρεσίες. Η εκπρόσωπος της Εσωτερικής Ασφάλειας Amy Kudwa επιβεβαίωσε ότι δεν υπήρξαν διακοπές, αν και θα συνεχιζόντουσαν περαιτέρω έλεγχοι ηλεκτρικού ρεύματος, νερού, λυμάτων και άλλων υπηρεσιών κοινής ωφέλειας (Dennis, 2021).

1.4 ΟΙΚΟΝΟΜΙΚΑ ΕΓΚΛΗΜΑΤΑ

Η απάτη μέσω υπολογιστή είναι οποιαδήποτε ανέντιμη παραπλάνηση των γεγονότων που έχει ως στόχο να αφήσει κάποιον άλλο να κάνει ή να αποφύγει να κάνει κάτι που προκαλεί απώλεια. Στο πλαίσιο αυτό, η απάτη θα έχει ως αποτέλεσμα την επίτευξη οφέλους από (Rosencrance, 2020):

Εικόνα 3: Η απάτη θα έχει ως αποτέλεσμα την επίτευξη οφέλους.

Και αναλυτικότερα:

- Αλλαγή με μη εξουσιοδοτημένο τρόπο. Αυτό απαιτεί μικρή τεχνική εμπειρογνωμοσύνη και είναι μια κοινή μορφή κλοπής από τους υπαλλήλους που τροποποιούν τα δεδομένα πριν από την είσοδο ή την εισαγωγή ψευδών δεδομένων ή εισάγοντας μη εξουσιοδοτημένες οδηγίες ή χρησιμοποιώντας μη εξουσιοδοτημένες διαδικασίες.
- Αλλαγή, καταστροφή, καταστολή ή κλοπή της παραγωγής, συνήθως για την απόκρυψη μη εξουσιοδοτημένων συναλλαγών, κάτι που είναι δύσκολο να εντοπιστεί.
- Τροποποίηση ή διαγραφή αποθηκευμένων δεδομένων.

Άλλες μορφές απάτης μπορούν να διευκολυνθούν με τη χρήση συστημάτων πληροφορικής, συμπεριλαμβανομένης της τραπεζικής απάτης, της κάρτας, της κλοπής ταυτότητας, του εκβιασμού και της κλοπής διαβαθμισμένων πληροφοριών. Αυτού του είδους τα εγκλήματα συχνά έχουν ως αποτέλεσμα την απώλεια ιδιωτικών πληροφοριών ή νομισματικών πληροφοριών.

1.5 ΚΥΒΕΡΝΟΤΡΟΜΟΚΡΑΤΙΑ

Κυβερνητικοί αξιωματούχοι και ειδικοί στον τομέα της ασφάλειας της τεχνολογίας των πληροφοριών έχουν τεκμηριώσει σημαντική αύξηση των προβλημάτων διαδικτύου και των σαρώσεων διακομιστών από τις αρχές του 2001. Υπάρχει μια αυξανόμενη ανησυχία μεταξύ των κυβερνητικών υπηρεσιών, όπως από το Ομοσπονδιακό Γραφείο Ερευνών (Federal Bureau of Investigations / FBI) και την Κεντρική Υπηρεσία Πληροφοριών (Central Intelligence Agency / CIA) ότι τέτοιες εισβολές αποτελούν μέρος μιας οργανωμένης προσπάθειας από τις ξένες υπηρεσίες πληροφοριών ή άλλες ομάδες να χαρτογραφήσουν πιθανές τρύπες ασφαλείας σε κρίσιμα συστήματα. Ο κυβερνοτρόμος εκφοβίζει ή εξαναγκάζει μια κυβέρνηση ή έναν οργανισμό να προωθήσει τους πολιτικούς ή κοινωνικούς στόχους του ξεκινώντας μια επίθεση που βασίζεται σε υπολογιστή εναντίον υπολογιστών, δικτύων ή των πληροφοριών που είναι αποθηκευμένες σε αυτούς.

Η κυβερνοτρομοκρατία, γενικά, μπορεί να οριστεί ως τρομοκρατική ενέργεια που διαπράττεται μέσω της χρήσης του κυβερνοχώρου ή των πόρων υπολογιστών. Ως εκ τούτου, ένα απλό κομμάτι προπαγάνδας στο Διαδίκτυο ότι θα υπάρξουν βομβιστικές επιθέσεις κατά

τη διάρκεια των διακοπών μπορεί να θεωρηθεί κυβερνοτρομοκρατία. Υπάρχουν επίσης δραστηριότητες πειρατείας που απευθύνονται σε άτομα, οικογένειες, οργανωμένες από ομάδες εντός δικτύων, που τείνουν να προκαλούν φόβο στους ανθρώπους, να επιδεικνύουν εξουσία, να συλλέγουν πληροφορίες σχετικές με την καταστροφή της ζωής των ανθρώπων, ληστείες, εκβιασμούς κ.λπ. (Rosencrance, 2020).

1.6 ΚΥΒΕΡΝΟΕΚΘΕΣΗ

Η κυβερνοέκθεση (cyberextortion) συμβαίνει όταν ένας ιστότοπος, ένας διακομιστής ηλεκτρονικού ταχυδρομείου ή ένα σύστημα υπολογιστή υποβάλλεται ή απειλείται με επανειλημμένη άρνηση υπηρεσίας ή άλλες επιθέσεις από κακόβουλους χάκερ. Αυτοί οι χάκερ απαιτούν χρήματα σε αντάλλαγμα για την υπόσχεση να σταματήσουν τις επιθέσεις και να προσφέρουν «προστασία». Σύμφωνα με το Ομοσπονδιακό Γραφείο Ερευνών, οι εκβιαστές του εγκλήματος στον κυβερνοχώρο επιτίθενται όλο και περισσότερο σε εταιρικούς ιστότοπους και δίκτυα, καταστρέφοντας την ικανότητά τους να λειτουργούν και απαιτώντας πληρωμές για την αποκατάσταση των υπηρεσιών τους. Περισσότερες από 20 υποθέσεις αναφέρονται κάθε μήνα στο FBI και πολλές δεν αναφέρονται για να μην δημοσιοποιηθεί το όνομα του θύματος. Οι δράστες συνήθως χρησιμοποιούν μια κατανεμημένη επίθεση άρνησης υπηρεσίας. Ωστόσο, υπάρχουν και άλλες τεχνικές κυβερνοέκθεσης, όπως ο εκβιασμός με doxing και η λαθροθηρία σφαλμάτων.

Ένα παράδειγμα κυβερνοέκθεσης ήταν η επίθεση στη Sony Pictures το 2014. Στις 24 Νοεμβρίου 2014, μια ομάδα χάκερ που ταυτοποιήθηκε με το όνομα «Φύλακες της Ειρήνης» διέρρευσε μια δημοσίευση εμπιστευτικών δεδομένων από το κινηματογραφικό στούντιο Sony Pictures. Τα δεδομένα περιλάμβαναν προσωπικές πληροφορίες σχετικά με τους υπαλλήλους της Sony Pictures και τις οικογένειές τους, μηνύματα ηλεκτρονικού ταχυδρομείου μεταξύ εργαζομένων, πληροφορίες σχετικά με τους μισθούς των στελεχών στην εταιρεία, αντίγραφα ταινιών της Sony που δεν είχαν κυκλοφορήσει, σχέδια για μελλοντικές ταινίες της Sony, σενάρια για ορισμένες ταινίες και άλλες πληροφορίες. Στη συνέχεια, οι δράστες χρησιμοποίησαν μια παραλλαγή του κακόβουλου λογισμικού υαλοκαθαριστήρων Shamoon για να διαγράψουν την υποδομή υπολογιστών της Sony (Rosencrance, 2020).

1.7 CYBERSEX

Η διακίνηση cybersex είναι η μεταφορά των θυμάτων και στη συνέχεια η ζωντανή ροή εξαναγκασμένων σεξουαλικών πράξεων ή βιασμών στην κάμερα. Τα θύματα απάγονται, απειλούνται ή εξαπατώνται και μεταφέρονται στα «κρησφύγετα cybersex». Τα κρησφύγετα μπορούν να είναι σε οποιαδήποτε θέση όπου οι διακινητές cybersex έχουν έναν υπολογιστή, ένα tablet, ή ένα τηλέφωνο με σύνδεση Διαδικτύου. Οι δράστες χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης, τις βιντεοδιασκέψεις, τις σελίδες γνωριμιών, τα σε απευθείας σύνδεση δωμάτια συνομιλίας, τις εφαρμογές, τους σκοτεινούς ιστοτόπους, και άλλες πλατφόρμες. Χρησιμοποιούν τα ηλεκτρονικά συστήματα πληρωμών και τα κρυπτονομίσματα για να κρύψουν τις ταυτότητές τους. Εκατομμύρια εκθέσεις της εμφάνισής του στέλνονται στις διωκτικές αρχές ετησίως. Είναι απαραίτητη μια νέα νομοθεσία και αστυνομικές διαδικασίες για την καταπολέμηση αυτού του είδους εγκλήματος στον κυβερνοχώρο (Jiang, Huang, & Tao, 2013).

1.8 ΗΛΕΚΤΡΟΝΙΚΟ «ΨΑΡΕΜΑ»

1.8.1 Phishing

Στην περίπτωση του ηλεκτρονικού ψαρέματος εκείνος που θέλει να βλάψει επιχειρεί να πάρει από το θύμα του μέσω των μηνυμάτων που στέλνει προσωπικά οικονομικά δεδομένα, όπως είναι τα στοιχεία τραπεζικού λογαριασμού ή πιστωτικής κάρτας. Αρχικά το υποψήφιο θύμα δέχεται ένα email, του οποίου ο αποστολέας εμφανίζεται ότι είναι η τράπεζα του. Με τον τρόπο αυτό ζητείται η επιβεβαίωση του username και του password του λογαριασμού του που διακινεί μέσω web. Η σχετική αιτιολογία αναφέρει προβλήματα στον Η/Υ της τράπεζας ή σε υποψίες ότι ο εν λόγω λογαριασμός έχει παραβιαστεί και σε περίπτωση που δεν γίνει επιβεβαίωση θα κλειδωθεί. Αυτό το email έχει σύνδεσμο προς την τράπεζα, χωρίς να είναι ο πραγματικός με αποτέλεσμα το θύμα να αποστέλλει τα στοιχεία απευθείας σε κάποιον απατεώνα (Τσουραμάνης, 2005).

1.8.2 Pharming

Η κατάχρηση μιας ευπάθειας στην υπηρεσία DNS (Domain Name) είναι το λεγόμενο Pharming, το οποίο δίνει τη δυνατότητα σε έναν hacker να κατευθύνει προς άλλη κατεύθυνση την κυκλοφορία αυτού του δικτυακού τόπου σε άλλο δικτυακό τόπο. Οι δράστες κατορθώνουν να εκτρέψουν τη ροή των επισκεπτών σε άλλον ιστοχώρο, στο οποίο τα καταχωρημένα στοιχεία των συναλλαγών χρησιμοποιούνται για την οικονομική εξαπάτηση των επισκεπτών. Οι δράστες δεν επιδιώκουν να εξαναγκάσουν το θύμα, αλλά κάνουν χρήση προγραμμάτων που ουσιαστικά επαναδρομολογούν την κυκλοφορία των δεδομένων. Ο χρήστης που θέλει να επισκεφθεί μια ιστοσελίδα και να πραγματοποιήσει κάποια συναλλαγή μετά από παρεμβάσεις στο λογισμικό του υπολογιστή του θύματος ή και σε άλλους υπολογιστές, κατευθύνεται σε άλλη σελίδα, αντίγραφο της γνήσιας. Ως εκ τούτου, ο χρήστης καταχωρεί τα στοιχεία του θεωρώντας ότι πρόκειται για την γνήσια ιστοσελίδα, ενώ ουσιαστικά τα «παραδίδει» στην ιστοσελίδα του δράστη. Επίσης, οι δράστες μπορούν να στέλνουν μέσω e-mail προγράμματα, τα οποία αφού εγκατασταθούν στον υπολογιστή του θύματος, συλλέγουν και αποστέλλουν τα στοιχεία (PIN, κωδικούς κ.λπ.) που θέλουν. Στη συνέχεια, τα χρησιμοποιούν προκαλώντας περιουσιακή ζημία στο θύμα (Τσουραμάνης, 2005).

1.9 ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

Ο ιός πρόκειται για ένα πρόγραμμα Η/Υ σχεδιασμένο να μολύνει άλλα προγράμματα με αντίγραφά του. Επειδή δεν μπορεί να αναπαράγεται συνεχώς, υπάρχει η δυνατότητα να μεταδίδεται από ένα σύστημα σε άλλο, προκειμένου να εκτελέσει την αποστολή του η οποία περιλαμβάνει την διαγραφή αρχείων, τη δυσλειτουργία ή και την καταστροφή ολόκληρων συστημάτων ή το σβήσιμο του συνόλου των σκληρών δίσκων.

Πρόκειται δηλαδή για είναι έναν βλαβερό εκτελέσιμο κώδικα, ο οποίος επιζεί με το να «κολλάει» ή να περιέχεται μέσα σε ένα άλλο πρόγραμμα ή σε ένα αρχείο. Δεν πρόκειται για έναν αυτόνομο βλαβερό εκτελέσιμο κώδικα ως ξεχωριστό πρόγραμμα. Επίσης, έχουν παρασιτική συμπεριφορά, διότι επιζούν «μολύνοντας» άλλα αρχεία, όπως συμβαίνει δηλαδή με τη συμπεριφορά, τον τρόπο που ζουν και πολλαπλασιάζονται οι οργανικοί ιοί. Ο πιο συνηθισμένος τρόπος μετάδοσης των ιών αποτελεί η διανομή τους μέσω ηλεκτρονικού ταχυδρομείου (e-mail).

Στη συνέχεια ακολουθούν τα βασικά κριτήρια και οι προσπάθειες των εγκληματιών ώστε να μην γίνουν αντιληπτοί (Τσουραμάνης, 2005):

a) Ιοί οι οποίοι μολύνουν τον τομέα εκκίνησης του σκληρού δίσκου, που περιλαμβάνει εντολές εκκίνησης του υπολογιστή (Boot Viruses).
b) Ιοί που μολύνουν προγράμματα Η/Υ μέσα σε εκτελέσιμα αρχεία (*.exe). Αυτοί τρέχουν μόλις ξεκινήσει το πρόγραμμα που έχουν μολύνει (Software Viruses).
c) Ιοί που προσκολλώνται σε διάφορα τμήματα του λογισμικού ή στο πρόγραμμα ελέγχου εφαρμογών και προσβάλλουν το σύστημα (System Cluster Viruses).
d) Ιοί που κρύβουν τις αλλαγές που κάνουν στον τομέα εκκίνησης ενός συστήματος ή ενός αρχείου, παρεμβαίνοντας στο λογισμικό του προσβαλλόμενου συστήματος (Stealth Viruses).
e) Ιοί που αναπαράγονται ποικιλοτρόπως με σκοπό να πετυχαίνουν την ανθεκτικότητα τους σε σχέση με τα διαφορά προγράμματα Anti-Virus (Polymorphous Viruses).
f) Ιοί που στοχεύουν να καταστρέψουν ή να σβήσουν εντελώς τα προγράμματα Anti-Virus (Retroviruses).
g) Ιοί που μολύνουν τις μακροεντολές σύγχρονων προγραμμάτων εφαρμογών (Data Viruses).

1.10 ΑΝΑΓΚΑΙΟΤΗΤΑ ΥΠΑΡΞΗΣ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (GDPR)

Από τα όσα εκτέθηκαν είναι σαφές ότι η ύπαρξη κατάλληλων νομοθετικών και θεσμικών παρεμβάσεων για την προστασία των προσωπικών δεδομένων στο διαδίκτυο αποτελεί conditio sine qua non για την ασφαλή περιήγηση στο διαδίκτυο. Ο ΓΚΠΔ παρέχει ένα πλέγμα νομοθετικών ρυθμίσεων, τεχνικών μέτρων και διαχείρισης κινδύνου για την αποτροπή ή/και τον μετριασμό της τέλεσης κυβερνοεγκλημάτων και κυβερνοεπιθέσεων, ώστε να τίθεται σε ασφαλές πλαίσιο η περιήγηση και η χρήση του διαδικτύου από τους χρήστες.

Με δεδομένο ότι τα συστήματα και οι τεχνολογίες επικοινωνιών και πληροφορίας αποτελούν σήμερα έναν από τους πιο σημαντικούς παράγοντες οικονομικής και κοινωνικής ανάπτυξης, γίνεται όλο και πιο ουσιαστική η ανάγκη προστασίας τους, έτσι ώστε οποιαδήποτε δραστηριότητα μέσω των τεχνολογιών αυτών να είναι ασφαλής. Ένα βασικό σύστημα ασφάλειας πρέπει να καλύπτει την εμπιστευτικότητα, την ακεραιότητα και την απρόσκοπτη

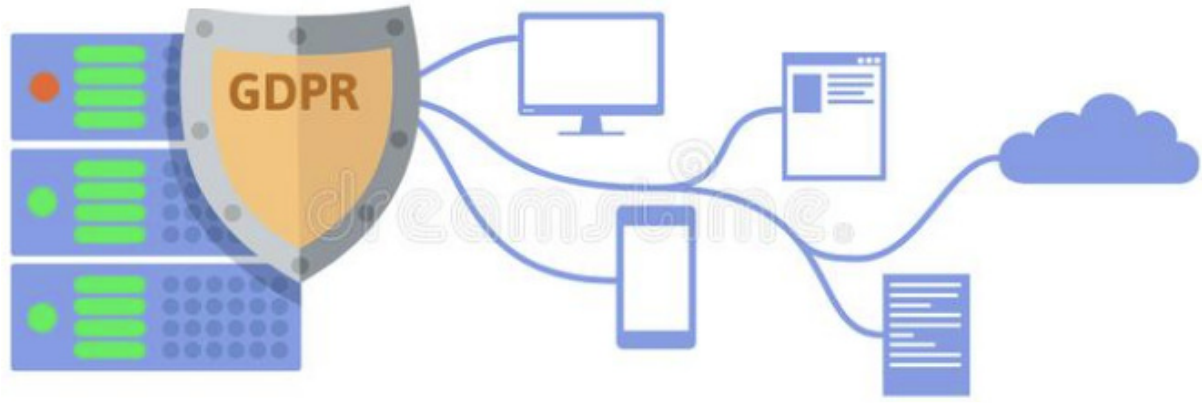
διαθεσιμότητα της υποδομής και των πληροφοριών, ενώ πρέπει να καθιστά τη λειτουργία της υποδομής αξιόπιστη, ευέλικτη και ελεγχόμενη.

Η ύπαρξη ενός ασφαλούς ηλεκτρονικού περιβάλλοντος αυξάνει τον βαθμό εμπιστοσύνης των χρηστών στις νέες τεχνολογίες και εφαρμογές και καθιστά πιο εύκολη τη ψηφιακή μετάβαση, το οποίο αποτελεί και το τελικό ζητούμενο.

2 ΚΕΦΑΛΑΙΟ: «ΕΠΙΣΚΟΠΗΣΗ ΤΟΥ GDPR»

2.1 ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) (ΕΕ) 2016/679 αποτελεί τον κανονισμό της ευρωπαϊκής νομοθεσίας αναφορικά με την προστασία των δεδομένων και της ιδιωτικής ζωής όλων των ατόμων εντός της Ευρωπαϊκής Ένωσης (ΕΕ) και του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ). Ο πρωταρχικός στόχος του GDPR είναι ο έλεγχος των πολιτών όσον αφορά τα προσωπικά τους δεδομένα και η απλοποίηση του ρυθμιστικού περιβάλλοντος για τις διεθνείς επιχειρήσεις με την αφομοίωση του κανονισμού εντός της ΕΕ (Protection of personal data, 2018).



Εικόνα 2.1:Απεικόνιση έννοιας GDPR Γενικός κανονισμός προστασίας δεδομένων.

Η προστασία των προσωπικών στοιχείων Εικονίδιο κεντρικών υπολογιστών και ασπίδων Διάνυσμα, που απομονώνεται στο άσπρο υπόβαθρο.

Πηγή: (Merkusheva, 2018)

Ο κανονισμός αντικαθιστά την οδηγία περί της προστασίας των δεδομένων 95/46 / ΕΚ και περιέχει τις διατάξεις και τις απαιτήσεις που αφορούν την επεξεργασία προσωπικών δεδομένων των ατόμων στο εσωτερικό της Ευρωπαϊκής Ένωσης, και ισχύει για όλες τις επιχειρήσεις, ανεξάρτητα από τη θέση, που συνεργάζονται με τον Ευρωπαϊκό Οικονομικό Χώρο. Δεν επιτρέπεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα εκτός εάν γίνεται σύμφωνα με νόμιμη βάση που καθορίζεται από τον κανονισμό ή εάν ο υπεύθυνος επεξεργασίας έχει λάβει ρητή συγκατάθεση από το πρόσωπο στο οποίο αναφέρονται τα δεδομένα (Jourová, 2016).

Εκείνος που επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα οφείλει να ανακοινώνει με σαφήνεια κάθε συλλογή δεδομένων, να αναφέρει τη νομιμότητα και την επιδίωξη της επεξεργασίας δεδομένων ή τη διάρκεια διατήρησης των δεδομένων. Τα πρόσωπα των οποίων επεξεργάζονται τα δεδομένα μπορούν να ζητήσουν ένα αντίγραφο των δεδομένων τους και μπορούν να ζητήσουν να διαγραφούν τα δεδομένα τους υπό ορισμένες συνθήκες (Protection of personal data, 2018).

2.2 ΥΠΕΥΘΥΝΟΙ ΕΦΑΡΜΟΓΗΣ GDPR

Οι υπεύθυνοι επεξεργασίας και οι επεξεργαστές προσωπικών δεδομένων πρέπει να εφαρμόσουν κατάλληλα τεχνικά και οργανωτικά μέτρα για την εφαρμογή των αρχών προστασίας δεδομένων. Οι επιχειρηματικές διαδικασίες που χειρίζονται προσωπικά δεδομένα πρέπει να σχεδιαστούν και να κατασκευαστούν με γνώμονα τις αρχές και να παρέχουν διασφαλίσεις για την προστασία των δεδομένων (για παράδειγμα, χρησιμοποιώντας ψευδώνυμο ή πλήρη ανωνυμία, όπου απαιτείται). Οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να σχεδιάζουν συστήματα πληροφοριών λαμβάνοντας υπόψη το απόρρητο. Για παράδειγμα, η χρήση των υψηλότερων δυνατών ρυθμίσεων απορρήτου από προεπιλογή, έτσι ώστε τα σύνολα δεδομένων να μην είναι δημόσια διαθέσιμα από προεπιλογή και να μην μπορούν να χρησιμοποιηθούν για την αναγνώριση ενός θέματος. Δεν επιτρέπεται η επεξεργασία προσωπικών δεδομένων εκτός εάν αυτή η επεξεργασία πραγματοποιείται σύμφωνα με μία από τις έξι νόμιμες βάσεις που καθορίζονται από τον κανονισμό (συγκατάθεση, σύμβαση, δημόσιο έργο, ζωτικό συμφέρον, νόμιμο συμφέρον ή νομική απαίτηση). Όταν η επεξεργασία βασίζεται στη συγκατάθεση, το υποκείμενο των δεδομένων έχει το δικαίωμα να την ανακαλέσει ανά πάσα στιγμή (Θεματολογικά δελτία για την Ευρωπαϊκή Ένωση, 2021).

Οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να αποκαλύπτουν σαφώς οποιαδήποτε συλλογή δεδομένων, να δηλώνουν τη νόμιμη βάση και τον σκοπό της επεξεργασίας δεδομένων και να δηλώνουν πόσο καιρό διατηρούνται τα δεδομένα και εάν κοινοποιούνται σε τρίτους ή εκτός του Ευρωπαϊκού Οικονομικού Χώρου / ΕΟΧ (European Economic Area / EEA). Οι εταιρείες έχουν την υποχρέωση να προστατεύουν τα δεδομένα των υπαλλήλων και των καταναλωτών στον βαθμό που μόνο τα απαραίτητα δεδομένα εξάγονται με ελάχιστη παρέμβαση στο απόρρητο των δεδομένων από υπαλλήλους, καταναλωτές ή τρίτους. Οι

επιχειρήσεις πρέπει να έχουν εσωτερικούς ελέγχους και κανονισμούς για διάφορα τμήματα, όπως έλεγχος, εσωτερικοί έλεγχοι και λειτουργίες. Τα υποκείμενα των δεδομένων έχουν το δικαίωμα να ζητήσουν ένα φορητό αντίγραφο των δεδομένων που συλλέγονται από έναν ελεγκτή σε κοινή μορφή και το δικαίωμα να διαγραφούν τα δεδομένα τους υπό ορισμένες συνθήκες. Οι δημόσιες αρχές και οι επιχειρήσεις των οποίων οι βασικές δραστηριότητες συνίστανται σε τακτική ή συστηματική επεξεργασία προσωπικών δεδομένων, υποχρεούνται να απασχολούν έναν υπεύθυνο προστασίας δεδομένων (data protection officer / DPO), ο οποίος είναι υπεύθυνος για τη διαχείριση της συμμόρφωσης με τον GDPR. Οι επιχειρήσεις πρέπει να αναφέρουν παραβιάσεις δεδομένων στις εθνικές εποπτικές αρχές εντός 72 ωρών εάν έχουν αρνητικές επιπτώσεις στο απόρρητο των χρηστών. Σε ορισμένες περιπτώσεις, στους παραβάτες του GDPR ενδέχεται να τους επιβληθούν πρόστιμα έως και 20 εκατομμύρια ευρώ ή έως και 4% του ετήσιου παγκόσμιου κύκλου εργασιών του προηγούμενου οικονομικού έτους σε περίπτωση επιχείρησης, όποιο από τα δύο είναι μεγαλύτερο (Θεματολογικά δελτία για την Ευρωπαϊκή Ένωση, 2021).

Ο κανονισμός έγινε πρότυπο για πολλούς εθνικούς νόμους εκτός ΕΕ, όπως στη Χιλή, στην Ιαπωνία, στη Βραζιλία, στη Νότια Κορέα, στην Αργεντινή και στην Κένυα. Ο νόμος περί απορρήτου των καταναλωτών της Καλιφόρνια (California Consumer Privacy Act / CCPA), που εγκρίθηκε στις 28 Ιουνίου 2018, έχει πολλές ομοιότητες με τον GDPR.

2.3 ΕΞΑΙΡΕΣΕΙΣ

Ορισμένες περιπτώσεις δεν αντιμετωπίζονται ειδικά στο GDPR, και επομένως αντιμετωπίζονται ως εξαιρέσεις. Αυτές είναι οι εξής:

- Προσωπικές ή οικιακές δραστηριότητες
- Επιβολή του νόμου
- Εθνική ασφάλεια

Όταν δημιουργήθηκε ο GDPR, δημιουργήθηκε αυστηρά για τη ρύθμιση των προσωπικών δεδομένων που πηγαίνει στα χέρια των εταιρειών. Αυτό που δεν καλύπτεται από τον GDPR είναι οι μη εμπορικές πληροφορίες ή οι οικιακές δραστηριότητες. Ένα παράδειγμα αυτών των οικιακών δραστηριοτήτων μπορεί να είναι μηνύματα ηλεκτρονικού ταχυδρομείου μεταξύ δύο φίλων γυμνασίου.

Επιπλέον, ο GDPR δεν ισχύει όταν τα δεδομένα συνδέονται ενδεχομένως με αστυνομική έρευνα. Παρόλο που δεν καλύπτεται από τον GDPR, ο νόμος για την προστασία δεδομένων του 2018, το Μέρος 3 καλύπτει ρητά αυτούς τους λόγους.

Τέλος, όταν τα δεδομένα αφορούν την εθνική ασφάλεια, είναι εκτός των ορίων του GPDR, οπότε καλύπτεται από τον Νόμο για την Προστασία Δεδομένων του 2018, Μέρος 2 Κεφάλαιο 3.

Αντίθετα, μια οντότητα ή πιο συγκεκριμένα μια «επιχείρηση» πρέπει να συμμετέχει σε «οικονομική δραστηριότητα» για να καλύπτεται από τον GPDR. Η οικονομική δραστηριότητα ορίζεται ευρέως στο δίκαιο ανταγωνισμού της Ευρωπαϊκής Ένωσης (Lawspot/GDPR: Ενσωματώθηκε στη Συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο, 2018).

2.4 ΕΦΑΡΜΟΓΗ ΕΚΤΟΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΈΝΩΣΗΣ

Ο GDPR ισχύει επίσης για υπεύθυνους επεξεργασίας δεδομένων και επεξεργαστές εκτός του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ) εάν ασχολούνται με την «προσφορά αγαθών ή υπηρεσιών» (ανεξάρτητα από το εάν απαιτείται πληρωμή) σε υποκείμενα δεδομένων εντός του ΕΟΧ ή παρακολουθούν τη συμπεριφορά των υποκειμένων των δεδομένων στον ΕΟΧ (άρθρο 3 παράγραφος 2). Ο κανονισμός ισχύει ανεξάρτητα από το πού γίνεται η επεξεργασία. Αυτό έχει ερμηνευτεί σκόπιμα για να παρέχει εξωεδαφική δικαιοδοσία στο GDPR για ιδρύματα εκτός ΕΕ εάν συνεργάζονται με άτομα που βρίσκονται στην ΕΕ (Lawspot/GDPR: Ενσωματώθηκε στη Συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο, 2018).

2.4.1 Εκπρόσωπος της ΕΕ

Σύμφωνα με το άρθρο 27, τα ιδρύματα εκτός ΕΕ που υπόκεινται στον GPDR υποχρεούνται να έχουν έναν εκπρόσωπο εντός της Ευρωπαϊκής Ένωσης, έναν «εκπρόσωπο της ΕΕ», που θα λειτουργεί ως σημείο επαφής για τις υποχρεώσεις τους βάσει του κανονισμού. Ο εκπρόσωπος της ΕΕ είναι ο υπεύθυνος επικοινωνίας του Ελεγκτή ή του Επεξεργαστή έναντι των Ευρωπαίων εποπτών απορρήτου και των υποκειμένων των δεδομένων, σε όλα τα θέματα που σχετίζονται με την επεξεργασία, για να διασφαλιστεί η συμμόρφωση με τον παρόντα GDPR. Ένα φυσικό (άτομο) ή ηθικό (εταιρικό) άτομο μπορεί να παίξει τον ρόλο ενός εκπροσώπου της ΕΕ. Η εγκατάσταση εκτός ΕΕ πρέπει να εκδώσει ένα δεόντως υπογεγραμμένο

έγγραφο (επιστολή διαπίστευσης) που να ορίζει ένα συγκεκριμένο άτομο ή εταιρεία ως εκπρόσωπο της ΕΕ. Η εν λόγω ονομασία μπορεί να δοθεί μόνο γραπτώς.

Η αποτυχία ενός ιδρύματος να ορίσει έναν εκπρόσωπο της ΕΕ θεωρείται άγνοια του κανονισμού και των σχετικών υποχρεώσεων, η οποία από μόνη της αποτελεί παραβίαση του GDPR με την επιβολή προστίμων έως και 10 εκατομμύρια ευρώ ή έως και 2% του ετήσιου παγκόσμιου κύκλου εργασιών του προηγούμενου οικονομικού έτους σε περίπτωση επιχείρησης, όποιο από τα δύο είναι μεγαλύτερο. Ο εκ προθέσεως ή αμελής χαρακτήρας της παράβασης (αποτυχία ορισμού εκπροσώπου της ΕΕ) μπορεί μάλλον να συνιστά επιβαρυντικούς παράγοντες.

Ένα ίδρυμα δεν χρειάζεται να ορίσει έναν εκπρόσωπο της ΕΕ εάν συμμετέχει σε περιστασιακή επεξεργασία που δεν περιλαμβάνει, σε ευρεία κλίμακα, επεξεργασία ειδικών κατηγοριών δεδομένων όπως αναφέρεται στο άρθρο 9 παράγραφος 1 του GDPR ή την επεξεργασία προσωπικών δεδομένων που σχετίζονται σε ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10, και η εν λόγω επεξεργασία είναι απίθανο να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, λαμβάνοντας υπόψη τη φύση, το πλαίσιο, το πεδίο εφαρμογής και τους σκοπούς της επεξεργασίας. Εξαιρούνται επίσης οι δημόσιες αρχές και οι οργανισμοί εκτός ΕΕ (Lawspot/GDPR: Ενσωματώθηκε στη Συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο, 2018).

2.4.2 Τρίτες χώρες

Το κεφάλαιο V του GDPR απαγορεύει τη μεταφορά των προσωπικών δεδομένων των υποκειμένων των δεδομένων της ΕΕ σε χώρες εκτός του ΕΟΧ - γνωστά ως τρίτες χώρες - εκτός εάν επιβληθούν κατάλληλες διασφαλίσεις, ή οι κανονισμοί προστασίας δεδομένων τρίτων χωρών θεωρούνται επίσημα επαρκείς από την Ευρωπαϊκή Επιτροπή (Άρθρο 45). Μεταξύ παραδειγμάτων είναι οι δεσμευτικοί εταιρικοί κανόνες, οι τυποποιημένες συμβατικές ρήτρες για την προστασία δεδομένων που εκδίδονται από ένα DPA ή ένα σύστημα δεσμευτικών και εκτελεστών δεσμεύσεων από τον υπεύθυνο επεξεργασίας δεδομένων ή τον επεξεργαστή που βρίσκεται σε τρίτη χώρα (Lawspot/GDPR: Ενσωματώθηκε στη Συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο, 2018).

2.4.3 Εφαρμογή στο Ηνωμένο Βασίλειο

Η δυνατότητα εφαρμογής του GDPR στο Ηνωμένο Βασίλειο επηρεάστηκε από το Brexit. Αν και το Ηνωμένο Βασίλειο αποχώρησε επισήμως από την Ευρωπαϊκή Ένωση στις

31 Ιανουαρίου 2020, παρέμεινε υπό το δίκαιο της ΕΕ, συμπεριλαμβανομένου του GDPR, έως το τέλος της μεταβατικής περιόδου στις 31 Δεκεμβρίου 2020. Το Ηνωμένο Βασίλειο χορήγησε βασιλική σύμφωνη γνώμη για την προστασία δεδομένων Νόμος 2018 στις 23 Μαΐου 2018, ο οποίος αύξησε τον GDPR, συμπεριλαμβανομένων πτυχών του κανονισμού που θα καθοριστεί από το εθνικό δίκαιο, και ποινικών αδικημάτων για τη λήψη εν γνώσει ή αμέλεια απόκτησης, αναδιανομής ή διατήρησης προσωπικών δεδομένων χωρίς τη συγκατάθεση του υπευθύνου επεξεργασίας δεδομένων.

Σύμφωνα με τον νόμο της Ευρωπαϊκής Ένωσης (Απόσυρση) 2018 , το υφιστάμενο και σχετικό δίκαιο της ΕΕ μεταφέρθηκε στο τοπικό δίκαιο μετά την ολοκλήρωση της μετάβασης και το GDPR τροποποιήθηκε με νόμιμο μέσο για την κατάργηση ορισμένων διατάξεων που δεν χρειάζονται πλέον λόγω της μη συμμετοχής του Ηνωμένου Βασιλείου στο ΕΕ. Στη συνέχεια, ο κανονισμός θα αναφέρεται ως «GDPR του Ηνωμένου Βασιλείου». Το Ηνωμένο Βασίλειο δεν θα περιορίσει τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε χώρες εντός του ΕΟΧ βάσει του GDPR του ΗΒ. Ωστόσο, το Ηνωμένο Βασίλειο θα γίνει τρίτη χώρα βάσει του EU GDPR, που σημαίνει ότι τα προσωπικά δεδομένα ενδέχεται να μην διαβιβάζονται στη χώρα, εκτός εάν επιβληθούν κατάλληλες διασφαλίσεις, ή εκτός εάν η Ευρωπαϊκή Επιτροπή λαμβάνει απόφαση επάρκειας σχετικά με την καταλληλότητα της βρετανικής νομοθεσίας για την προστασία δεδομένων (Κεφάλαιο V). Στο πλαίσιο της συμφωνίας απόσυρσης, η Ευρωπαϊκή Επιτροπή δεσμεύτηκε να πραγματοποιήσει αξιολόγηση της επάρκειας (Lawspot/GDPR: Ενσωματώθηκε στη Συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο, 2018).

Τον Απρίλιο του 2019, το Γραφείο Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου (ICO) εξέδωσε έναν προτεινόμενο κώδικα πρακτικής για υπηρεσίες κοινωνικής δικτύωσης όταν χρησιμοποιείται από ανηλίκους, ο οποίος μπορεί να εφαρμοστεί βάσει του GDPR, ο οποίος περιλαμβάνει επίσης περιορισμούς στους μηχανισμούς «like» και «streak» για να αποθαρρύνει τον εθισμό στα μέσα κοινωνικής δικτύωσης και τη χρήση αυτών των δεδομένων για την επεξεργασία ενδιαφερόντων.

Τον Μάρτιο του 2021, ο υφυπουργός Ψηφιακών, Πολιτισμού, Μέσων Ενημέρωσης και Αθλητισμού Oliver Dowden δήλωσε ότι το Ηνωμένο Βασίλειο διερευνά την απόκλιση από το GDPR της ΕΕ προκειμένου να «[εστιάσει] περισσότερο στα αποτελέσματα που θέλουμε να έχουμε και λιγότερο στα βάρη των τους κανόνες που επιβάλλονται σε μεμονωμένες επιχειρήσεις».

2.5 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ GDPR

Ο κανονισμός εφαρμόζεται από τον υπεύθυνο επεξεργασίας δεδομένων (ένας οργανισμός που συλλέγει δεδομένα από κάτοικους της ΕΕ) ή τον μεταποιητή (ένας οργανισμός που επεξεργάζεται δεδομένα για λογαριασμό υπεύθυνου επεξεργασίας δεδομένων όπως οι πάροχοι υπηρεσιών Cloud computing[1]) ή το πρόσωπο στο οποίο αναφέρονται τα δεδομένα (πρόσωπο). Υπό ορισμένες συνθήκες, ο κανονισμός εφαρμόζεται επίσης σε οργανισμούς που εδρεύουν εκτός ΕΕ, εάν συλλέγουν ή επεξεργάζονται προσωπικά δεδομένα ατόμων που βρίσκονται εντός της ΕΕ. (Data protection in the EU, 2018).

Σύμφωνα με την Ευρωπαϊκή Επιτροπή, «τα προσωπικά δεδομένα είναι οποιαδήποτε πληροφορία που αφορά ένα άτομο, είτε σχετίζεται με την ιδιωτική, επαγγελματική ή δημόσια ζωή του, μπορεί να είναι οτιδήποτε από ένα όνομα, μια διεύθυνση κατοικίας, μια φωτογραφία, τραπεζικές λεπτομέρειες, αναρτήσεις σε ισότοπους κοινωνικής δικτύωσης, ιατρικές πληροφορίες ή διεύθυνση IP υπολογιστή» (Προστασία δεδομένων στην ΕΕ, 2018).

Ο κανονισμός δεν έχει ως στόχο να εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα για δραστηριότητες εθνικής ασφάλειας ή για επιβολή του νόμου στην ΕΕ. Το άρθρο 48 ορίζει ότι οποιαδήποτε απόφαση δικαστηρίου και οποιαδήποτε απόφαση διοικητικής αρχής τρίτης χώρας που απαιτεί από τον υπεύθυνο επεξεργασίας ή τον μεταποιητή να μεταβιβάσει ή να αποκαλύψει προσωπικά δεδομένα δεν μπορεί να αναγνωριστεί ή να εκτελεσθεί με οποιονδήποτε τρόπο εκτός εάν βασίζεται σε διεθνή συμφωνία, μια συνθήκη αμοιβαίας δικαστικής συνδρομής ισχύουσα μεταξύ της αιτούσας τρίτης χώρας (εκτός ΕΕ) και της ΕΕ ή ενός κράτους μέλους. Η δέσμη μεταρρυθμίσεων για την προστασία των δεδομένων περιλαμβάνει επίσης ξεχωριστή οδηγία για την προστασία των δεδομένων για τον τομέα της αστυνομίας και της ποινικής δικαιοσύνης, η οποία προβλέπει κανόνες για την ανταλλαγή προσωπικών δεδομένων σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο.

Ένα ενιαίο σύνολο κανόνων θα ισχύει για όλα τα κράτη μέλη της ΕΕ. Κάθε κράτος μέλος θα συστήσει μια ανεξάρτητη εποπτική αρχή (ΑΕΑ) για να ακούσει και να διερευνήσει καταγγελίες, να τιμωρήσει διοικητικά αδικήματα κλπ. Οι ΑΕΑ σε κάθε κράτος μέλος θα

[1]Υπηρεσίες τεχνολογίας πληροφορικής (IT) που επιτρέπουν την συνεχή πρόσβαση σε κοινόχρηστες βάσεις δεδομένων διαμορφωμένων πόρων συστήματος και υπηρεσιών υψηλότερου επιπέδου που μπορούν γρήγορα να παρέχονται με ελάχιστη προσπάθεια διαχείρισης, μέσω του Διαδικτύου.

συνεργαστούν με άλλες ΑΕ, παρέχοντας αμοιβαία συνδρομή και οργανώνοντας κοινές επιχειρήσεις. Η κυρίαρχη αρχή θα λειτουργήσει ως «μονοαπευθυντική θυρίδα» για την επίβλεψη όλων των δραστηριοτήτων επεξεργασίας αυτής της επιχείρησης σε ολόκληρη την ΕΕ (άρθρα 46-55 του GDPR). Ένα Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (European Data Protection Board - EDPB) θα συντονίσει τις ΑΕ. Το EDPB θα αντικαταστήσει την ομάδα εργασίας για την προστασία δεδομένων του άρθρου 29. (Protection of personal data, 2018).

2.6 ΝΟΜΙΜΗ ΒΑΣΗ GDPR

Εάν ένα υποκείμενο των δεδομένων έχει δώσει ρητή συγκατάθεση για την επεξεργασία δεδομένων για έναν ή περισσότερους σκοπούς, τότε τα προσωπικά δεδομένα ενδέχεται να μην υποβάλλονται σε επεξεργασία, εκτός εάν υπάρχει τουλάχιστον μία νομική βάση για να γίνει κάτι τέτοιο (Επίσημη Εφημερίδα τον Ευρωπαϊκών Κοινοτήτων, 1995):

- Για τα νόμιμα συμφέροντα ενός υπεύθυνου επεξεργασίας δεδομένων ή ενός τρίτου, εκτός εάν αυτά τα συμφέροντα παραβιάζονται από τον Χάρτη των Θεμελιωδών Δικαιωμάτων(ιδίως στην περίπτωση των παιδιών).
- Να εκτελεί καθήκον δημοσίου συμφέροντος ή δημόσιας εξουσίας.
- Να συμμορφωθεί με τις νομικές υποχρεώσεις του υπεύθυνου επεξεργασίας δεδομένων.
- Να εκπληρώνει τις συμβατικές υποχρεώσεις με ένα υποκείμενο των δεδομένων.
- Να εκτελεί καθήκοντα κατόπιν αιτήσεως ενός υποκειμένου των δεδομένων το οποίο βρίσκεται στη διαδικασία σύναψης σύμβασης με υπεύθυνο επεξεργασίας δεδομένων.
- Να προστατεύει τα ζωτικά συμφέροντα ενός υποκειμένου των δεδομένων ή άλλου προσώπου.

Εάν η συγκατάθεση χρησιμοποιείται ως νόμιμη βάση για τη μεταποίηση, η συγκατάθεση πρέπει να είναι ρητή για τα δεδομένα που συλλέγονται και χρησιμοποιούνται για κάθε σκοπό (άρθρο 7, όπως ορίζεται στο άρθρο 4). Οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να μπορούν να αποδείξουν τη συγκατάθεσή τους («opt-in») και η συγκατάθεσή τους μπορεί να αποσυρθεί. Η συγκατάθεση των παιδιών, που ορίζεται στον κανονισμό ως ηλικία κάτω των 16 ετών, πρέπει να δοθεί από τον γονέα του παιδιού ή τον κηδεμόνα (άρθρο8).

Η παροχή υπηρεσίας στο υποκείμενο των δεδομένων δεν μπορεί να εξαρτάται από τη συγκατάθεσή του στην επεξεργασία δεδομένων που δίνει είναι απολύτως απαραίτητη για τη χρήση της υπηρεσίας (Άρθρο 7, παράγραφος 4).

Εάν για την επεξεργασία είχε ήδη χορηγηθεί συναίνεση σύμφωνα με την οδηγία για την προστασία των δεδομένων, ο υπεύθυνος επεξεργασίας δεν χρειάζεται να λάβει νέα/ανανεωμένη συγκατάθεση εάν η επεξεργασία τεκμηριώνεται και λαμβάνεται σύμφωνα με τις απαιτήσεις της GDPR.

2.7 ΣΥΝΟΨΗ ΤΩΝ ΑΡΘΡΩΝ ΠΟΥ ΠΕΡΙΕΧΟΝΤΑΙ ΣΤΟ GDPR

Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Summary of Articles Contained in the GDPR, 2018).

Τα άρθρα που περιέχονται στο GDPR φαίνονται στο παρακάτω Σχήμα 2.1.

Σχήμα 2.1: Τα άρθρα που περιέχονται στο GDPR.

Πηγή: (Summary of Articles Contained in the GDPR, 2018).

2.8 ΕΠΙΣΚΟΠΗΣΗ ΒΑΣΙΚΩΝ ΣΥΜΒΑΝΤΩΝ GDPR

Μια επισκόπηση των βασικών συμβάντων GDPR από την πρόταση, την τροποποίηση, την έγκριση, την υιοθέτηση έως την εφαρμογή έχει ως εξής (GDPR Timeline of Events, 2018):

1. **Προηγούμενη νομοθεσία**

- «1995-24 Οκτωβρίου, η οδηγία 95/46/ΕΚ για την προστασία των δεδομένων που δημιουργήθηκε για τη ρύθμιση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα».

2. **Νομοθετικές προτάσεις**

- «2012-25 Ιανουαρίου, αρχική πρόταση για επικαιροποιημένη ρύθμιση προστασίας δεδομένων από την Ευρωπαϊκή Επιτροπή».
- «2014-12 Μαρτίου, το Ευρωπαϊκό Κοινοβούλιο ενέκρινε τη δική του εκδοχή του κανονισμού στην πρώτη του ανάγνωση».
- «2015-15 Ιουνίου, το Συμβούλιο της Ευρωπαϊκής Ένωσης ενέκρινε την πρώτη του ανάγνωση, γνωστή ως γενική προσέγγιση, επιτρέποντας στον κανονισμό να περάσει στο τελικό στάδιο της νομοθεσίας που είναι γνωστή ως '*Τριόγκο*'».

3. Χρονοδιάγραμμα τριλόγων

- 2015-24 Ιουνίου, συνεδρίαση που εφαρμόζει:
    - «Προσέγγιση δέσμης: Στόχος της προεδρίας του Λουξεμβούργου για την προτεινόμενη οδηγία».
    - «Συμφωνία για τον γενικό χάρτη πορείας για τις διαπραγματεύσεις του τριμερούς διαλόγου».
    - «Γενική μέθοδος και προσέγγιση για τις κατ' εξουσιοδότηση πράξεις και τις εκτελεστικές πράξεις».
- 2015-14 Ιουλίου, συνεδρίαση που εφαρμόζει:
    - «Εδαφικό πεδίο εφαρμογής (άρθρο3), αντιπρόσωπος (άρθρο25)».
    - «Διεθνείς μεταφορές (Κεφάλαιο V), σχετικοί ορισμοί».
- 2015-16-17 Σεπτεμβρίου, συνεδρίαση που εφαρμόζει:
    - «Αρχές προστασίας δεδομένων (κεφάλαιο II)».
    - «Δικαιώματα των υποκειμένων των δεδομένων (κεφάλαιο III)».
    - «Ελεγκτής και Επεξεργαστής (Κεφάλαιο IV)».
- 2015-29-30 Σεπτεμβρίου, συνεδρίαση που εφαρμόζει:
    - «Αρχές προστασίας δεδομένων (κεφάλαιο II)».
    - «Δικαιώματα των υποκειμένων των δεδομένων (κεφάλαιο III)».
    - «Ελεγκτής και Επεξεργαστής (Κεφάλαιο IV)».
- 2015-15 Οκτωβρίου, Τρίλογος που εφαρμόζει:
    - «Ανεξάρτητες Εποπτικές Αρχές (Κεφάλαιο VI)».
    - «Συνεργασία και συνοχή (κεφάλαιο VII)».
    - «Διορθωτικά μέτρα, ευθύνη και κυρώσεις (Κεφάλαιο VIII)».
- 2015-28 Οκτωβρίου, συνεδρίαση που εφαρμόζει:
    - «Ανεξάρτητες Εποπτικές Αρχές (Κεφάλαιο VI)».

- «Συνεργασία και συνοχή (κεφάλαιο VII)».
- «Διορθωτικά μέτρα, ευθύνη και κυρώσεις (Κεφάλαιο VIII)».

- 2015-11-12 Νοεμβρίου, συνεδρίαση που εφαρμόζει:
  - «Στόχοι και υλικό πεδίο (Κεφάλαιο I)».
  - «Ειδικά καθεστώτα (Κεφάλαιο IX)».
- 2015-24 Νοεμβρίου, συνεδρίαση που εφαρμόζει:
  - «Όλα τα ανοιχτά θέματα από τα κεφάλαια I έως IX».
- 2015-10 Δεκεμβρίου, συνεδρίαση που εφαρμόζει:
  - «Κατ' εξουσιοδότηση πράξεις (κεφάλαιο X)»
  - «Τελικές διατάξεις (Κεφάλαιο XI)»
  - «Εναλλακτικά θέματα».
- 2015-15 Δεκεμβρίου, συνεδρίαση που εφαρμόζει:
  - «Κατ' εξουσιοδότηση πράξεις (κεφάλαιο X)»
  - «Τελικές διατάξεις (Κεφάλαιο XI)»
  - «Εναλλακτικά θέματα».

4. Έγκριση και Υιοθέτηση

- «2015-15 Δεκεμβρίου, το Κοινοβούλιο και το Συμβούλιο κατέληξαν σε συμφωνία, και το κείμενο θα είναι τελικό από την υπογραφή του επίσημου που θα γίνει στις αρχές Ιανουαρίου του 2016».
- 2016- Ιανουάριος
  - «8 Απριλίου- Έγκριση από το Συμβούλιο της Ευρωπαϊκής Ένωσης».
  - «16 Απριλίου- Έγκριση από το Ευρωπαϊκό Κοινοβούλιο».
  - «Μάιος- Ο κανονισμός θα τεθεί σε ισχύ 20 ημέρες μετά τη δημοσίευσή του στην Επίσημη Εφημερίδα της ΕΕ».

5. Επιβολή

- «2018- Μάιος- Μετά από μια περίοδο χάριτος 2 ετών μετά την υιοθέτηση, το GDPR θα καταστεί πλήρως εκτελεστό σε ολόκληρη την Ευρωπαϊκή Ένωση».

2.9 ΑΜΦΙΛΕΓΟΜΕΝΑ ΘΕΜΑΤΑ ΓΙΑ ΤΟ GDPR

Ένας από τους βασικούς παράγοντες που οδήγησαν στη δημιουργία ενός νέου κανονισμού ήταν η εναρμόνιση των νόμων για την προστασία των δεδομένων σε όλη την

Ευρώπη και η αρχή της ενιαίας θυρίδας φαίνεται να είναι μια λογική προσθήκη. Ωστόσο, η αρχή δεν είναι τόσο απλή στην πράξη όσο μπορεί να εμφανιστεί σε χαρτί και η αρχική πρόταση της Επιτροπής τροποποιήθηκε έντονα από τις μεταγενέστερες υιοθεσίες GDPR.

Η πρόταση της Επιτροπής στο άρθρο 15 είναι μακράν η πιο απλή και γενικότερη προσέγγιση: Όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματοποιείται στο πλαίσιο δραστηριοτήτων μιας εγκατάστασης ελεγκτή ή μεταποιητή στην Ένωση και ο υπεύθυνος της επεξεργασίας ή ο μεταποιητής είναι εγκατεστημένος σε περισσότερα του ενός κράτη μέλη, η εποπτική αρχή της κύριας εγκατάστασης του υπεύθυνου επεξεργασίας ή του μεταποιητή είναι αρμόδια για την εποπτεία των δραστηριοτήτων επεξεργασίας του υπευθύνου επεξεργασίας ή του μεταποιητή σε όλα τα κράτη μέλη.

Το Κοινοβούλιο εξέφρασε την ανησυχία του για την ενδεχόμενη παραβίαση των δικαιωμάτων των υποκειμένων των δεδομένων όταν δεν είναι σε θέση να υποβάλουν εύκολα καταγγελία σε αρμόδιο DPA εάν, για παράδειγμα, οι επαφές γίνονται δύσκολα από γλώσσα ή οικονομικά μέσα. Στο άρθρο 54 του εγκριθέντος κειμένου, το Κοινοβούλιο εξακολουθεί να βασίζεται σε επικεφαλής DPA για την εξάλειψη των ένδικων μέσων, αλλά απαιτεί τη συνεργασία όλων των ενδιαφερόμενων ΑΠΔ. Το ποσό των εμπλεκόμενων DPA θα αυξηθεί επίσης σημαντικά δεδομένου ότι προστίθεται επίσης μια διάταξη για τα πρόσωπα στα οποία αναφέρονται τα δεδομένα να καταθέτουν καταγγελίες στην τοπική DPA τους, προκειμένου να συνεργάζονται με τον επικεφαλής DPA για λογαριασμό του υποκειμένου των δεδομένων. Τέλος, ο ρόλος του Συμβουλίου Προστασίας Δεδομένων αυξάνεται όσον αφορά την ικανότητά του να αποφασίζει στην περίπτωση μιας ασαφούς προτίμησης DPA και την τελική απόφαση του σε περίπτωση επικλήσεως του μηχανισμού συνέπειας.

Το Συμβούλιο έχει αναμφισβήτητα την πιο «αποδυναμωμένη» εκδοχή μιας ενιαίας θυρίδας στην υιοθετημένη γενική προσέγγισή της. Παρέχει σε κάθε DPA την αρμοδιότητα να επιβάλλει το GDPR στην κυριότητά του και απαιτεί από τον επικεφαλής DPA να συμβουλεύεται και να μοιράζεται όλες τις πληροφορίες με κάθε ενδιαφερόμενο DPA. Επιτρέπει επίσης σε κάθε ενδιαφερόμενη DPA να παραπέμψει μια υπόθεση στο Συμβούλιο Προστασίας Δεδομένων εάν πιστεύει ότι ο επικεφαλής DPA δεν έχει λάβει υπόψη τη γνώμη του. Συνολικά, αυτό αυξάνει τη σχετική γραφειοκρατία σε σημείο πέραπό την αρχική πρόθεση της αρχής της ενιαίας θυρίδας και επιτρέπει τη δυνατότητα των «ιδιόρρυθμων παραπομπών» που υπονομεύουν την εξουσία της επικεφαλής DPA και ενδεχομένως να

ασκήσουν πίεση Το Συμβούλιο Προστασίας Δεδομένων, το οποίο έχει συσταθεί στο πλαίσιο του GDPR αλλά δεν διαθέτει καμία συγκεκριμένη χρηματοδότηση ή υποδομή.

Ο διάχυτος διάλογος σε ολόκληρη την αρχή της ενιαίας θυρίδας είναι η πράξη εξισορρόπησης μεταξύ της μείωσης της γραφειοκρατίας με την εναρμόνιση των νομοθεσιών για την προστασία των δεδομένων σε ολόκληρη την Ευρώπη και της διασφάλισης των δικαιωμάτων των προσώπων στα οποία αναφέρονται τα δεδομένα εξασφαλίζεται από τη δυνατότητα προσφυγής τους με την κατάλληλη DPA (Controversial Topics GDPR, 2018).

2.10 ΕΠΙΠΤΩΣΕΙΣ ΕΦΑΡΜΟΓΗΣ ΤΟΥ GDPR

Ακαδημαϊκοί εμπειρογνώμονες που συμμετείχαν στη διαμόρφωση του GDPR έγραψαν ότι ο νόμος είναι η πιο επακόλουθη κανονιστική ανάπτυξη στην πολιτική πληροφοριών σε μια γενιά. Ο GDPR φέρνει τα προσωπικά δεδομένα σε ένα περίπλοκο και προστατευτικό ρυθμιστικό καθεστώς.

Παρά το γεγονός ότι είχαν τουλάχιστον δύο χρόνια για να προετοιμαστούν, πολλές εταιρείες και ιστότοποι άλλαξαν τις πολιτικές απορρήτου και τις λειτουργίες τους παγκοσμίως πριν από την εφαρμογή του GDPR και συνήθως παρείχαν email και άλλες ειδοποιήσεις που συζητούσαν αυτές τις αλλαγές. Αυτό επικρίθηκε επειδή είχε ως αποτέλεσμα έναν κουραστικό αριθμό επικοινωνιών, ενώ οι ειδικοί σημείωσαν ότι ορισμένα μηνύματα ηλεκτρονικού ταχυδρομείου υπενθύμισης ισχυρίστηκαν λανθασμένα ότι έπρεπε να ληφθεί νέα συναίνεση για την επεξεργασία δεδομένων για το πότε τέθηκε σε ισχύ ο GDPR (οποιαδήποτε προηγούμενη συγκατάθεση για επεξεργασία ισχύει, εφόσον πληρούσε τις απαιτήσεις του κανονισμού). Οι απάτες ηλεκτρονικού «ψαρέματος» εμφανίστηκαν επίσης χρησιμοποιώντας ψευδείς εκδόσεις των μηνυμάτων ηλεκτρονικού ταχυδρομείου που σχετίζονται με το GDPR και υποστηρίχθηκε επίσης ότι ορισμένα μηνύματα ηλεκτρονικού ταχυδρομείου ειδοποίησης του GDPR ενδέχεται να έχουν αποσταλεί κατά παράβαση των νόμων κατά των ανεπιθύμητων μηνυμάτων. Τον Μάρτιο του 2019, ένας πάροχος λογισμικού συμμόρφωσης διαπίστωσε ότι πολλοί ιστότοποι που διαχειρίζονται οι κυβερνήσεις των κρατών μελών της ΕΕ περιείχαν ενσωματωμένη παρακολούθηση από παρόχους τεχνολογίας διαφημίσεων.

Ο κατακλυσμός των ειδοποιήσεων που σχετίζονται με το GDPR ενέπνευσε επίσης τα μιμίδια, συμπεριλαμβανομένων εκείνων που περιβάλλουν τις ειδοποιήσεις για την πολιτική

απορρήτου που παραδόθηκαν με άτυπα μέσα. Ένα blog, το GDPR Hall of Shame, δημιουργήθηκε για να παρουσιάσει ασυνήθιστη παράδοση ειδοποιήσεων GDPR και απόπειρες συμμόρφωσης που περιείχαν τρομερές παραβιάσεις των απαιτήσεων του κανονισμού. Ο συγγραφέας του παρατήρησε ότι ο κανονισμός «έχει πολλές λεπτομέρειες, αλλά δεν έχει πολλές πληροφορίες σχετικά με τον τρόπο συμμόρφωσης», αλλά επίσης αναγνώρισε ότι οι επιχειρήσεις είχαν δύο χρόνια να συμμορφωθούν, καθιστώντας ορισμένες από τις απαντήσεις του αδικαιολόγητες.

Η έρευνα δείχνει ότι περίπου το 25% των ευπαθειών λογισμικού έχουν επιπτώσεις στο GDPR. Δεδομένου ότι το άρθρο 33 δίνει έμφαση στις παραβιάσεις, όχι στα σφάλματα, οι εμπειρογνώμονες ασφαλείας συμβουλεύουν τις εταιρείες να επενδύσουν σε διαδικασίες και δυνατότητες για τον εντοπισμό τρωτών σημείων πριν από την εκμετάλλευσή τους, συμπεριλαμβανομένων των συντονισμένων διαδικασιών αποκάλυψης ευπάθειας. Μια έρευνα σχετικά με τις πολιτικές απορρήτου των εφαρμογών Android, τις δυνατότητες πρόσβασης σε δεδομένα και τη συμπεριφορά πρόσβασης σε δεδομένα έδειξε ότι πολλές εφαρμογές εμφανίζουν μια κάπως φιλική προς το απόρρητο συμπεριφορά από την εφαρμογή του GDPR, ωστόσο εξακολουθούν να διατηρούν τα περισσότερα από τα προνόμια πρόσβασης στα δεδομένα τους στον κωδικό τους. Μια έρευνα του Συμβουλίου Καταναλωτών της Νορβηγίας (που ονομάζεται Forbrukerrådet στα Νορβηγικά) σχετικά με τους πίνακες εργαλείων μετά το GDPR σε πλατφόρμες κοινωνικών μέσων (όπως ο πίνακας ελέγχου Google) κατέληξε στο συμπέρασμα ότι μεγάλες εταιρείες κοινωνικών μέσων χρησιμοποιούν παραπλανητικές τακτικές προκειμένου να αποθαρρύνουν τους πελάτες τους να ακονίσουν τις ρυθμίσεις απορρήτου τους.

Την ημερομηνία έναρξης ισχύος, ορισμένοι διεθνείς ιστότοποι άρχισαν να αποκλείουν εντελώς τους χρήστες της ΕΕ (συμπεριλαμβανομένων των Instapaper, Unroll.me, και εφημερίδων που ανήκουν στην Tribune Publishing, όπως το Chicago Tribune και οι Los Angeles Times) ή να τους ανακατευθύνουν απογυμνωμένες εκδόσεις των υπηρεσιών τους στην περίπτωση του Εθνικού Δημόσιου Ραδιοφώνου και των ΗΠΑ με περιορισμένη λειτουργικότητα ή / και χωρίς διαφημίσεις, έτσι ώστε να μην είναι υπεύθυνες. Ορισμένες εταιρείες, όπως η Klout, και πολλά διαδικτυακά βιντεοπαιχνίδια, σταμάτησαν να λειτουργούν εντελώς ώστε να συμπίπτουν με την εφαρμογή του, αναφέροντας το GDPR ως επιβάρυνση για τη συνέχιση των δραστηριοτήτων τους, ειδικά λόγω του επιχειρηματικού μοντέλου του

πρώτου. Ο όγκος των πωλήσεων διαδικτυακών τοποθετήσεων διαφημίσεων συμπεριφοράς στην Ευρώπη μειώθηκε κατά 25-40% στις 25 Μαΐου 2018.

Το 2020, δύο χρόνια μετά την έναρξη της εφαρμογής του GDPR, η Ευρωπαϊκή Επιτροπή αξιολόγησε ότι οι χρήστες σε ολόκληρη την ΕΕ είχαν αυξήσει τις γνώσεις τους για τα δικαιώματά τους, δηλώνοντας ότι «το 69% του πληθυσμού άνω των 16 ετών στην ΕΕ έχει ακούσει για τον GDPR και το 71% των ατόμων άκουσε για την εθνική τους αρχή προστασίας δεδομένων». Η Επιτροπή διαπίστωσε επίσης ότι η ιδιωτική ζωή έχει καταστεί ανταγωνιστική ποιότητα για εταιρείες τις οποίες οι καταναλωτές λαμβάνουν υπόψη κατά τη διαδικασία λήψης αποφάσεων.

2.10.1 Επιβολή και ασυνέπεια

Το Facebook και οι θυγατρικές WhatsApp και Instagram, καθώς και η Google LLC (στόχευση Android), μήνυσαν αμέσως το μη κερδοσκοπικό NOYB του Max Schrems λίγες ώρες μετά τα μεσάνυχτα στις 25 Μαΐου 2018, για τη χρήση της «αναγκαστικής συγκατάθεσης». Ο Schrems ισχυρίζεται ότι αμφότερες οι εταιρείες παραβίασαν το άρθρο 7 παράγραφος 4, επειδή δεν παρουσίασαν τη δυνατότητα συγκατάθεσης για επεξεργασία δεδομένων σε εξατομικευμένη βάση απαιτώντας από τους χρήστες να συναινέσουν σε όλες τις δραστηριότητες επεξεργασίας δεδομένων (συμπεριλαμβανομένων εκείνων που δεν είναι απολύτως απαραίτητες) ή αλλιώς θα απαγορευόταν να χρησιμοποιούν Υπηρεσίες. Στις 21 Ιανουαρίου 2019, η Google επέβαλε πρόστιμο 50 εκατομμυρίων ευρώ από το γαλλικό DPA επειδή δεν παρουσίασε επαρκή έλεγχο, συγκατάθεση και διαφάνεια στη χρήση προσωπικών δεδομένων για συμπεριφορική διαφήμιση. Τον Νοέμβριο του 2018, μετά από μια δημοσιογραφική έρευνα για το Liviu Dragnea, το ρουμανικό DPA (ANSPDCP) χρησιμοποίησε ένα αίτημα GDPR για να ζητήσει πληροφορίες σχετικά με τις πηγές του έργου RISE.

Τον Ιούλιο του 2019, το Γραφείο του Επιτρόπου Πληροφοριών της Βρετανίας εξέδωσε την πρόθεση να επιβάλει πρόστιμο στη British Airways ύψους 183 εκατομμυρίων λιρών (1,5% του κύκλου εργασιών) για κακές ρυθμίσεις ασφαλείας που επέτρεψαν μια επίθεση ισορροπίας Ιστού του 2018 που επηρέασε περίπου 380.000 συναλλαγές. Στην British Airways επιβλήθηκε τελικά ως πρόστιμο το μειωμένο ποσό των 20 εκατομμυρίων λιρών, με τον ICO να σημειώνει

ότι «είχαν εξετάσει και τις δύο εκπροσώπους από την ΒΑ και τον οικονομικό αντίκτυπο της COVID-19 πριν από την οριστική ποινή».

Τον Δεκέμβριο του 2019, η Politico ανέφερε ότι η Ιρλανδία και το Λουξεμβούργο - δύο μικρότερες χώρες της ΕΕ που είχαν τη φήμη ως φορολογικοί παράδεισοι και (ειδικά στην περίπτωση της Ιρλανδίας) ως βάση για τις ευρωπαϊκές θυγατρικές των μεγάλων τεχνολογιών των ΗΠΑ - αντιμετώπιζαν σημαντικές καθυστερήσεις τις έρευνές τους για μεγάλες ξένες εταιρείες στο πλαίσιο του GDPR, με την Ιρλανδία να αναφέρει την πολυπλοκότητα του κανονισμού ως παράγοντα. Οι επικριτές που πήραν συνέντευξη από την Politico ισχυρίστηκαν επίσης ότι η επιβολή παρεμποδίστηκε επίσης από διάφορες ερμηνείες μεταξύ των κρατών μελών, την ιεράρχηση της καθοδήγησης για την επιβολή ορισμένων αρχών και την έλλειψη συνεργασίας μεταξύ των κρατών μελών.

Ενώ οι εταιρείες υπόκεινται πλέον σε νομικές υποχρεώσεις, εξακολουθούν να υπάρχουν διάφορες ασυνέπειες στην πρακτική και τεχνική εφαρμογή του GDPR. Για παράδειγμα, σύμφωνα με το δικαίωμα πρόσβασης του GDPR, οι εταιρείες υποχρεούνται να παρέχουν στα υποκείμενα των δεδομένων τα δεδομένα που συλλέγουν για αυτά. Ωστόσο, σε μια μελέτη σχετικά με τις κάρτες επιβράβευσης στη Γερμανία, οι εταιρείες δεν παρείχαν στα υποκείμενα των δεδομένων τις ακριβείς πληροφορίες των αγορασθέντων άρθρων. Κάποιος μπορεί να υποστηρίξει ότι τέτοιες εταιρείες δεν συλλέγουν τις πληροφορίες των αντικειμένων που αγοράστηκαν, τα οποία δεν συμμορφώνονται με τα επιχειρηματικά τους μοντέλα. Επομένως, τα υποκείμενα των δεδομένων τείνουν να το βλέπουν ως παραβίαση του GDPR. Ως αποτέλεσμα, μελέτες έχουν προτείνει έναν καλύτερο έλεγχο μέσω των αρχών.

Σύμφωνα με το GDPR, η συναίνεση των τελικών χρηστών πρέπει να είναι έγκυρη, ελεύθερη, συγκεκριμένη, ενημερωμένη και ενεργή. Ωστόσο, η έλλειψη εκτέλεσης όσον αφορά τη λήψη νόμιμων συγκατάθεσης υπήρξε πρόκληση. Για παράδειγμα, μια μελέτη του 2020, έδειξε ότι η Big Tech, δηλαδή η Google, η Amazon, το Facebook, η Apple και η Microsoft (GAFAM), χρησιμοποιούν μοτίβα στη συγκατάθεσή τους για τη λήψη μηχανισμών, γεγονός που δημιουργεί αμφιβολίες σχετικά με τη νομιμότητα της αποκτηθείσας συγκατάθεσης.

Τον Μάρτιο του 2021, τα κράτη μέλη της ΕΕ υπό την ηγεσία της Γαλλίας ανέφεραν ότι προσπαθούν να τροποποιήσουν τον αντίκτυπο του κανονισμού περί προστασίας της ιδιωτικής ζωής στην Ευρώπη εξαιρώντας τις εθνικές υπηρεσίες ασφαλείας.

2.10.2 Επίδραση στους διεθνείς νόμους

Η μαζική υιοθέτηση αυτών των νέων προτύπων απορρήτου από διεθνείς εταιρείες έχει αναφερθεί ως παράδειγμα του «φαινομένου των Βρυξελλών», ένα φαινόμενο όπου οι ευρωπαϊκοί νόμοι και κανονισμοί χρησιμοποιούνται ως παγκόσμια γραμμή βάσης λόγω της βαρύτητας τους.

Η πολιτεία της Καλιφόρνια των ΗΠΑ ψήφισε τον νόμο περί απορρήτου των καταναλωτών στην Καλιφόρνια στις 28 Ιουνίου 2018, με ισχύ από την 1η Ιανουαρίου 2020 και παραχώρησε δικαιώματα στη διαφάνεια και τον έλεγχο της συλλογής προσωπικών πληροφοριών από εταιρείες με παρόμοιο τρόπο με τον GDPR. Οι επικριτές έχουν υποστηρίξει ότι τέτοιοι νόμοι πρέπει να εφαρμοστούν σε ομοσπονδιακό επίπεδο για να είναι αποτελεσματικοί, καθώς μια συλλογή νόμων σε επίπεδο κράτους θα έχει διαφορετικά πρότυπα που θα περιπλέκουν τη συμμόρφωση.

Η Δημοκρατία της Τουρκίας, μια χώρα που κατέχει το υποψήφιο καθεστώς για ένταξη στην Ευρωπαϊκή Ένωση, ενέκρινε τον νόμο για την προστασία των προσωπικών δεδομένων στις 24 Μαρτίου 2016 σύμφωνα με το κεκτημένο της ΕΕ.

3 ΚΕΦΑΛΑΙΟ: «ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ»

3.1 ΜΕΛΛΟΝΤΙΚΑ ΖΗΤΗΜΑΤΑ

Οι Hedley και Jacobs (2017) μελέτησαν τα μελλοντικά ζητήματα ασφαλείας, όπως η παραβίαση του Equifax, το GDPR και η ασφάλεια ανοικτού κώδικα.

Παρόλο που ο Κανονισμός Γενικής Προστασίας Δεδομένων (GDPR) χαιρετίζεται ως ένα είδος επανάστασης, αυτό που πραγματικά αντιπροσωπεύει είναι ο νόμος που καλύπτει την πραγματικότητα. Το GDPR συνοδεύεται από την οδηγία για την ασφάλεια δικτύων και πληροφοριών (NISD). Τόσο το GDPR όσο και το NISD αρχίζουν να ισχύουν από τον Μάιο του 2018.

Ο Daniel Hedley από τον Irwin MitchellL LP και ο Matthew Jacobs από το Black Duck Software περιγράφουν τις συνέπειες της μη αντιμετώπισης του GDPR και των διαδικασιών και πολιτικών που χρειάζονται για να τεθεί σε ισχύ (Hedley&Jacobs, 2017)

3.2 ΚΑΝΟΝΙΣΤΙΚΕΣ ΠΡΟΚΛΗΣΕΙΣ ΤΗΣ ΑΝΑΓΝΩΡΙΣΗΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Η Wachter (2018) σε άρθρο της κατέγραψε τις κανονιστικές προκλήσεις της αναγνώρισης στο Διαδίκτυο των πραγμάτων για την προστασία της ιδιωτικής ζωής, την δημιουργία προφίλ, τις διακρίσεις και τέλος το GDPR.

Στο Διαδίκτυο των πραγμάτων (IoT/Internet of things), οι τεχνολογίες αναγνώρισης και ελέγχου πρόσβασης παρέχουν την απαραίτητη υποδομή για τη σύνδεση δεδομένων μεταξύ των συσκευών ενός χρήστη με μοναδικές ταυτότητες και για την παροχή συνεχών και αδιάλειπτων υπηρεσιών. Ταυτόχρονα, οι μέθοδοι δημιουργίας προφίλ που βασίζονται σε συνδεδεμένα αρχεία μπορούν να αποκαλύψουν απροσδόκητες λεπτομέρειες σχετικά με την ταυτότητα και την ιδιωτική ζωή των χρηστών, οι οποίες ενδέχεται να έρχονται σε σύγκρουση με τα δικαιώματα ιδιωτικής ζωής και να οδηγήσουν σε οικονομικές, κοινωνικές και άλλες

μορφές διακριτικής μεταχείρισης. Πρέπει να επιτευχθεί ισορροπία μεταξύ της αναγνώρισης και του ελέγχου της πρόσβασης που απαιτείται για να λειτουργεί το IoT και τα δικαιώματα των χρηστών στην προστασία της ιδιωτικής ζωής και της ταυτότητας. Η επίτευξη αυτής της ισορροπίας δεν είναι εύκολη υπόθεση εξαιτίας των αδυναμιών στις τεχνικές της ασφάλειας του κυβερνοχώρου και των ανωνυμοποιήσεων. Ο γενικός κανονισμός για την προστασία των δεδομένων της ΕΕ (GDPR), που τέθηκε σε ισχύ τον Μάιο του 2018, μπορεί να παράσχει ουσιαστική καθοδήγηση για την επίτευξη δίκαιης ισορροπίας μεταξύ των συμφερόντων των πάροχων και των χρηστών του Διαδικτύου. Μέσω της ανασκόπησης της ακαδημαϊκής και πολιτικής βιβλιογραφίας, το έγγραφο αυτό χαρτογραφεί την εγγενή ένταση μεταξύ της ιδιωτικής ζωής και της αναγνωσιμότητας στο Διαδίκτυο. Επικεντρώνεται σε τέσσερις προκλήσεις:

1. Τον προσδιορισμό προφίλ, συμπεράσματα και διακρίσεις
2. Τον έλεγχο και την ευαίσθητη κατανόηση της ταυτότητας
3. Τη συναίνεση και αβεβαιότητα
4. Την ειλικρίνεια, εμπιστοσύνη και διαφάνεια

Το έγγραφο θα εξετάσει έπειτα τον βαθμό στον οποίο πολλά πρότυπα που ορίζονται στο GDPR θα παρέχουν ουσιαστική προστασία για την προστασία της ιδιωτικής ζωής και τον έλεγχο της ταυτότητας των χρηστών του IoT. Το έγγραφο καταλήγει στο συμπέρασμα ότι γίνεται προσπάθεια να ελαχιστοποιηθεί ο αντίκτυπος της ιδιωτικής ζωής στις συγκρούσεις μεταξύ αρχών προστασίας δεδομένων και ταυτοποίησης στο Διαδίκτυο (Wachter, 2018).

3.3 ΠΡΟΕΤΟΙΜΑΣΙΑ ΜΕ ΤΟ GDPR

Από τότε που ψηφίστηκε ο νέος ευρωπαϊκός κανονισμός για την προστασία των δεδομένων προσωπικού χαρακτήρα (GDPR) για την προστασία των προσωπικών δεδομένων, οι επιχειρήσεις εργάζονται για τη μετάβαση που έλαβε χώρα τον Μάιο του 2018. Με ένα χρόνο μόνο για να συμμορφωθούν, εξετάζουν θέματα όπως την ενίσχυση της ασφάλειας του κυβερνοχώρου, την ευθύνη των φορέων συλλογής δεδομένων και τις νέες υποχρεωτικές διαδικασίες.

Με αφορμή τον γενικό κανονισμό για την προστασία των δεδομένων της ΕΕ (GDPR), πολλές επιχειρήσεις εργάζονται για τη μετάβαση αυτή.

Με ένα μόνο χρόνο συμμόρφωσης, εξετάζουν θέματα όπως η ενισχυμένη ασφάλεια στον κυβερνοχώρο, η ευθύνη των φορέων συλλογής δεδομένων και οι νέες υποχρεωτικές διαδικασίες. Το GDPR θα υποχρεώσει τις επιχειρήσεις να καλύψουν την απειλή της ασφάλειας στον κυβερνοχώρο σε σχέση με τη στρατηγική, τη νομοθεσία και τις επιχειρήσεις. Οι επιχειρήσεις πρέπει να αποκαταστήσουν τη λειτουργία τους και αυτό έχει πολλές πτυχές και προκλήσεις, όπως εξηγεί ο Jocelyn Krystlik από το Stormshield (Krystlik, 2017)

3.4 ICO ΚΑΙ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

Ο Butterworth (2018) μελέτησε την σχέση της ICO (Information Commissioner's Office / Γραφείο Επιτρόπου Πληροφοριών) και της τεχνητής νοημοσύνης: Ο ρόλος της δικαιοσύνης στο πλαίσιο της GDPR.

Το έτος 2017 πραγματοποιήθηκαν πολλές νομοθετικές πρωτοβουλίες και προτάσεις της ΕΕ και του Ηνωμένου Βασιλείου για να εξεταστεί και να αντιμετωπιστεί ο αντίκτυπος της τεχνητής νοημοσύνης στην κοινωνία, καλύπτοντας ζητήματα ευθύνης, νομικής προσωπικότητας και άλλα δεοντολογικά και νομικά ζητήματα, μεταξύ άλλων και στο πλαίσιο της επεξεργασίας δεδομένων. Τον Μάρτιο του 2017, το γραφείο του Επιτρόπου Πληροφόρησης (UK) ενημέρωσε τις μεγάλες κατευθυντήριες γραμμές για την αντιμετώπιση της ανάπτυξης της τεχνητής νοημοσύνης και της μηχανικής μάθησης και την παροχή (GDPR).

Η μελέτη αυτή τοποθετεί την καθοδήγηση του ICO στο πλαίσιο ευρύτερων νομικών και δεοντολογικών παραμέτρων και παρέχει μια κριτική για τη θέση που υιοθέτησε ο ICO. Από την ανάλυση του ICO, η βασική πρόκληση για τα προσωπικά δεδομένα επεξεργασίας τεχνητής νοημοσύνης είναι να διαπιστωθεί ότι η επεξεργασία αυτή είναι δίκαιη. Αυτή η μετατόπιση αντικατοπτρίζει το ενδεχόμενο η τεχνητή νοημοσύνη να έχει αρνητικές κοινωνικές συνέπειες που δεν αντιμετωπίζονται διαφορετικά από το GDPR. Το ζήτημα της «δίκαιης μεταχείρισης» είναι σημαντικό, για να αντιμετωπιστεί η έλλειψη ισορροπίας μεταξύ των μεγάλων ο οργανισμών δεδομένων και των μεμονωμένων προσώπων στα οποία αναφέρονται τα δεδομένα, με ορισμένες δεοντολογικές και κοινωνικές επιπτώσεις που πρέπει να αξιολογηθούν (Butterworth, 2018).

3.5 ΤΟ GDPR ΓΙΑ ΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

Ο Tankard (2016) μελέτησε την σημασία του GDPR για τις επιχειρήσεις. Ο πολυαναμενόμενος κανονισμός γενικής προστασίας δεδομένων (GDPR) της ΕΕ εγκρίθηκε προσωρινά τον Δεκέμβριο του 2015, με τη δημοσίευση της τελικής έκδοσης του κανονισμού να αναμένεται γύρω στον Ιούλιο του 2016. Στη συνέχεια, υπάρχει διετής περίοδος αναμονής έως ότου κάθε οργανισμός που ασκεί επιχειρηματική δραστηριότητα στην ΕΕ ή με την ΕΕ να συμμορφωθεί με τον κανονισμό. Δεδομένου ότι πρόκειται για έναν κανονισμό, όχι για μια οδηγία, η συμμόρφωση είναι υποχρεωτική, χωρίς να χρειάζεται κάθε κράτος μέλος να το επικυρώσει στη δική του νομοθεσία.

Το GDPR επεκτείνει το πεδίο προστασίας των δεδομένων έτσι ώστε να εφαρμόζεται σε οποιονδήποτε ή σε οποιονδήποτέ ε οργανισμό που συλλέγει και επεξεργάζεται πληροφορίες σχετικές με πολίτες της ΕΕ, ανεξάρτητα από τον τόπο στον οποίο βασίζονται ή όπου αποθηκεύονται τα δεδομένα. Ο Colin Tankard των Ψηφιακών Διαδρομών εξετάζει το αποτέλεσμα που μπορεί να έχει ο νέος κανονισμός στους οργανισμούς (Tankard, 2016).

3.6 ΔΙΚΑΙΩΜΑ ΜΕΤΑΦΟΡΑΣ ΔΕΔΟΜΕΝΩΝ ΣΤΟ GDPR

Οι De Hert, Papakonstantinou, Malgieri, Beslay και Sanchez (2018) κατέγραψαν το δικαίωμα μεταφοράς δεδομένων στο GDPR: προς τη διαλειτουργικότητα των ψηφιακών υπηρεσιών με γνώμονα το χρήστη.

Το δικαίωμα στη φορητότητα δεδομένων είναι μία από τις σημαντικότερες καινοτομίες στο πλαίσιο του γενικού κανονισμού της ΕΕ για την προστασία των δεδομένων, τόσο όσον αφορά την εξασφάλιση των δικαιωμάτων ελέγχου στα πρόσωπα στα οποία αναφέρονται τα δεδομένα όσο και όσον αφορά τη διασταύρωση μεταξύ προστασίας δεδομένων και άλλων τομέων δικαίου, πνευματικής ιδιοκτησίας, προστασίας των καταναλωτών κλπ.). Αποτελεί, συνεπώς, πολύτιμη περίπτωση ανάπτυξης και διάδοσης αποτελεσματικών τεχνολογιών για την ενίσχυση της προστασίας της ιδιωτικής ζωής και ενός πρώτου εργαλείου που επιτρέπει στα άτομα να απολαμβάνουν τον άυλο πλούτο των προσωπικών δεδομένων τους στην οικονομία των δεδομένων. Πράγματι, η ελεύθερη δυνατότητα μεταφοράς δεδομένων προσωπικού χαρακτήρα από έναν ελεγκτή σε άλλο μπορεί να αποτελέσει ισχυρό εργαλείο για τα υποκείμενα των δεδομένων προκειμένου να προωθηθεί ο ανταγωνισμός των ψηφιακών

υπηρεσιών και της δια λειτουργικότητας των πλατφορμών και να ενισχυθεί η ελεγκτική λειτουργία των ατόμων με τα δικά τους δεδομένα. Ωστόσο, η υιοθετηθείσα διατύπωση του δικαιώματος στη φορητότητα δεδομένων στο GDPR θα μπορούσε να επωφεληθεί από περαιτέρω διευκρινίσεις: πολλές ερμηνείες είναι δυνατές, ιδίως όσον αφορά το αντικείμενο του δικαιώματος και τις αλληλεξαρτήσεις του με άλλα δικαιώματα, γεγονός που ενδέχεται να οδηγήσει σε πρόσθετες προκλήσεις στο πλαίσιο της τεχνικής του εφαρμογής.

Στόχος του άρθρου αυτού είναι να προτείνει μια πρώτη συστηματική ερμηνεία αυτού του νέου δικαιώματος, προτείνοντας μια ρεαλιστική και εκτεταμένη προσέγγιση, αξιοποιώντας κατά το δυνατόν όσο το δυνατόν περισσότερο την αλληλεξάρτηση που μπορεί να έχει αυτή η νέα νομική διάταξη όσον αφορά την ενιαία ψηφιακή αγορά και τα θεμελιώδη δικαιώματα των ψηφιακών χρηστών (DeHert, Papakonstantinou, Malgieri, Beslay, &Sanchez, 2018).

3.7 ΚΑΤΑΝΟΗΣΗ ΤΗΣ ΕΝΝΟΙΑΣ ΤΟΥ ΚΙΝΔΥΝΟΥ ΣΤΟΝ ΚΑΝΟΝΙΣΜΟ ΓΕΝΙΚΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Ο Gellert (2018) ερεύνησε την έννοια του κινδύνου στον κανονισμό γενικής προστασίας δεδομένων.

Σκοπός αυτής της συνεισφοράς είναι να κατανοηθεί η έννοια του κινδύνου, όπως αυτή κατοχυρώνεται στον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR), με ιδιαίτερη αναφορά στην Art. 35 που προβλέπει την υποχρέωση διενέργειας αξιολογήσεων επιπτώσεων για την προστασία των δεδομένων (DPIA), το πρώτο εργαλείο διαχείρισης του κινδύνου που πρέπει να κατοχυρωθεί στη νομοθεσία της ΕΕ για την προστασία των δεδομένων και το οποίο περιέχει επομένως ορισμένα βασικά στοιχεία για την κατανόηση της έννοιας. Ένα από τα βασικά συμπεράσματα είναι ότι ο κίνδυνος GDPR αφορά τον «κίνδυνο συμμόρφωσης» (δηλαδή όσο χαμηλότερη είναι η συμμόρφωση, τόσο μεγαλύτερες είναι οι συνέπειες για τα δικαιώματα των υποκειμένων των δεδομένων). Η στάση αυτή έρχεται σε άμεση αντίθεση με ορισμένες θέσεις που υποστηρίζουν τον αυστηρό διαχωρισμό μεταξύ συμμόρφωσης και ζητημάτων κινδύνου (Gellert, 2018).

Αυτή η συμβολή αντιλαμβάνεται τα θέματα συμμόρφωσης και κινδύνου για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, καθώς είναι βαθιά διασυνδεδεμένα. Το συμπέρασμα θα χρησιμοποιήσει αυτές τις συζητήσεις ως βάση για την

αντιμετώπιση της μακροχρόνιας συζήτησης σχετικά με τις διαφορές μεταξύ των αξιολογήσεων των επιπτώσεων στην ιδιωτική ζωή (PIAs) και των DPIA. Θα προειδοποιήσουν επίσης για το γεγονός ότι τελικά ο τρόπος με τον οποίο ο κίνδυνος ορίζεται στο GDPR είναι κάπως άσχετος: το σημαντικότερο είναι η χρησιμοποιούμενη μεθοδολογία και ο τύπος κινδύνου στην εργασία. Όσο χαμηλότερη είναι η συμμόρφωση, τόσο μεγαλύτερες είναι οι συνέπειες για τα δικαιώματα των υποκειμένων των δεδομένων (Gellert, 2018).

3.8 ΒΙΟΜΗΧΑΝΙΚΗ ΑΣΦΑΛΕΙΑ ΚΑΙ FUD

Ο Curry (2018) σε μελέτη του συμπέρανε γιατί η βιομηχανική ασφάλεια πρέπει να σταματήσει να βασίζεται στο FUD.

Η αφήγηση γύρω από την ασφάλεια των πληροφοριών ήταν πάντα πολύ πιο αρνητική από τον υπόλοιπο τομέα της τεχνολογίας. Οι συζητήσεις γύρω από τον κυβερνοχώρο τείνουν να επικεντρώνονται στις απειλές και τις συνέπειες, πάρα στην αισιόδοξη έμφαση στην πρόοδο και τις ευκαιρίες που υπάρχουν σε τομείς όπως το σύννεφο ή η κινητή τεχνολογία.

Η βιομηχανία έχει καθήκον να χρησιμοποιήσει τις γνώσεις και την εμπειρία της για να καθοδηγήσει τους οργανισμούς να κάνουν επιλογές που θα βελτιώσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους όταν συμβαίνει κάποιο συμβάν ασφάλειας (Curry, 2018).

3.9 Η ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΩΣ ΣΤΡΑΤΗΓΙΚΗ ΕΠΙΧΕΙΡΗΜΑΤΙΚΗ ΠΡΟΤΕΡΑΙΟΤΗΤΑ

Σύμφωνα με τον James (2018) η ασφάλεια στον κυβερνοχώρο υφίσταται ως στρατηγική επιχειρηματική προτεραιότητα.

Πριν από πέντε χρόνια, η ασφάλεια στον κυβερνοχώρο δεν ήταν κάτι που θα συνδέονταν απαραίτητα με την καθημερινή επιχειρηματική πρακτική. Οι περισσότερες εταιρείες δεν επιθυμούσαν να επανεξετάσουν τις στρατηγικές τους για την καταπολέμηση αυτής της δυνητικής απειλής και μια στάση «δεν θα συμβεί σε εμένα» ήταν συνηθισμένη.

Πλέον η στρατηγική ασφάλειας ενός οργανισμού πρέπει να ευθυγραμμίζεται με την επιχειρησιακή στρατηγική και να είναι αναπόσπαστη στη διαδικασία λήψης αποφάσεων της ανώτερης ηγεσίας.

Για να μπορούν οι οργανώσεις να λειτουργούν με ασφάλεια στο σύγχρονο τοπίο απειλής, πρέπει να βεβαιωθούν ότι αξιολογούν με συνέπεια την αποτελεσματικότητα των αμυντικών τους μέσων ώστε να είναι όσο το δυνατόν πιο ασφαλείς. Ταυτόχρονα, πρέπει να διασφαλίσουν ότι χρησιμοποιούν τις πιο σύγχρονες λύσεις και έχουν τη σωστή τεχνογνωσία στο χέρι (James, 2018).

3.10 GDPR: Η ΣΥΝΔΕΣΗ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΚΑΙ ΤΟΥ ΝΟΜΟΥ ΠΕΡΙ ΕΜΠΟΡΙΚΩΝ ΣΗΜΑΤΩΝ

Οι νόμοι περί απορρήτου επηρεάζουν την επιβολή εμπορικών σημάτων πριν από μια συνεδρία που εξετάζει τις διαφορετικές προσεγγίσεις σε όλο τον κόσμο (Burton, 2019).

Από τότε που ο Γενικός Κανονισμός Προστασίας Δεδομένων της ΕΕ (GDPR) τέθηκε σε ισχύ, έχει γίνει όλο και πιο δύσκολο για τους ιδιοκτήτες πνευματικής ιδιοκτησίας (intellectual property / IP) να διερευνήσουν τις παραβάσεις στο Διαδίκτυο.

Οι νόμοι περί απορρήτου έχουν περιορίσει την πρόσβαση στους πόρους στους οποίους βασίστηκαν ιστορικά οι ιδιοκτήτες IP για να ελέγχουν τις διαδικτυακές παραβάσεις - από καταλόγους ονομάτων τομέα όπως WHOIS, έως αρχεία που διατηρούνται από παρόχους υπηρεσιών Διαδικτύου και πλατφόρμες κοινωνικών μέσων.

«*Ως αποτέλεσμα, οι ιδιοκτήτες IP θα πρέπει να επιστρέψουν σε άλλα μέτρα έρευνας και επιβολής, όπως ανάλυση περιεχομένου ιστότοπου και ουσιαστικών αποδεικτικών στοιχείων, διαβούλευση με σχετικούς ιστότοπους και υποβολή αιτήσεων αποκάλυψης σε διαδικτυακούς διαμεσολαβητές που ελέγχουν τα στοιχεία αναγνώρισης και επικοινωνίας του (δυνητικού) παραβάτες*».

Όμως οι νόμοι περί απορρήτου δεν επηρεάζουν μόνο την επιβολή εμπορικών σημάτων στο διαδίκτυο, σημειώνεται ότι οι μάρκες (Brand name) σε όλο τον κόσμο αισθάνονται επίσης τον εκτεταμένο και άνευ προηγουμένου αντίκτυπο των νόμων περί απορρήτου σε σχέση με την καλή θέληση, τις προσπάθειες μάρκετινγκ και τις τελωνειακές διαδικασίες.

Το GDPR είναι μόνο η αρχή και στο μέλλον, η παγκόσμια προστασία δεδομένων θα χρησιμοποιηθεί για την ενίσχυση της εμπιστοσύνης και της εμπιστοσύνης της μάρκας. Η «ισορροπία» πρέπει να είναι η λέξη κλειδί. Λέει ότι η περαιτέρω ανάπτυξη και εφαρμογή των εθνικών και παγκόσμιων νόμων για την προστασία της ιδιωτικής ζωής πρέπει να εξισορροπηθεί όχι μόνο με τα δικαιώματα πνευματικής ιδιοκτησίας, αλλά με όλα τα θεμελιώδη δικαιώματα και συμφέροντα όπως το δικαίωμα στην ελευθερία της έκφρασης, την πρόσβαση σε πληροφορίες και την προστασία των καταναλωτών (Burton, 2019).

4 ΚΕΦΑΛΑΙΟ: «ΣΗΜΕΙΑ ΚΛΕΙΔΙΑ ΤΟΥ GDPR ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ»

4.1 ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ

Η υφιστάμενη Ευρωπαϊκή Οδηγία του 1995 για την Προστασία Δεδομένων αντικαθίσταται από τον νέο κανονισμό EU General Data Protection Regulation (GDPR), τον οποίο ενέκρινε το Ευρωπαϊκό Κοινοβούλιο στις αρχές του 2016, και έχει τεθεί σε ισχύ από τον Μάιο του 2018.

Σημαντική πτυχή του νέου κανονισμού αποτελεί ο τρόπος με τον οποίο ορίζονται τα προσωπικά δεδομένα. Με τον νέο Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) ορίζονται τα προσωπικά δεδομένα ως τα δεδομένα που επιτρέπουν την άμεση ή έμμεση εξακρίβωση της ταυτότητας του ατόμου. Δηλαδή η νέα νομοθεσία καλύπτει ακόμα και τις διευθύνσεις διαδικτυακού πρωτοκόλλου (IP), δεδομένα τοποθεσίας ή άλλους παράγοντες μέσω των οποίων μπορεί να εξακριβωθεί η ταυτότητα ενός ατόμου.

Στο πλαίσιο του κανονισμού ο ορισμός «προσωπικά δεδομένα», φανερώνει το ύφος της νέας νομοθεσίας, κατά την οποία τα προσωπικά δεδομένα θεωρούνται ως ένα πολύτιμο περιουσιακό στοιχείο και οι κανόνες που τα αφορούν πρόκειται να γίνουν αυστηρότεροι. Μάλιστα αυτό συμβαδίζει με τεχνολογικές τάσεις, όπως το cloud computing, τα social media, τα κινητά και οι ηλεκτρονικές συσκευές με ενσωματωμένους αισθητήρες συλλογής δεδομένων (Internet of Things), όπου η συλλογή δεδομένων και η επαρκής ανάλυσή τους γίνονται στρατηγικοί φορείς διαφοροποίησης για τους οργανισμούς. Συνεπώς, ο Ευρωπαίος νομοθέτης αντιλαμβάνεται πλέον την πραγματικότητα (Σπυριδάκη, 2018).

4.2 ΒΑΣΙΚΗ ΔΙΑΦΟΡΟΠΟΙΗΣΗ ΤΟΥ GDPR

Ο νέος Γενικός Κανονισμός (ΕΕ) 2016/679 δεν παρουσιάζει ουσιώδεις διαφορές από τις γενικές αρχές του υφιστάμενου πλαισίου προστασίας των προσωπικών δεδομένων, ενώ επιχειρεί να δημιουργήσει ένα αυστηρότερο θεσμικό πλαίσιο επεξεργασίας των προσωπικών δεδομένων και κατ' επέκταση προστασίας τους (Κανελλόπουλος, 2018).

Το χαρακτηριστικό του είναι η ριζική αλλαγή του συστήματος ευθύνης για τήρηση της νομοθεσίας με την αρχή της Λογοδοσίας (Accountability Principle),σύμφωνα με την οποία οι εταιρείες που συλλέγουν και επεξεργάζονται προσωπικά δεδομένα πρέπει να διαμορφώσουν τις διαδικασίες και τα τεχνικά και οργανωτικά συστήματά τους ώστε να συμμορφώνονται πλήρως με όσα προβλέπει ο νέος Κανονισμός. Οι εταιρείες έχουν πλέον το βάρος απόδειξης και όχι οι Αρχές Προστασίας Προσωπικών Δεδομένων, καθώς οι εταιρείες οφείλουν να αποδεικνύουν σε οποιαδήποτε περίπτωση ελέγχου τι είναι πλήρως εναρμονισμένες με τις διατάξεις του Κανονισμού.

Επιπλέον, σύμφωνα με τον Κανονισμό πρέπει να υπάρχει ξεκάθαρη συναίνεση του υποκειμένου των δεδομένων για κάθε σκοπό επεξεργασίας. Έτσι, λοιπόν, δημιουργείται η ανάγκη άμεσου εκσυγχρονισμού των μεθόδων και συστημάτων που εφαρμόζονται για την επεξεργασία των προσωπικών δεδομένων προκειμένου να τηρούνται οι αυστηρές προϋποθέσεις συγκατάθεσης και επεξεργασίας.

Τα δεδομένα προσωπικού χαρακτήρα αφορούν κάθε εν ζωή φυσικού προσώπου, δηλαδή πρόκειται για κάθε πληροφορία που αφορά ταυτοποιημένο φυσικό πρόσωπο ή κάθε πληροφορία που μπορεί άμεσα ή έμμεσα να ταυτοποιήσει ένα φυσικό πρόσωπο. Η ταυτοποίηση αυτή μπορεί να γίνει ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης ή σε στοιχεία που αφορούν τη σωματική, ψυχολογική, οικονομική ή κοινωνική κατάσταση του εν λόγω φυσικού προσώπου. Δεν πρόκειται δηλαδή για τα δεδομένα των νομικών προσώπων(εταιρειών κλπ.),ενώ αφορά τα δεδομένα μιας Μονοπρόσωπης εταιρίας ή μιας ατομικής επιχείρησης που νομικά αντιμετωπίζεται ως φυσικό πρόσωπο (Data protection in the EU, 2018).

4.3 ΠΡΟΫΠΟΘΕΣΕΙΣ ΝΟΜΙΜΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η έκαστη πράξη που συντελείται με τη βοήθεια ή όχι αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα μπορεί να περιλαμβάνει τη συλλογή, την οργάνωση, την καταχώριση, τη διάρθρωση, την αποθήκευση, την ανάκτηση, την προσαρμογή ή τη μεταβολή, την αναζήτηση πληροφοριών, τη χρήση, την κοινολόγηση με διαβίβαση, τον περιορισμό, τη

διάδοση ή κάθε άλλη μορφή διάθεσης, τη συσχέτιση ή τον συνδυασμό, τη διαγραφή ή την καταστροφή (Προστασία δεδομένων στην ΕΕ, 2018).

Ως εκ τούτου, η επεξεργασία των προσωπικών δεδομένων αποτελεί μια ευρύτατη έννοια, περιλαμβάνει ακόμη και τη συλλογή προσωπικών δεδομένων.

Εφόσον συντρέχουν τουλάχιστον μία από τις προϋποθέσεις που ακολουθούν, τότε η επεξεργασία είναι νόμιμη (Κανελλόπουλος, 2018):

a). Το υποκείμενο των δεδομένων έχει συναινέσει να επεξεργαστούν τα δεδομένα προσωπικού χαρακτήρα του εάν εξυπηρετούν έναν ή περισσότερους συγκεκριμένους σκοπούς.
b). Η επεξεργασία χρειάζεται για την εκτέλεση σύμβασης της οποίας το υποκείμενο συμμετέχει προκειμένου να ληφθούν μέτρα κατόπιν αιτήσεως του υποκειμένου των δεδομένων πριν συναφθεί η σύμβαση.
c). Η επεξεργασία είναι απαραίτητη για να συμμορφωθεί ο υπεύθυνος επεξεργασίας με έννομη υποχρέωση του.
d). Η επεξεργασία είναι απαραίτητη για να διαφυλαχθεί το ζωτικό συμφέρον του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.
e). Η επεξεργασία είναι απαραίτητη για να εκπληρωθεί το καθήκον που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.
f). 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.

Στην επεξεργασία των προσωπικών δεδομένων τα εμπλεκόμενα μέρη είναι αυτά που φαίνονται στο Σχήμα 4.1 (Κανελλόπουλος, 2018):

Σχήμα 4.1: Εμπλεκόμενα μέρη στην επεξεργασία των προσωπικών δεδομένων

Πηγή: (Κανελλόπουλος, 2018).

4.4 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ

Όταν ο υπεύθυνος ή ο εκτελών την επεξεργασία των δεδομένων προσωπικού χαρακτήρα έχει την εγκατάστασή του στην ΕΕ, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης τότε εφαρμόζεται ο Νέος Κανονισμός.

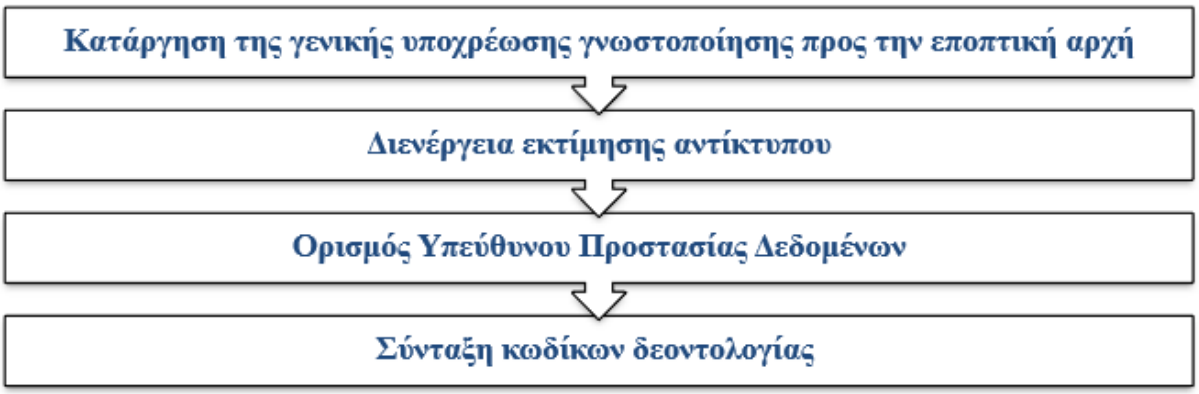
Επίσης βρίσκει εφαρμογή στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση, εφόσον οι δραστηριότητες επεξεργασίας σχετίζονται με (Κανελλόπουλος, 2018):

a). την παροχή αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ένωση, χωρίς να εξαρτάται από το εάν είναι αναγκαία πληρωμή από τα υποκείμενα των δεδομένων,

b). τον έλεγχο της συμπεριφοράς τους, όσο η συμπεριφορά αυτή υπάρχει εντός της Ένωσης.

Επιπλέον, ο Κανονισμός βρίσκει εφαρμογή στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην Ένωση, αλλά σε τόπο όπου εφαρμόζεται το δίκαιο κράτους μέλους δυνάμει του δημόσιου διεθνούς δικαίου.

Στην συνέχεια ακολουθούν οι βασικές καινοτομίες του Κανονισμού (Κανελλόπουλος, 2018) (Σχήμα 4.2):



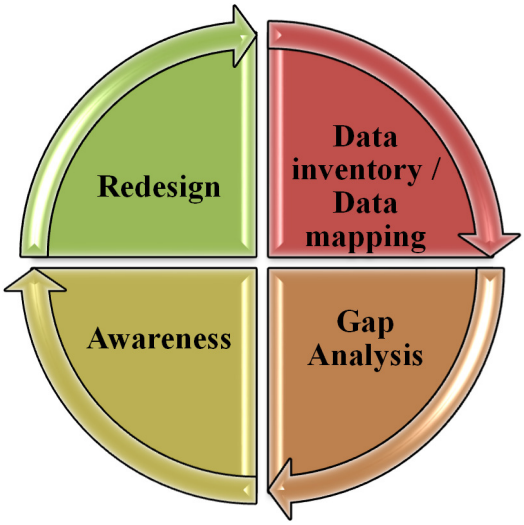
Σχήμα 4.2: Οι βασικές καινοτομίες του Κανονισμού.

Πηγή: (Κανελλόπουλος, 2018).

4.4.1 Κατάργηση της γενικής υποχρέωσης γνωστοποίησης προς την εποπτική αρχή

Ο νέος GDPR αυτή την καταργούμενη υποχρέωση την αντικαθιστά με την δέσμευση για τους υπευθύνους επεξεργασίας να εφαρμόζουν τα αρχεία των δραστηριοτήτων επεξεργασίας όλων των δεδομένων προσωπικού χαρακτήρα, για τις οποίες ευθύνονται, αλλά και με την δέσμευση για εκείνους που επιτελούν την επεξεργασία να εφαρμόζουν τα αρχεία όλων των κατηγοριών δραστηριοτήτων επεξεργασίας, οι οποίες γίνονται για λογαριασμό υπευθύνου επεξεργασίας.

Ήδη, τόσο για τους υπευθύνους, όσο και για τους εκτελούντες επεξεργασία, ένας ικανοποιητικός τρόπος προετοιμασίας είναι (Σχήμα 4.3) (Protection of personal data, 2018):



Σχήμα 4.3: Τρόπος προετοιμασίας κατάργησης γενικής υποχρέωσης γνωστοποίησης προς την εποπτική αρχή.

Πηγή: (Protection of personal data, 2018).

4.4.2 Διενέργεια εκτίμησης αντίκτυπου

Πρόκειται για το καθήκον του υπεύθυνου επεξεργασίας προς εκτέλεση εκτίμησης αντίκτυπου (Data protection impact assessment – DPIA) αναφορικά με την προάσπιση δεδομένων σε καθορισμένες κατηγορίες επεξεργασιών.

Πιο συγκεκριμένα, ο υπεύθυνος επεξεργασίας υποχρεούται να εκτελέσει DPIA πριν από την σημαντική επεξεργασία όποτε μια μορφή επεξεργασίας, κυρίως με τη χρησιμοποίηση νέων τεχνολογιών μαζί με το πεδίο εφαρμογής, τη φύση, το πλαίσιο και τις επιδιώξεις αυτής της επεξεργασίας, πιθανόν να προξενήσει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων (Κανελλόπουλος, 2018).

4.4.3 Ορισμός Υπεύθυνου Προστασίας Δεδομένων

Πρόκειται για το χρέος των υπευθύνων επεξεργασίας και όσων πραγματοποιούν την επεξεργασία, να καθορίσουν έναν Υπεύθυνο Προστασίας Δεδομένων (Data Protection Officer-DPO) στη βάση καθορισμένων ποιοτικών κριτηρίων, περικλείοντας την ενέργεια καθορισμένων τύπων επεξεργασιών. Επίσης, καθορίζονται πότε ορίζεται υποχρεωτικά DPO και πότε δίνεται η δυνατότητα στον υπεύθυνο επεξεργασίας ή σε άλλους φορείς, να καθορίσουνε DPO και πέραν των περιπτώσεων του υποχρεωτικού ορισμού.

Για τις εταιρείες είναι εξαιρετικά σημαντική η ύπαρξη και λειτουργία του DPO διότι πρόκειται για το πρόσωπο που θα οδηγεί τον οργανισμό προς την ολοκλήρωση και εφαρμογή ενός ικανού προγράμματος συμμόρφωσης με τον GDPR, θα διαχειριστεί τυχόν καταγγελίες και παραβάσεις και θα εκπροσωπήσει την εταιρεία στην εποπτική αρχή για κάθε σχετικό ζήτημα (Κανελλόπουλος, 2018).

Ως εκ τούτου ακόμα και όταν δεν είναι υποχρεωτικός ο διορισμός DPO, θα ήταν ιδιαίτερα συμφέρον για κάθε εταιρεία να έχει εθελοντικά ορίσει έναν DPO. Από τον GDPR δεν προβλέπονται συγκεκριμένα κριτήρια ή πιστοποιήσεις για την επιλογή του DPO, όμως θα πρέπει να είναι πρόσωπο έμπειρο στη νομοθεσία των προσωπικών δεδομένων και τη διαχείριση τυχόν σχετικών παραβάσεων.

4.4.4 Σύνταξη κωδικών δεοντολογίας

Είναι πολύ ενθαρρυντική η σύνταξη κωδικών δεοντολογίας από ενώσεις και άλλους φορείς υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία ώστε να προσδιορίσουν την εφαρμογή του GDPR. Επίσης, σημαντική είναι και η θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων, με σκοπό την απόδειξη συμμόρφωσης προς το GDPR.

Ο νέος Γενικός Κανονισμός εξασφαλίζει την σταθεροποίηση, μεταξύ της διαρκούς ροής, συγκέντρωσης και επεξεργασίας προσωπικών δεδομένων αλλά και των υποχρεωτικών δικαιωμάτων προστασίας τους που πρέπει να διατηρούνται αλλά και να «επικαιροποιούνται» (Κανελλόπουλος, 2018).

Οι βασικοί στόχοι του Κανονισμού είναι να διευκολύνεται το υποκείμενο στην προσέγγιση σε διοικητικές και δικαστικές διαδικασίες ώστε να προσβάλλουν μη νόμιμες επεξεργασίες ή για να διεκδικήσουν την επανόρθωση της βλάβης που έχουν υποστεί.

Επίσης, ο κανονισμός ασπάζεται την «αρχή της εγγύτητας» προς το υποκείμενο των δεδομένων, ώστε κάθε πρόσωπο που πιστεύει ότι παραβιάζονται τα δικαιώματά του στην προστασία των δεδομένων του, να μπορεί να καταγγείλει σε οποιαδήποτε εποπτική αρχή (Κανελλόπουλος, 2018).

Επιπροσθέτως διευρύνονται τα δικαιώματα του υποκειμένου. Χαρακτηριστικό παράδειγμα είναι η ρητή νομοθετική κατοχύρωση του δικαιώματος στη λήθη, δηλαδή το δικαίωμα του φυσικού προσώπου να διαγραφούν προσωπικά του δεδομένα. Πρόκειται για ένα

βασικό δικαίωμα του υποκειμένου να διατηρεί τον έλεγχο των προσωπικών πληροφοριών του κυρίως στον ψηφιακό κόσμο.

Επιπλέον, το υποκείμενο των προσωπικών δεδομένων έχει το δικαίωμα να στραφεί δικαστικά εναντίον εκείνου που ευθύνεται για την επεξεργασία και εναντίον εκείνου που εκτελεί την επεξεργασία.

Ακόμα, υπάρχει στον Κανονισμό εξειδικευμένη πρόβλεψη αναφορικά με τη συλλογική υποστήριξη των δικαιωμάτων του υποκειμένου. Πρόκειται για το δικαίωμα του υποκειμένου να αναθέτει σε μη κερδοσκοπικό φορέα, οργάνωση ή ένωση, να υποβάλλει την καταγγελία για λογαριασμό του και να ασκεί τα δικαιώματα ενώπιον του δικαστηρίου.

Συμπερασματικά, ο νέος Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων είναι ένα νέο και απαραίτητο βήμα προόδου, όσον αφορά την ενίσχυση του δικαίου προστασίας των προσωπικών δεδομένων αλλά και την παιδεία μιας νοοτροπίας αυτορρύθμισης των επιχειρήσεων και φορέων για την προστασία της προσωπικότητας του ατόμου (Κανελλόπουλος, 2018).

4.5 ΑΥΣΤΗΡΗ ΕΠΙΒΟΛΗ ΝΟΜΟΥ

Η επιβολή του νόμου με τον νέο κανονισμό, γίνεται αυστηρότερη. Πλέον οι αρχές προστασίας προσωπικών δεδομένων κερδίζουν πιο πολλούς πόρους και συνενώνουν τις δυνάμεις τους σε ένα νέο πανευρωπαϊκό σώμα το οποίο θα παραδίδει δεσμευτικές αποφάσεις. Επιπλέον, τα πρόστιμα θα είναι τόσο μεγάλα ώστε το GDPR να εγείρει αυτομάτως τους οργανισμούς σε όλους τους κλάδους (Σπυριδάκη, 2018).

Για παράδειγμα, στην Ευρώπη τέτοιου επιπέδου πρόστιμα συναντώνται μόνο στο Δίκαιο Ανταγωνισμού. Βέβαια, δεν θα έπρεπε ο φόβος της επιβολής προστίμου να είναι το κύριο κίνητρο των οργανισμών για τήρηση, αν και είναι σίγουρα ένας λόγος για να προσέξουν τώρα περισσότερο.

Πλέον, το ύψος των απειλούμενων διοικητικών προστίμων, όταν διαπιστωθεί παράβαση των διατάξεων του Κανονισμού, εφόσον δεν λαμβάνονται άλλα μέτρα, με τον νέο Κανονισμό εκτοξεύεται.

Κατά συνέπεια, συγκεκριμένες παραβάσεις των υποχρεώσεων των υπευθύνων και εκτελούντων επεξεργασία επισύρουν πρόστιμα έως 10.000.000€ ή σε περίπτωση επιχειρήσεων

έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους(όποιο είναι υψηλότερο).Μάλιστα, και αυτή η απουσία των κατάλληλων οργανωτικών μέτρων για συμμόρφωση με τον ΓΚΠΔ, έχει τη δυνατότητα να επισύρει το εν λόγω πρόστιμο, χωρίς καν να υφίσταται περίπτωση παράβασης.

Για τις παραβάσεις σε βάρος των δικαιωμάτων των υποκειμένων των δεδομένων, των βασικών αρχών για την επεξεργασία, της διαβίβασης δεδομένων προσωπικού χαρακτήρα σε αποδέκτη σε τρίτη χώρα ή σε διεθνή οργανισμό και τη μη συμμόρφωση προς εντολή ή προς προσωρινό ή οριστικό περιορισμό της επεξεργασίας ή προς αναστολή της κυκλοφορίας δεδομένων που επιβάλλει η εποπτική αρχή ή μη παροχή πρόσβασης επιφυλάσσονται τα βαρύτερα πρόστιμα (Κανελλόπουλος, 2018).

4.6 ΑΥΞΗΜΕΝΗ ΥΠΟΧΡΕΩΣΗ ΛΟΓΟΔΟΣΙΑΣ

Το GDPR για την προστασία των προσωπικών δεδομένων καθιστά τους οργανισμούς υπόλογους. Όσον αφορά το εάν, το πώς και το πόσο καλά προστάτευσαν τα προσωπικά δεδομένα θα φέρουν το βάρος της απόδειξης. Πλέον υπάρχει μια αρκετά τυπική διαδικασία για την απόκτηση άδειας πρόσβασης σε προσωπικά δεδομένα, όπως τι είδους δεδομένα επεξεργάζονται, ή εάν μεταφέρονται σε τρίτους. Μελλοντικά, αυτό που θα έχει περισσότερη σημασία θα είναι το πόσο καλά οργανωμένες είναι οι διαδικασίες των επιχειρήσεων και όχι η απόκτηση τυπικής άδειας πρόσβασης. Για το λόγο αυτό, θα είναι απαραίτητο να υπάρχει κάποιος, είτε εσωτερικά είτε εξωτερικά, ο οποίος θα αντιλαμβάνεται την έννοια του απορρήτου των δεδομένων και γνωρίζει πώς να επιφέρει αλλαγές και να εφαρμόζει τη νομοθεσία (Σπυριδάκη, 2018).

4.7 ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Για κάθε οργανισμό το αρχικό βήμα είναι μια άσκηση χαρτογράφησης της κίνησης των δεδομένων όπου θα λάβει μέρος το σύνολο του οργανισμού, καθώς η προστασία της ιδιωτικότητας ήδη απαιτεί από τον σχεδιασμό ότι όλες οι υπηρεσίες θα ερευνήσουν τα δεδομένα τους και τον τρόπο με τον οποίο τα χειρίζονται. Αφού εντοπιστούν τα προσωπικά δεδομένα και πώς ακριβώς χρησιμοποιούνται, θα πρέπει να διασφαλιστούν με τον σωστό τρόπο. Η πλειοψηφία των εταιρειών έχει ήδη υιοθετήσει ένα σύστημα το οποίο μπορεί να προσδιορίζει τα προσωπικά δεδομένα, καθώς πρέπει να έχουν συμμορφωθεί με την κείμενη

νομοθεσία για την προστασία των δεδομένων. Με τη νέα νομοθεσία υποχρεώνονται οι οργανισμοί να υιοθετήσουν πιο λεπτομερείς διαδικασίες, αλλά ευτυχώς υπάρχουν πολλές λύσεις που μπορούν να υποστηρίξουν αυτή τη διαδικασία ελέγχου.

Ήδη από τον σχεδιασμό η προστασία της ιδιωτικότητας προϋποθέτει ότι υπάρχει μεγαλύτερη διαφάνεια σχετικά με τα δεδομένα και τη μεταφορά δεδομένων. Ένα από τα πιο σημαντικά ζητήματα στο πλαίσιο του νέου κανονισμού είναι το δικαίωμα διαγραφής των δεδομένων προσωπικού χαρακτήρα (Right to be Forgotten) (Σπυριδάκη, 2018).

4.8 ΑΤΟΜΙΚΗ ΕΛΕΥΘΕΡΙΑ / ΕΞΟΥΣΙΑ

Με τον νέο κανονισμό για την προστασία προσωπικών δεδομένων δίνεται μεγαλύτερη εξουσία στο άτομο, έχοντας τον πελάτη στο κέντρο της προστασίας των δεδομένων. Δηλαδή, το δικαίωμα στη φορητότητα των δεδομένων προβλέπει ότι όταν οι πελάτες θέλουν να αλλάξουν πάροχο για τα e-mail τους, τότε θα πρέπει να μπορούν να μεταφέρουν το σύνολο των δεδομένων τους στο νέο πάροχο.

Οι καταναλωτές, πλέον, μπορούν να ζητήσουν την διαγραφή των προσωπικών τους στοιχείων, αλλά το GDPR ενισχύει αυτό το δικαίωμα διαγραφής με το λεγόμενο «Right to be Forgotten».

Ωστόσο, η πιο μεγάλη αλλαγή, εκτός της συμμόρφωσης θα είναι η μετάθεση της στάσης του οργανισμού απέναντι στην προστασία της ιδιωτικής ζωής. Το πιο σημαντικό θα είναι να καταφέρουν να κερδίσουν την εμπιστοσύνη των πελατών και να αποκτήσουν ανταγωνιστικό πλεονέκτημα. Τέλος, εκτιμούν τις απλές και διαφανείς διαδικασίες για την προάσπιση των δικαιωμάτων τους (Σπυριδάκη, 2018).

4.9 ΚΑΙΝΟΤΟΜΙΑ

Στην αγορά μαζί με την ανανέωση των κανόνων προστασίας των δεδομένων, εισέρχονται φορείς καινοτομίας. Ένα χαρακτηριστικό παράδειγμα είναι η εταιρία Hoxton Analytics, η οποία έχει σύστημα καταμέτρησης ανθρώπων ένα νέας γενιάς (people counter system) το οποίο βοηθά τα καταστήματα λιανικής να καταλάβουν τους πελάτες τους χωρίς να καταγραφούν τα δεδομένα προσωπικού χαρακτήρα (Σπυριδάκη, 2018).

Στην ψηφιοποίηση (digitalization) του κόσμου υπάρχει μια μετασχηματιστική δύναμη με αποτέλεσμα να προκύπτουν περισσότερες καινοτομίες στον τομέα των δεδομένων και της ιδιωτικότητας. Συνεπώς, εμφανίζονται περισσότεροι κανονισμοί που εισάγονται για να βοηθήσουν τους ανθρώπους να νιώσουν άνετα με τις καινοτομίες οι οποίες αφορούν τα προσωπικά δεδομένα. Τώρα η προστασία των προσωπικών δεδομένων και της ιδιωτικότητας είναι σε μια μεταβατική εποχή.

Η Παπαδοπούλου (2017) αναφέρει ότι κατά την σύγκριση του κλάδου των δεδομένων με έναν πιο παραδοσιακό τομέα, όπως για παράδειγμα οι χρηματοπιστωτικές υπηρεσίες, δημιουργείται η γνώμη ότι στα γενικά στοιχεία του κλάδου των δεδομένων απουσιάζουν δικλείδες ασφαλείας / κανονισμοί, καθώς προβλέπεται για μια νέα αγορά. Έτσι, χρειάζονται αρκετά χρόνια, ώστε ο κλάδος των δεδομένων, να συγκροτήσει μια ρυθμιζόμενη αγορά (Παπαδοπούλου, 2017).

Τέλος, είναι πλέον τεκμηριωμένο ότι η Ευρώπη -δίχως υπερβολές- ανέδειξε την νομοθεσία για την προστασία της ιδιωτικής ζωής, και ακολουθούν και άλλες χώρες στον κόσμο όπως για παράδειγμα, ο Καναδάς ή η Αυστραλία, οι οποίες βρίσκονται σε συγκρίσιμο επίπεδο στο χώρο των κανονιστικών ρυθμίσεων των δεδομένων / GDPR. Σύμφωνα με την Σπυριδάκη (2018), πλέον είναι πολύ πιο εύκολο να μεταφερθούν προσωπικά δεδομένα στα κράτη μέλη της ΕΕ που διαθέτουν επαρκές επίπεδο προστασίας των δεδομένων/GDPR. Άρα στους κόλπους της Ευρωπαϊκής Ένωσης, το GDPR θα επιφέρει μεγαλύτερη διαφάνεια και θα δημιουργήσει πιο εναρμονισμένους κανόνες. Είναι γεγονός ότι η ερμηνεία της καθ' αυτής οδηγίας για την προστασία των δεδομένων / GDPR, ίσως παρουσιάζει διαφορές(στην ερμηνεία) μεταξύ των κρατών μελών της ΕΕ. Το σίγουρο είναι ότι η εναρμόνιση θα έχει θετική επίδραση στις επιχειρήσεις (Σπυριδάκη, 2018).

5 ΚΕΦΑΛΑΙΟ: «ΣΥΖΗΤΗΣΗ ΚΑΙ ΠΡΟΚΛΗΣΕΙΣ ΓΙΑ ΤΟ GDPR»

5.1 ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ

Η πρόταση για το νέο κανονισμό δημιούργησε πολλές συζητήσεις και αντιπαραθέσεις, με χιλιάδες τροπολογίες να προτείνονται. Ωστόσο, όπως δείχνει μια μελέτη που πραγματοποίησε η Dimensional Research και η TrustArc, σύμφωνα με επαγγελματίες της πληροφορικής η συμμόρφωση με το GDPR θα απαιτήσει πρόσθετες επενδύσεις συνολικά, καθώς πάνω από το 80% των ερωτηθέντων θεωρούν ότι οι δαπάνες GDPR θα είναι τουλάχιστον 100.000$. Οι ανησυχίες εκφράστηκαν σε μια έκθεση που ζήτησε η δικηγορική εταιρεία Baker & McKenzie[2] που διαπίστωσε ότι «περίπου το 70% των ερωτηθέντων πιστεύουν ότι οι οργανισμοί θα χρειαστεί να επενδύσουν πρόσθετο προϋπολογισμό / προσπάθεια για να συμμορφωθούν με τη συγκατάθεση, τη χαρτογράφηση δεδομένων και τις απαιτήσεις διασυνοριακής μεταφοράς δεδομένων στο πλαίσιο του GDPR» (Controversial Topics GDPR, 2018).

Επίσης, επισημαίνονται και άλλα θέματα, όπως (Παπαδοπούλου, 2017):

- Η απαίτηση να έχει ένας υπεύθυνος προστασίας δεδομένων (DPO), είναι νέα για πολλές χώρες της ΕΕ και επικρίνεται για τη διοικητική επιβάρυνσή του.
- Το GDPR αναπτύχθηκε με επίκεντρο τα κοινωνικά δίκτυα και τους παρόχους Cloud, αλλά δεν εξέτασε αρκετές απαιτήσεις για το χειρισμό δεδομένων προσωπικού χαρακτήρα.
- Η φορητότητα δεδομένων δεν θεωρείται βασική πτυχή για την προστασία των δεδομένων, αλλά περισσότερο λειτουργική προϋπόθεση για τα κοινωνικά δίκτυα και τους παρόχους Cloud, παρόλο που η φορητότητα των δεδομένων δημιουργεί διαφάνεια για την αξιολόγηση των ανησυχιών περί προστασίας της ιδιωτικής ζωής των ελεγκτών.
- Παρόλο που η ελαχιστοποίηση των δεδομένων αποτελεί απαίτηση, ο κανονισμός δεν παρέχει καθοδήγηση σχετικά με το πώς ή τι συνιστά ένα αποτελεσματικό σύστημα αποχαρακτηρισμού δεδομένων.

[2]Ο Baker McKenzie, που ιδρύθηκε το 1949 ως Baker & McKenzie, είναι μια πολυεθνική εταιρία νομικών. Από τον Αύγουστο του 2017, κατατάσσεται ως η δεύτερη μεγαλύτερη διεθνής δικηγορική εταιρία στον κόσμο.

- Η προστασία έναντι των αυτοματοποιημένων αποφάσεων του άρθρου 22,η οποία προωθείται από το άρθρο 15 της οδηγίας για την προστασία των δεδομένων, υποστηρίζεται ότι παρέχει προστασία έναντι αυξανόμενου αριθμού αλγοριθμικών αποφάσεων σε απευθείας σύνδεση και εκτός σύνδεσης, συμπεριλαμβανομένου ενδεχομένως δικαιώματος επεξήγησης. Το κατά πόσον οι παλαιές διατάξεις παρέχουν ουσιαστική προστασία είναι θέμα συνεχούς συζήτησης.
- Γλωσσικές προκλήσεις και προκλήσεις όσον αφορά τη στελέχωση των εθνικών αρχών προστασίας δεδομένων (DPA), δεδομένου ότι οι πολίτες της ΕΕ δεν διαθέτουν πλέον ενιαία DPA για να επικοινωνήσουν για τις ανησυχίες τους, αλλά πρέπει να ασχοληθούν με την DPA που επέλεξε η εμπλεκόμενη εταιρεία.
- Τα προσωπικά δεδομένα δεν μπορούν να μεταφερθούν σε χώρες εκτός της Ευρωπαϊκής Ένωσης εκτός εάν εγγυηθούν το ίδιο επίπεδο προστασίας δεδομένων.
- Υπάρχει ανησυχία σχετικά με την εφαρμογή του GDPR σε συστήματα blockchain, καθώς το διαφανές και σταθερό ιστορικό συναλλαγών με μπλοκ αλυσίδα αντιβαίνει στην ίδια τη φύση του GDPR.

Βέβαια οι μεγαλύτερες προκλήσεις μπορεί να είναι η εφαρμογή του GDPR, διότι (Summary of Articles Contained in the GDPR, 2018):

- Η εφαρμογή του GDPR θα απαιτήσει εκτεταμένες αλλαγές στις επιχειρηματικές πρακτικές για τις εταιρείες που δεν είχαν εφαρμόσει ένα συγκρίσιμο επίπεδο προστασίας της ιδιωτικής ζωής πριν από την έναρξη ισχύος του κανονισμού, ιδίως οι μη ευρωπαϊκές εταιρείες που χειρίζονται προσωπικά δεδομένα της ΕΕ.
- Υπάρχει ήδη έλλειψη εμπειρογνωμόνων και γνώσεων για την προστασία της ιδιωτικής ζωής και έτσι οι νέες απαιτήσεις ενδέχεται να επιδεινώσουν την κατάσταση. Συνεπώς, η εκπαίδευση στην νομοθεσία περί προστασίας δεδομένων και ιδιωτικού απορρήτου, ιδίως για την τήρηση των νέων κανόνων που προκύπτουν, θα αποτελέσει κρίσιμο παράγοντα για την επιτυχία της GDPR. Η «προστασία της ιδιωτικής ζωής από το σχεδιασμό» και τα συναφή θέματα ήταν γνωστά στους ειδικούς μόνο πριν από την GDPR και συζητήθηκαν μαζικά σε κοινότητες, σε νομικές σχολές και στην έρευνα κρυπτογραφίας. Πρόσφατες προσφορές πανεπιστημίων άρχισαν να διαδίδουν γνώση σχετικά με το σχεδιασμό της ιδιωτικής ζωής από τη νομική, τεχνολογική και διαχειριστική προοπτική, για παράδειγμα την ελεύθερη και ανοικτή on-Line πορεία του πανεπιστημίου Karlstad σε επίπεδο μάστερ.

- Η Ευρωπαϊκή Επιτροπή και οι αρχές προστασίας δεδομένων πρέπει να παρέχουν επαρκείς πόρους και εξουσίες για την επιβολή της εφαρμογής.
- Ένα μοναδικό επίπεδο προστασίας δεδομένων πρέπει να συμφωνηθεί από όλες τις ευρωπαϊκές αρχές προστασίας δεδομένων, δεδομένου ότι μια διαφορετική ερμηνεία του κανονισμού ενδέχεται να οδηγήσει σε διαφορετικά επίπεδα προστασίας της ιδιωτικής ζωής.
- Η διεθνής εμπορική πολιτική της Ευρώπης δεν είναι ακόμη σύμφωνη με το GDPR.

5.2 ΕΠΗΡΕΑΣΜΟΣ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

Οι επιχειρήσεις, σύμφωνα με το GDPR, έχουν την υποχρέωση να διασφαλίσουν ότι όλα τα προσωπικά δεδομένα που συλλέγονται πραγματοποιούνται νόμιμα και αυστηρά. Επίσης, πρέπει να προστατεύουν τα δεδομένα από την εκμετάλλευση, αλλά και να σέβονται τα δικαιώματα των κατόχων των δεδομένων. Τέλος, χρειάζεται η αντιμετώπιση κάποιων πολύ σοβαρών κυρώσεων εφόσον αποτύχει η προστασία των δεδομένων.

Είναι αξιοσημείωτο το γεγονός ότι το GDPR εφαρμόζεται σε επιχειρήσεις και επαγγελματίες οι οποίοι εργάζονται και διαμένουν στην ΕΕ, αλλά και για επιχειρήσεις εκτός της ΕΕ εάν προσφέρουν υπηρεσίες ή αγαθά σε πελάτες στην ΕΕ. Ουσιαστικά το GDPR πρόκειται για μια νομοθεσία που εξαπλώνεται σε όλο τον κόσμο, διότι οι εταιρείες που εδρεύουν εκτός ΕΕ θα εξακολουθούν να συμμορφώνονται.

Η Ευρωπαϊκή Επιτροπή όσον αφορά το πώς θα επηρεάσει το GDPR τις επιχειρήσεις, υποστηρίζει ότι με την ενοποίηση των κανόνων της Ευρώπης όσον αφορά την προστασία των δεδομένων, οι νομοθέτες δημιουργούν μια επιχειρηματική ευκαιρία και στηρίζουν την καινοτομία. Επίσης, με την ύπαρξη μιας αρχής για ολόκληρη την ΕΕ, θα δημιουργηθεί μια πιο απλή και πιο φθηνή διαδικασία για επιχειρήσεις που κινούνται στην περιοχή. Αυτό θα συμβεί με προϊόντα και τεχνολογίες που θα προσφέρουν ουσιαστικά «προστασία δεδομένων από τον σχεδιασμό και από προεπιλογή» (Προστασία δεδομένων στην ΕΕ, 2018).

5.2.1 Email marketing

Στον τομέα του email marketing η επίδραση του GDPR είναι πολύ σημαντική. Προσωπικό δεδομένο θεωρείται οποιαδήποτε πληροφορία που θα μπορούσε να

χρησιμοποιηθεί από μόνη της ή σε συνδυασμό με άλλα δεδομένα, για τον εντοπισμό ενός ατόμου (Προστασία δεδομένων στην ΕΕ, 2018).

Οι βασικές αλλαγές είναι οι εξής (Σχήμα 5.1):

Σχήμα 5.1: Οι βασικές αλλαγές στο email marketing.

Πηγή: (Προστασία δεδομένων στην ΕΕ, 2018).

1. Λήψη συγκατάθεσης

Κάθε φορά που συλλέγονται διευθύνσεις ηλεκτρονικού ταχυδρομείου για να προστεθούν στη λίστα αλληλογραφίας, ο συνδρομητής πρέπει να λάβει ενημέρωση και να συναινέσει σε αυτό. Δηλαδή πρέπει να εκπαιδευτεί ο συνδρομητής για το τι θα κάνει με τη διεύθυνση του ηλεκτρονικού ταχυδρομείου, ακόμα κι αν αυτό σημαίνει ότι θα παρακολουθείται η συμπεριφορά του. Όταν συμφωνηθεί από τον συνδρομητή λοιπόν, μόνο τότε μπορεί να σταλεί το email.

Πρέπει επίσης να ληφθούν παρόμοια δικαιώματα από τους συνδρομητές και για τις υπάρχουσες διευθύνσεις ηλεκτρονικού ταχυδρομείου που υπάρχουν στην database που συλλέχθηκαν πριν από τις 25 Μαΐου 2018.

2. Δικαίωμα χρήσης

Ο συνδρομητής έχει το δικαίωμα να λάβει την επιβεβαίωση, ότι τα δεδομένα που συλλέγονται χρησιμοποιούνται αποκλειστικά για το σκοπό για τον οποίο συλλέχθηκαν. Επιπλέον, αντίγραφο των δεδομένων πρέπει να του παρέχονται χωρίς κόστος σε ηλεκτρονική μορφή.

3. Δικαίωμα στην Λήθη

Όταν ο συνδρομητής ζητήσει να ξεχαστεί, τότε τα προσωπικά δεδομένα διαγράφονται. Σε αυτό περιλαμβάνονται όλες οι βάσεις δεδομένων που τα περιλαμβάνουν όπως επίσης και από τα αντίγραφα ασφαλείας όπου και να είναι αυτά.

4. Ειδοποίηση παραβίασης

Σε ενδεχόμενο διαρροής των δεδομένων η εταιρεία οφείλει να ειδοποιήσει τους πελάτες και τους ελεγκτές χωρίς αδικαιολόγητη επιβράδυνση.

5. Τοπική δικαιοδοσία

Για τις εταιρείες που επεξεργάζονται προσωπικά δεδομένα από οποιονδήποτε κάτοικο της ΕΕ, τότε ισχύουν όλες οι προαναφερόμενες προϋποθέσεις. Αυτό δεν περιορίζεται μόνο σε εταιρείες που είναι στην ΕΕ, αλλά και σε αυτές που εδρεύουν σε χώρες εκτός ΕΕ εάν προσφέρουν αγαθά και υπηρεσίες στους κατοίκους της ΕΕ.

5.2.2 GDPR και Πολίτες

Ο τρόπος με τον οποίο οι πολίτες είναι τώρα εξασφαλισμένοι με το δικαίωμα να γνωρίζουν πότε έχουν παραβιαστεί τα δεδομένα τους είναι μία από τις μεγαλύτερες αλλαγές που επέφερε το GDPR. Οι εταιρίες υποχρεούνται από το νόμο να ειδοποιούν τους καθορισμένους αρμόδιους εθνικούς οργανισμούς στην περίπτωση που εντοπιστεί παράβαση στα συστήματα τους, προκειμένου να διασφαλιστεί ότι τα δεδομένα των πελατών που διατηρούν δεν έχουν καταχραστεί. Με τον τρόπο αυτό, οι πελάτες θα έχουν μια πιο διαφανή εικόνα του τρόπου επεξεργασίας των δεδομένων τους.

Ήδη πολλές εταιρίες έχουν προοδεύσει προς αυτή τη διαφάνεια μεταξύ αυτών και των πελατών τους. Αυτό γίνεται με την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου από εταιρείες που δίνουν πολύ περισσότερες πληροφορίες σχετικά με τον τρόπο χρήσης των δεδομένων. Ακόμα, πολλοί οργανισμοί συνομιλούν με τους πελάτες για να διαπιστώσουν εάν επιθυμούν ή όχι να είναι μέρος της βάσης δεδομένων τους, καθιστώντας έτσι το ίδιο εύκολο για τον πελάτη να αποχωρήσει από την ύπαρξη του σε λίστες αλληλογραφίας (Προστασία δεδομένων στην ΕΕ, 2018).

5.2.3 GDPR και Παραβιάσεις Δεδομένων

Με την εκκίνηση του GDPR, ενεργοποιείται ένα νέο σύνολο κανόνων το οποίο πρέπει να ακολουθούν όλες οι επιχειρήσεις όσον αφορά την παραβίαση δεδομένων. Αρχικά, οι επιχειρήσεις υποχρεούνται να αναφέρουν πιθανή παραβίαση ή μη εξουσιοδοτημένο περιστατικό το οποίο σχετίζεται με τα προσωπικά δεδομένα των πελατών της. Εάν ένα όνομα, ιατρικό αρχείο, διεύθυνση, λεπτομέρεια τράπεζας ή οποιοδήποτε άλλο κομμάτι ιδιωτικών δεδομένων παραβιαστεί, τότε η επιχείρηση οφείλει να ειδοποιεί τους θιγόμενους και να το αναφέρει στον αρμόδιο ρυθμιστικό φορέα, ώστε η έκταση της ζημιάς να περιοριστεί.

Η παραβίαση πρέπει να αναφέρεται στον αρμόδιο ρυθμιστικό φορέα μέσα σε 72 ώρες από την επιχείρηση, τη στιγμή που εντοπιστεί παραβίαση δεδομένων. Παράλληλα, το GDPR αποφασίζει ότι οι πελάτες πρέπει να ειδοποιούνται για να διαχειριστούν τη ζημία όσο πιο σύντομα γίνεται, στην περίπτωση που το είδος της παραβίαση απαιτεί την ενημέρωση των πελατών.

Όταν συμβαίνει παραβίαση, η επιχείρηση πρέπει να ενημερώνει άμεσα τους θιγόμενους μέσω της κοινοποίησης παραβίασης (άρθρο 33) απευθείας στα θύματα. Με άλλα λόγια, ένα δελτίο τύπου ή μια ανακοίνωση στην ιστοσελίδα της εταιρείας δεν καλύπτει το καθήκον της επιχείρησης ως δημοσίευση προς τους πελάτες της. Η κοινοποίηση πρέπει να γίνεται προσωπικά (Protection of personal data, 2018).

5.2.4 Πρόστιμα και Κυρώσεις

Όταν δεν υπάρχει συμμόρφωση με το GDPR προκαλούνται οικονομικές επιπτώσεις ανάλογα με τη σοβαρότητα της παραβίασης των δεδομένων αλλά και από το εάν η επιχείρηση υπολογίζει τους κανονισμούς συμμόρφωσης και ασφάλειας. Τα πρόστιμα από 10 εκατομμύρια ευρώ έως 4% του συνολικού ετήσιου κύκλου εργασιών της επιχείρησης. Βέβαια, υπάρχει και ένα υψηλό πρόστιμο ύψους 20 εκατομμυρίων ευρώ ή έως 4% του συνολικού ετήσιου κύκλου εργασιών της επιχείρησης σε περίπτωση παραβίασης των δεδομένων, εάν δεν προσφέρουν στους πελάτες πρόσβαση όταν ζητούνται δεδομένα τους, παράνομη ή μη εξουσιοδοτημένη διεθνή μεταφορά προσωπικών δεδομένων, όπως επίσης στην περίπτωση που δεν θέσουν σε εφαρμογή τις απαραίτητες διαδικασίες GDPR (Προστασία δεδομένων στην ΕΕ, 2018).

5.3 ΤΟ GDPR ΩΣ ΕΥΚΑΙΡΙΑ

Όσον αφορά τα προσωπικά δεδομένα που τηρούνται στις εταιρείες, αποθηκεύονται διαρκώς νέες πληροφορίες σχετικά με πελάτες, υπαλλήλους και συνεργάτες, για την διεκπεραίωση διάφορων εργασιών, όπως (Σχήμα 5.2) (Droukas, 2017):

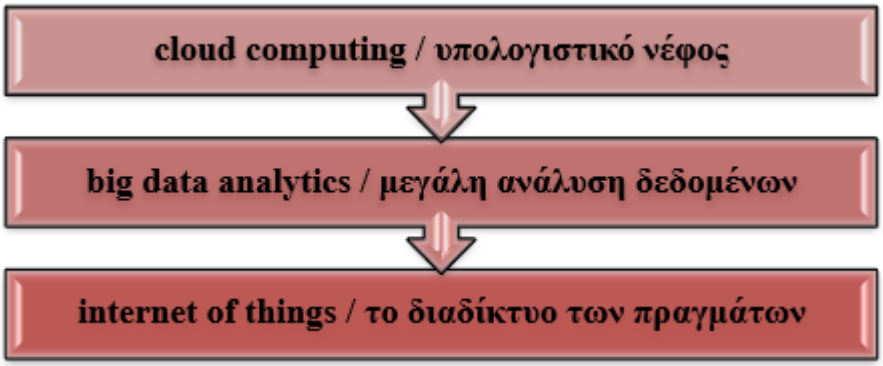
Σχήμα 5.2: Εργασίες Εταιρειών.

Πηγή: (Droukas, 2017).

Δίχως ο υπεύθυνος να διερωτηθεί εάν χρειάζονται σε διαφορετική/επιπλέον εργασία (π.χ. παραγγελιοληψία, τιμολόγηση, πληρωμή κ.ά.). Επιπροσθέτως, τα ίδια στοιχεία τα αποθηκεύουν/συλλέγουν διαφορετικές μονάδες της ίδιας εταιρείας για το ίδιο φυσικό πρόσωπο για διαφορετικούς σκοπούς, με αποτέλεσμα να αποθηκεύονται τα στοιχεία του προμηθευτή ή του πελάτη, πολλές φορές, σε πολλές θέσεις και μάλιστα δίχως λόγο.

Άρα είναι ευκαιρία για οποιαδήποτε εταιρεία να προβεί σε «γενική καθαριότητα» σε επίπεδο προσωπικών δεδομένων. Πρέπει άμεσα να αλλαχθεί η λανθασμένη συμπεριφορά και η στάση απέναντι στη διαχείριση προσωπικών δεδομένων, διότι με την εφαρμογή του Κανονισμού (Κανονισμός ΕΕ 2016 / 679 ή GDPR), υποχρεώνονται όλες οι επιχειρήσεις, να χαρτογραφήσουν ποια δεδομένα αφορούν ποιο φυσικό πρόσωπο και να υλοποιήσουν κατάλληλα μέτρα προστασίας. (Droukas, 2017):

Το πρόβλημα της διευθέτησης των προσωπικών δεδομένων είναι πολύ μεγάλο εάν ληφθούν υπόψη οι τεχνολογικές εξελίξεις στις λειτουργίες, όπως (Σχήμα 5.3) (Droukas, 2017):



Σχήμα 5.3: Λειτουργίες Εταιρειών.

Πηγή: (Droukas, 2017)

Σήμερα, ανά τον κόσμο, πραγματοποιείται υλοποίηση προγραμμάτων προστασίας της ιδιωτικότητας (data privacy protection program), με κύριο στόχο τη σωστότερη, καλύτερη και αποτελεσματικότερη οργάνωση των προσωπικών δεδομένων.

Ήδη διάφοροι Διεθνείς Οργανισμοί χρησιμοποιούν βέλτιστες πρακτικές, οι οποίες είναι συμμορφωμένες με τους κανονισμούς GDPR και εφαρμόζονται από τις περισσότερες επιχειρήσεις/φορείς/οργανισμούς. Οι χρησιμοποιηθείσες διαδικασίες έχουν διερευνηθεί και τεκμηριωθεί από διεθνείς φορείς εξειδικευμένους σε θέματα ηλεκτρονικής διακυβέρνησης και συμμόρφωσης σύμφωνα με τους κανονισμούς GDPR.

Σε αυτό το πλαίσιο κατευθύνεται και ο διεθνής οργανισμός ISACA International, με την δημιουργία / διαμόρφωση προτύπων, αλλά και επαγγελματικών πιστοποιήσεων στο χώρο της Ηλεκτρονικής Διακυβέρνησης και της Ασφάλειας/Ελέγχου Πληροφορικών συστημάτων σύμφωνα με τους κανονισμούς GDPR. Έχει δημιουργήσει 3 εργαλεία για την σωστότερη και αποτελεσματικότερη τυποποίηση των κανόνων GDPR, τα οποία είναι (Droukas, 2017):

- «ISACA Privacy Principles & Program Management Guide»
- «Implementing a Privacy Protection Program: Using COBIT 5 Enablers with the ISACA Privacy Principles»,
- «GDPR Data Protection Impact Assessments & the Assessment Tool».

6 ΚΕΦΑΛΑΙΟ: «Η ΕΠΙΔΡΑΣΗ ΤΟΥ GDPR ΣΤΗΝ ΑΣΦΑΛΕΙΑ»

6.1 ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ

Ο στόχος της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι η εξυπηρέτηση του ανθρώπου. Ωστόσο δεν είναι απόλυτο το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα και συνεπώς θα πρέπει να εκτιμάται σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται με άλλα θεμελιώδη δικαιώματα, σύμφωνα με την αρχή της αναλογικότητας,. Στον παρόντα κανονισμό όλα τα θεμελιώδη δικαιώματα είναι σεβαστά και εφαρμόζονται οι ελευθερίες και οι αρχές οι οποίες σημειώνονται στον Χάρτη όπως κατοχυρώνονται στις Συνθήκες. Αφορά κυρίως τον σεβασμό της ιδιωτικής και οικογενειακής ζωής, την προστασία των δεδομένων προσωπικού χαρακτήρα, της κατοικίας και των επικοινωνιών, την ελευθερία έκφρασης και πληροφόρησης, την ελευθερία σκέψης, συνείδησης και θρησκείας, την επιχειρηματική ελευθερία, το δικαίωμα πραγματικής προσφυγής και αμερόληπτου δικαστηρίου και την πολιτιστική, θρησκευτική και γλωσσική πολυμορφία (Data protection in the EU, 2018).

Νέες προκλήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα δημιουργήθηκαν από τις ραγδαίες τεχνολογικές εξελίξεις και η παγκοσμιοποίηση. Σημαντικά, επίσης, αυξήθηκε η κλίμακα της συλλογής και της ανταλλαγής δεδομένων προσωπικού χαρακτήρα. Η τεχνολογία δίνει τη δυνατότητα στις ιδιωτικές επιχειρήσεις και δημόσιες αρχές να χρησιμοποιήσουν δεδομένα προσωπικού χαρακτήρα σε πρωτόγνωρη κλίμακα ώστε να επιτευχθούν οι δραστηριότητές τους. Ολοένα και περισσότερο τα φυσικά πρόσωπα κοινοποιούν προσωπικές πληροφορίες και τις διαθέτουν παγκοσμίως. Τόσο την οικονομία όσο και την κοινωνική ζωή η τεχνολογία έχει αλλάξει και θα πρέπει να διευκολύνει περαιτέρω την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης και τη διαβίβαση σε τρίτες χώρες και διεθνείς οργανισμούς, διασφαλίζοντας παράλληλα υψηλό επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα.

Οι εξελίξεις αυτές προϋποθέτουν ένα δυνατό και πιο συνεκτικό πλαίσιο προστασίας των δεδομένων στην Ένωση, το οποίο θα υποστηρίζεται από αυστηρή εφαρμογή της νομοθεσίας, καθώς είναι σημαντικό να δημιουργηθεί η απαραίτητη εμπιστοσύνη που θα επιτρέψει στην ψηφιακή οικονομία να αναπτυχθεί στην εσωτερική αγορά. Τα φυσικά πρόσωπα

θα πρέπει να έχουν τον έλεγχο των δικών τους δεδομένων προσωπικού χαρακτήρα. Θα πρέπει να ενισχυθούν η ασφάλεια δικαίου και η πρακτική ασφάλεια για τα φυσικά πρόσωπα, τους οικονομικούς παράγοντες και τις δημόσιες αρχές (lawspot.gr/GDPR, 2018).

6.2 ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ

Έννομο συμφέρον του ενδιαφερόμενου υπευθύνου επεξεργασίας δεδομένων αποτελεί η επεξεργασία δεδομένων προσωπικού χαρακτήρα, στον βαθμό που είναι αυστηρά αναγκαία και ανάλογη για τους σκοπούς της διασφάλισης της ασφάλειας δικτύων και πληροφοριών. Πρόκειται για την ικανότητα ενός δικτύου ή ενός συστήματος πληροφοριών να ανθίσταται, σε ένα δεδομένο επίπεδο εμπιστοσύνης, σε τυχαία γεγονότα ή παράνομες ενέργειες οι οποίες βάζουν σε κίνδυνο τη γνησιότητα, τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα αποθηκευμένων ή διαβιβαζόμενων δεδομένων προσωπικού χαρακτήρα. Επίσης, κινδυνεύει και η ασφάλεια των σχετικών υπηρεσιών που παρέχουν τα συγκεκριμένα δίκτυα και συστήματα ή που είναι προσπελάσιμες μέσω των εν λόγω δικτύων και συστημάτων, ή που προσφέρονται από δημόσιες αρχές, από ομάδες χειρισμού έκτακτων αναγκών στην πληροφορική (CERT), από ομάδες παρέμβασης για συμβάντα σχετικά με την ασφάλεια των υπολογιστών (CSIRT), από παρόχους δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών και από παρόχους τεχνολογιών και υπηρεσιών ασφάλειας (Protection of personal data, 2018).

6.3 ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Κατάλληλα τεχνικά και οργανωτικά μέτρα εφαρμόζονται από τον υπεύθυνο επεξεργασίας και από τον εκτελούντα την επεξεργασία ώστε να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων (Protection of personal data, 2018):

a). την ψευδωνυμοποίηση και την κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα,

b). τη δυνατότητα διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,

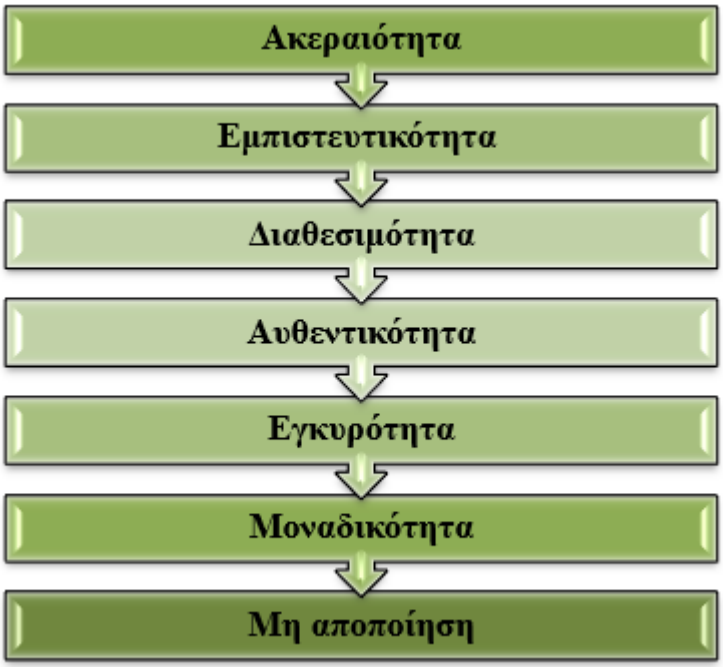
c). τη διαδικασία για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

d). τη δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος.

6.4 ΤΡΟΠΟΙ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ

Για τα προσωπικά δεδομένα σε ηλεκτρονική μορφή ο σχεδιασμός ασφαλών πολιτικών, είναι άμεσα συνδεδεμένος τόσο με τεχνικές, διαδικασίες και διοικητικά μέτρα όσο και με ηθικό-κοινωνικές αντιλήψεις, αρχές και παραδοχές, ώστε να προφυλάσσονται από κάθε είδους απειλή τυχαία ή σκόπιμη. Ως εκ τούτου, οι διαδικασίες σχεδιασμού πολιτικών ασφαλείας, δεν θα πρέπει να παρεμβαίνουν στην απαρακώλυτη λειτουργία των πληροφοριακών συστημάτων, ενώ υποχρεούνται να εφαρμόζουν την αρχή της αποκέντρωσης, της ύπαρξης αντικατάστασης και την αρχή της άμυνας σε βάθος.

Ο εντοπισμός και χαρακτηρισμός ως εμπιστευτικών των πληροφοριών που πρόκειται να χρησιμοποιηθούν και να προστατευθούν αποτελούν το πιο βασικό σημείο στη διαδικασία σχεδιασμού ασφαλών πολιτικών. Οι πολιτικές ασφάλειας εκτός από τις αρχές της Ακεραιότητας Πληροφοριών, την Εμπιστευτικότητα και τη Διαθεσιμότητα Πληροφοριών, οφείλουν να περικλείουν και τους όρους αυθεντικότητα, εγκυρότητα, μοναδικότητα και μη αποποίηση (Controversial Topics GDPR, 2018).



Σχήμα 6.1: Αρχές κατά την διαδικασία σχεδιασμού ασφαλών πολιτικών για την ασφάλεια των προσωπικών δεδομένων.

Πηγή: (Controversial Topics GDPR, 2018).

Πιο συγκεκριμένα, οι τρεις βασικές αρχές της διαδικασίας σχεδιασμού ασφαλών πολιτικών για την ασφάλεια των προσωπικών δεδομένων είναι (Controversial Topics GDPR, 2018):

1. Ακεραιότητα

Πρόκειται για τη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από άτομα που δεν είναι εξουσιοδοτημένα, αλλά και στην απαγόρευση της πρόσβασης ή χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς την απαραίτητη άδεια.

2. Διαθεσιμότητα

Σχετίζεται με την εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε πρέπει να χρησιμοποιηθούν.

3. Εμπιστευτικότητα

Σημαίνει ότι ευαίσθητες πληροφορίες απαγορεύεται να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα. Για τη διαρροή ευαίσθητων πληροφοριών μπορούν να χρησιμοποιηθούν πιο παραδοσιακές μέθοδοι από την ψηφιακή υποκλοπή.

6.4.1 Κρυπτογράφηση

Ένας βασικός τρόπος για την αποτελεσματική προστασία, είναι η κρυπτογράφηση των δεδομένων, δηλαδή η διαδικασία κωδικοποίησης της πληροφορίας, ώστε να εμποδίζεται η ανάγνωσή της από μη εξουσιοδοτημένα μέρη.

Η ισχύς της κρυπτογράφησης πραγματοποιείται με μέγιστο μήκος του κλειδιού (bits) και τον αλγόριθμο κρυπτογράφησης που χρησιμοποιείται.

Επίσης, για να «σπάσει» η κρυπτογράφηση, δοκιμάζονται όλα τα πιθανά κλειδιά, με το μήκος των κλειδιών κρυπτογράφησης να έχει κάνει αυτή την προσέγγιση ανέφικτη.

Η κρυπτογράφηση γίνεται με δύο (2) διαφορετικούς τρόπους (Controversial Topics GDPR, 2018):

1. Κρυπτογραφημένη αποθήκευση: εφαρμόζεται για την κρυπτογράφηση ενός ολόκληρου δίσκου, drive ή συσκευής.
2. Κρυπτογραφημένο περιεχόμενο ή τμηματική κρυπτογράφηση: πρόκειται για την κρυπτογράφηση αρχείων, ή κειμένου, σε επίπεδο εφαρμογής. Το πιο συχνό είδος κρυπτογράφησης είναι το email (Controversial Topics GDPR, 2018).

6.5 ΤΑ ΠΙΟ ΚΟΙΝΑ ΖΗΤΗΜΑΤΑ ΣΤΟ INTERNET SECURITY

Το Διαδίκτυο προσφέρει μια πληθώρα ευκαιριών αλλά φέρνει και πολλούς κινδύνους. Για παράδειγμα, όταν κάποιος κάνει online πληρωμές υπάρχουν πολλές απειλές που προέρχονται από πολλαπλές πηγές (Nguyen, 2018):

1. Hackers

Πρόκειται για εκείνους που επιχειρούν να παραβιάσουν τα μέτρα ασφάλειας. Τα κίνητρά τους, κατά καιρούς, ποικίλλουν, όπως απλώς επιθυμούν να αναδείξουν ελλείψεις σε εταιρείες και άλλους ιδιοκτήτες ιστοχώρου, έτσι ώστε να μπορούν να εντείνουν τα μέτρα ασφάλειας τους.

Άλλοι χάκερ φαίνονται να αποσκοπούν σε οικονομικά οφέλη από την αντιγραφή ιδιωτικών πληροφοριών, ενώ άλλοι απλώς θέλουν να προκαλέσουν αναστάτωση. Ανεξάρτητα από τους λόγους των χάκερ, μπορεί να αποτελέσει σοβαρή απειλή για την ασφάλεια.

2. Ιοί

Πρόκειται για προγράμματα που είναι σχεδιασμένα για να κερδίσουν την είσοδο στους υπολογιστές ανυποψίαστων χρηστών. Από τη στιγμή που έχουν κερδίσει μια θέση μέσα σε ένα σύστημα υπολογιστή, στη συνέχεια θα προσπαθήσει να επαναληφθεί πριν εξαπλωθεί μέσω e-mail, στα δίκτυα ή / και στις αποσπώμενες συσκευές αποθήκευσης.

Συνήθως, η αποστολή τους είναι να διαφθείρουν ή να καταστρέψουν τα δεδομένα ή να βλάψουν τη λειτουργία του υπολογιστή. Οι ιοί μπορεί να αποκτηθούν με πολλούς τρόπους, όπως μέσω του ηλεκτρονικού ταχυδρομείου, του peer-to-peer downloading, των υπηρεσιών μηνυμάτων στο διαδίκτυο και κατεβάζοντας μολυσμένα αρχεία που βρέθηκαν στο διαδίκτυο.

3. Spywarε

Το Spyware μπορεί να αποδειχθεί μια σημαντική ενόχληση, διότι συνήθως στοχεύει στη συλλογή προσωπικών πληροφοριών και στην περιήγηση συνηθειών, προκειμένου να παραδώσει στοχευμένες διαφημίσεις.

Εκτός από την αύξηση των διαφημιστικών μηνυμάτων είναι πιθανό να επηρεάσει και την απόδοση του υπολογιστή με hogging πόρους.

4. Σκουλήκια

Ένας ιός τύπου worm είναι ένα αυτοαναπαραγόμενο πρόγραμμα το οποίο θα προσπαθήσει να εξαπλωθεί σε όλο το δίκτυο, είτε μέσω routers, του διαδικτύου ή μέσω ηλεκτρονικού ταχυδρομείου. Σε αντίθεση με έναν ιό, ένα σκουλήκι δεν χρειάζεται να συνδεθεί με ένα άλλο πρόγραμμα, προκειμένου να διαδοθεί. Τα σκουλήκια μπορούν να προκαλέσουν αναστάτωση σε συστήματα ηλεκτρονικών υπολογιστών, λόγω του υπερβολικού ποσού του εύρους ζώνης που χρησιμοποιούν μερικές φορές.

5. Phishing

Για ορισμένους, το phishing είναι ένα τέχνασμα εμπιστοσύνης, που σχεδιάστηκε από τους επίδοξους κλέφτες, προκειμένου να υποκλέψουν από ανυποψίαστους χρήστες ηλεκτρονικών υπολογιστών τα πιο πολύτιμα προσωπικά δεδομένα ή/και οικονομικές πληροφορίες.

Παραδοσιακά, μέσω του phishing γίνονται προσπάθειες για απόκτηση δεδομένων, όπως τα στοιχεία του τραπεζικού λογαριασμού, οι αριθμοί κοινωνικής ασφάλισης και αριθμοί πιστωτικών καρτών, είτε για άμεσο οικονομικό όφελος ή για να διευκολυνθεί η κλοπή ταυτότητας.

Επίσης είναι εξίσου πιθανό να απευθύνονται σε χρήστες των δικτυακών τόπων κοινωνικής δικτύωσης, προκειμένου να προσπαθήσουν και να κλέψουν τους λογαριασμούς τους είτε να τα χρησιμοποιήσουν ως εφαλτήριο για απάτες ή ως μέσο για spamming στους φίλους του θύματος και άλλες επαφές.

Οι Phishing απάτες φτάνουν μέσω e-mail και έχουν σχεδιαστεί για να εμφανίζονται από νόμιμες οργανώσεις, έτσι ώστε να εξαπατήσουν τον παραλήπτη.

6. Spamming

Πρόκειται για οποιαδήποτε μορφή αυτόκλητων μηνυμάτων, είτε πρόκειται για email, προσωπικό μήνυμα forum ή ακόμα Tweet. Όσοι βρίσκονται πίσω από το Spam γνωρίζουν ότι το ποσοστό ανταπόκρισης στα σκουπίδια τους θα είναι απίστευτα χαμηλή. Συνεχίζουν, όμως, επειδή μπορεί να στείλουν πολλές χιλιάδες spam μηνύματα κάθε ώρα της ημέρας χωρίς κόστος. Συνεπώς, ακόμη και ένα πολύ μικρό ποσοστό ανταπόκρισης μπορεί να οδηγήσει σε τεράστια κέρδη για τους spammers. Τα Spam μηνύματα συνήθως δεν αποτελούν απειλή για την ασφάλεια, αλλά μπορεί να είναι απίστευτα ενοχλητικό και αποσπούν την προσοχή. Είναι, όμως, να κρύψουν άλλα ανεπιθύμητα αντικείμενα, όπως ιούς, worms, spy ware και άλλα κακόβουλα λογισμικά.

7. Κλοπή Ταυτότητας

Η κλοπή ταυτότητας είναι ένα πρόβλημα που διαρκώς αυξάνεται. Αυτό το έγκλημα μπορεί να βλάψει σοβαρά τα οικονομικά του θύματος για πολλά χρόνια. Κλέφτες ταυτότητας αποκτούν πληροφορίες σχετικά με κάποιον μέσα από μια ποικιλία μέσων των οποίων το συνηθέστερο είναι το phishing. Αν μπορούν να πάρουν τα προσωπικά δεδομένα, όπως ονόματα, ημερομηνίες γέννησης, αριθμούς κοινωνικής ασφάλισης, κλπ. Η ψεύτικη ταυτότητα μπορεί να χρησιμοποιηθεί σε πολλά άλλα εγκλήματα (Nguyen, 2018).

Συνεπώς είναι απαραίτητη η χρήση ενός πλήρως ενημερωμένου προγράμματος anti-virus. Δηλαδή ο χρήστης θα πρέπει να:

- Βεβαιωθεί ότι έχει ένα τείχος προστασίας και ότι είναι πλήρως λειτουργικό.
- Επιλέξει ασφαλείς και δύσκολους κωδικούς πρόσβασης και να τους αλλάζει σε τακτική βάση.
- Εγκαταστήσει τις ενημερώσεις και τα patches για το λειτουργικό του σύστημα μόλις αυτά καταστούν διαθέσιμα.

- Μην κάνει κλικ σε συνδέσμους σε μηνύματα ηλεκτρονικού ταχυδρομείου εάν δεν είναι 100% σίγουροι ότι είναι αξιόπιστοι.

7 ΚΕΦΑΛΑΙΟ: «ΣΥΜΠΕΡΑΣΜΑΤΑ»

Ο κύριος στόχος του Κανονισμού Προστασίας Προσωπικών Δεδομένων (General Data Protection Regulation / GDPR) είναι η προστασία όλων των πολιτών της ΕΕ από την εισβολή τρίτων στην ιδιωτική τους ζωή αλλά και τις παραβιάσεις των δεδομένων σε μία κοινωνία περισσότερο βασισμένη στην διάδοση πληροφοριών, η οποία μετασχηματίστηκε ραγδαία, από τον χρόνο σύστασης της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου για την «*προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών*».

Αναμφίβολα η πιο μεγάλη αλλαγή στο ρυθμιστικό περιβάλλον της ιδιωτικής ζωής των δεδομένων επήλθε με την εκτενή αρμοδιότητα του GDPR, καθώς ισχύει για όλες τις εταιρείες οι οποίες επεξεργάζονται τα προσωπικά δεδομένα των υποκειμένων που διαμένουν στην Ένωση, χωρίς να λαμβάνεται υπόψη η τοποθεσία της εταιρείας. Αρχικά, η εδαφική εφαρμογή της οδηγίας δε ήταν ξεκάθαρη και αναφέρεται σε διαδικασία επεξεργασίας δεδομένων «στο πλαίσιο εγκατάστασης».

Το γεγονός ότι η Ευρωπαϊκή Ένωση σε μια εποχή που τα προσωπικά δεδομένα κυκλοφορούν ελεύθερα στο διαδίκτυο, έρχεται να αντικαταστήσει κεντρικά μία παρωχημένη οδηγία με έναν κανονισμό, είναι ένα πολύ θετικό βήμα. Με το ίντερνετ να αποτελεί ένα μέσο του οποίου ο ρόλος συνεχώς ενισχύεται, οι χρήστες πρέπει να νιώσουν σίγουροι για τις πληροφορίες που μοιράζονται με εταιρείες, φορείς και οργανισμούς. Η έρευνα του Ευρωβαρόμετρού 2015, κατέδειξε ότι 8 στους 10 Ευρωπαίους νιώθουν ότι δεν έχουν τον πλήρη έλεγχο των δεδομένων προσωπικού χαρακτήρα που τους αφορούν και αυτό είναι κάτι που ο GDPR επιδιώκει να αλλάξει ταυτόχρονα.

Πλέον η υποχρεωτική εφαρμογή του GDPR είναι σε ισχύ από τις 25 Μαΐου, με σημαντικό αριθμό εταιρειών να έχουν αναθεωρήσει τις μεθόδους συλλογής, επεξεργασίας και αποθήκευσης προσωπικών δεδομένων.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) (ΕΕ) 2016/679 είναι ένας κανονισμός της νομοθεσίας της ΕΕ για την προστασία των δεδομένων και της ιδιωτικής ζωής για όλα τα άτομα εντός της Ευρωπαϊκής Ένωσης (ΕΕ) και του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ).

Ο κανονισμός εφαρμόζεται εάν ο υπεύθυνος επεξεργασίας δεδομένων (ένας οργανισμός που συλλέγει δεδομένα από κάτοικους της ΕΕ) ή ο μεταποιητής (ένας οργανισμός που επεξεργάζεται δεδομένα για λογαριασμό υπεύθυνου επεξεργασίας δεδομένων όπως οι πάροχοι υπηρεσιών Cloud computing) ή το πρόσωπο στο οποίο αναφέρονται τα δεδομένα (πρόσωπο). Υπό ορισμένες συνθήκες, ο κανονισμός εφαρμόζεται επίσης σε οργανισμούς που εδρεύουν εκτός ΕΕ, εάν συλλέγουν ή επεξεργάζονται προσωπικά δεδομένα ατόμων που βρίσκονται εντός της ΕΕ. Ο κανονισμός δεν εφαρμόζεται στην επεξεργασία δεδομένων από ένα πρόσωπο για «καθαρά προσωπική ή οικιακή δραστηριότητα και συνεπώς χωρίς σύνδεση με επαγγελματική ή εμπορική δραστηριότητα».

Οι καταναλωτές, πλέον, μπορούν να ζητήσουν την διαγραφή των προσωπικών τους στοιχείων, αλλά το GDPR ενισχύει αυτό το δικαίωμα διαγραφής με το λεγόμενο«Right to be Forgotten».

Ωστόσο, η μεγαλύτερη αλλαγή, πέρα από την τήρηση θα είναι η μετατόπιση της στάσης του οργανισμού απέναντι στην προστασία της ιδιωτικής ζωής. Το πιο σημαντικό θα είναι η απόκτηση της εμπιστοσύνης των πελατών και η απόκτηση ανταγωνιστικού πλεονεκτήματος, ακριβώς επειδή οι πελάτες προσέχουν ιδιαίτερα την ιδιωτική τους ζωή. Τέλος, εκτιμούν τις απλές και διαφανείς διαδικασίες για την προάσπιση των δικαιωμάτων τους.

Κατάλληλα τεχνικά και οργανωτικά μέτρα εφαρμόζονται από τον υπεύθυνο επεξεργασίας και από τον εκτελούντα την επεξεργασία προκειμένου να εξασφαλίζεται το απαραίτητο επίπεδο ασφάλειας απέναντι στους κινδύνους, όπως:

a). Τη δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος,
b). Την ψευδωνυμοποίηση και την κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα,
c). Τη δυνατότητα διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,

Στη διαδικασία σχεδιασμού ασφαλών πολιτικών ο εντοπισμός και χαρακτηρισμός ως εμπιστευτικών των πληροφοριών που πρόκειται να χρησιμοποιηθούν και να προστατευθούν είναι το πιο βασικό σημείο. Οι πολιτικές ασφάλειας εκτός από τις αρχές της Ακεραιότητας Πληροφοριών, την Εμπιστευτικότητα και τη Διαθεσιμότητα Πληροφοριών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ

Επίσημη Εφημερίδα τον Ευρωπαϊκών Κοινοτήτων. (1995, 11 23). *ΟΔΗΓΙΑ 95/46/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.* Ανάκτηση από Επίσημη Εφημερίδα τον Ευρωπαϊκών Κοινοτήτων: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=EL

Ευρωπαϊκό Κοινοβούλιο: 31995L0046-Οδηγία 95/46/ΕΚ. (1995, 11 23). *Προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.* Ανάκτηση από Ευρωπαϊκό Κοινοβούλιο: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:31995L0046&from=EL

Θεματολογικά δελτία για την Ευρωπαϊκή Ένωση. (2021). Ανάκτηση από Ευρωπαϊκό Κοινοβούλιο: https://www.europarl.europa.eu/factsheets/el/sheet/169/the-european-economic-area-eea-switzerland-and-the-north

Κανελλόπουλος, Ν. (2018, 3 9). *Φορολογική και λογιστική πύλη ενημέρωσης Taxheaven*. Ανάκτηση από Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα (GDPR): https://www.taxheaven.gr/laws/circular/view/id/28194

Παπαδοπούλου, Λ. (2017, 12 14). *GDPR: έλεγχος 20 σημείων – για μικρές και μεσαίες επιχειρήσεις*. Ανάκτηση από averway: http://www.averway.com/gdpr-checklist/

Προστασία δεδομένων στην ΕΕ. (2018). Ανάκτηση από Ευρωπαϊκή Επιτροπή: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_el

Σπυριδάκη, Κ. (2018). *Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (GDPR)*. Ανάκτηση από SAS Institute: https://www.sas.com/el_gr/insights/articles/data-management/local/eu-data-protection-gdpr.html

Τσουραμάνης, Χ. (2005). *Ψηφιακή Εγκληματικότητα.* Β.Ν.Κατσαρού.

ΞΕΝΟΓΛΩΣΣΗ – ΔΙΕΘΝΗΣ

Burton, A. (2019, 5 19). *GDPR and Beyond: The Intersection of Privacy and Trademark Law*. Ανάκτηση από worldipreview.com: https://www.worldipreview.com/contributed-article/gdpr-and-beyond-the-intersection-of-privacy-and-trademark-law

Butterworth, M. (2018, 4). The ICO and artificial intelligence: The role of fairness in the GDPR framework. *Computer Law & Security Review, 34*(2), σσ. 257-268.

Controversial Topics GDPR. (2018, 5). Ανάκτηση από eugdpr: https://www.eugdpr.org/controversial-topics.html

Curry, S. (2018, 3). Why the security industry should stop relying on FUD. *Computer Fraud & Security, 2018*(3), σσ. 10-12.

CyberCrime-ΚΕΔΙΒΙΜ. (2020). *Έγκλημα στον Κυβερνοχώρο*. Ανάκτηση από ΚΕΔΙΒΙΜ: http://www.diaviou.auth.gr/programs/egklima-ston-kyvernochoro/

Data protection in the EU. (2018, 5). Ανάκτηση από European Commission: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en#data-protection-in-the-eu-institutions-and-bodies

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018, 4). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review, 34*(2), σσ. 193-203.

Dennis, M. A. (2021, 3). *Cybercrime*. Ανάκτηση από Encyclopædia Britannica, Inc.: https://www.britannica.com/topic/cybercrime

Droukas, P. (2017). Πώς να μετατρέψετε το GDPR σε ευκαιρία. *6th ISACA Athens Chapter Conference and Data Privacy Workshop.* Athens: ISACA .

GDPR Timeline of Events. (2018, 5). Ανάκτηση από eugdpr: https://www.eugdpr.org/gdpr-timeline.html

Gellert, R. (2018, 4). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review, 34*(2), σσ. 279-288.

Hedley, D., & Jacobs, M. (2017, 11). The shape of things to come: the Equifax breach, the GDPR and open-source security. *Computer Fraud & Security, 2017*(11), σσ. 5-7.

James, L. (2018, 5). Making cyber-security a strategic business priority. *Network Security, 2018*(5), σσ. 6-8.

Jiang, Q., Huang, X., & Tao, R. (2013). Internet Addiction: Cybersex. *Principles of Addiction, 1*, σσ. 809-818.

Jourová, V. (2016, 1). *How will the data protection reform help fight international crime?* Ανάκτηση από European Union: file:///C:/Users/DHPE/Downloads/PP-2016-02548-00-08-EN-00.pdf

Krystlik, J. (2017). With GDPR, preparation is everything. *Computer Fraud & Security, 2017*(6), σσ. 5-8.

lawspot.gr/GDPR. (2018, 5 25). *Infographic: Τα δικαιώματα των πολιτών με βάση τον GDPR.* Ανάκτηση από Lawspot.gr: https://www.lawspot.gr/nomika-nea/infographic-ta-dikaiomata-ton-politon-me-vasi-ton-gdpr?lspt_context=gdpr

Lawspot/GDPR: Ενσωματώθηκε στη Συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο. (2018, 7 11). *GDPR: Ενσωματώθηκε στη Συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο*. Ανάκτηση από Lawspot.gr: https://www.lawspot.gr/nomika-nea/gdpr-ensomatothike-sti-symfonia-gia-ton-eyropaiko-oikonomiko-horo

Lewis, J. (2018, February). *Economic Impact of Cybercrime-No Slowing Down.* Ανάκτηση από McAfee: https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

Lotha, G. (2019, 11 19). *Cyber Crimes: An Overview*. Ανάκτηση από britannica.com: https://www.britannica.com/editor/Gloria-Lotha/7666594

Merkusheva, T. (2018). *Απεικόνιση της έννοιας του GDPR.* Ανάκτηση από dreamstime: https://gr.dreamstime.com/%CE%B1%CF%80%CE%B5%CE%B9%CE%BA%CF%8C%CE%BD%CE%B9%CF%83%CE%B7-%CE%AD%CE%BD%CE%BD%CE%BF%CE%B9%CE%B1%CF%82-gdpr-%CE%B3%CE%B5%CE%BD%CE%B9%CE%BA%CF%8C%CF%82-%CE%BA%CE%B1%CE%BD%CE%BF%CE%BD%CE%B9%CF%83%CE%BC%CF%8C%CF%82-%CF%80%CF%81%CE%

Nguyen, N. (2018). *Essential Cyber Security Handbook In Greek.* Nam H. Nguyen.

Personal Identification Number (PIN). (2021). Ανάκτηση από 123rf.com: https://www.123rf.com/photo_37919936_personal-identification-number-pin-sticky-note-business-concept-acronym.html

Protection of personal data. (2018, 5). Ανάκτηση από European Commission: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en#fundamental-rights

Ray, M. (2018, 3 9). *Cybercrime: Additional Information*. Ανάκτηση από britannica.com.

Rosencrance, L. (2020). *cyberextortion*. Ανάκτηση από searchsecurity: https://searchsecurity.techtarget.com/definition/cyberextortion

Summary of Articles Contained in the GDPR. (2018, 5). Ανάκτηση από eugdpr: https://www.eugdpr.org/article-summaries.html

Tankard, C. (2016, 6). What the GDPR means for businesses. *Network Security, 2016*(6), σσ. 5-8.

Villas, M. V., Macedo-Soares, D., & Russo, G. M. (2008, Apr./June). Bibliographical research method for business administration studies: a model based on scientific journal ranking. *Brazilian Administration Review, 5*(2).

Wachter, S. (2018, 6). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review, 34*(3), σσ. 436-449.

Πνευματικά δικαιώματα

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν. 1599/1988 και τα άρθρα 2,4,6 παρ. 3 του Ν. 1256/1982, η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον.

Χονδρογιάννη Λυγερή, 2021