ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2021-2022

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
της ΜΠΑΛΤΑ Ιωάννας (Α.Μ.: ΜΔΙ2032)

[Η ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΗ ΣΥΓΧΡΟΝΗ ΨΗΦΙΑΚΗ ΕΠΟΧΗ]

Επιβλέπων:

Στέφανος Γκρίτζαλης

Πειραιάς, Φεβρουάριος 2022

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία πραγματεύεται το ζήτημα της ασφάλειας στον Κυβερνοχώρο και πιο συγκεκριμένα το ζήτημα της Κυβερνοασφάλειας. Τις τελευταίες δεκαετίες, ο καταιγισμός των εξελίξεων στον τομέα της ψηφιακής τεχνολογίας και των πληροφοριών ήταν αναπόφευκτο να δημιουργήσει κενά ασφάλειας σε αυτούς τους τομείς. Αυτά τα προβλήματα έρχεται να επιλύσει η Κυβερνοασφάλεια ώστε να καταστεί ο Κυβερνοχώρος ασφαλής και προσβάσιμος για όλους τους χρήστες, άτομα και οντότητες.

Αρχικά, παρουσιάζεται το γενικότερο περιεχόμενο της Κυβερνοασφάλειας, οι διαφορές της από την ασφάλεια πληροφοριών, η σημασία της και στο τι αποτελεί κυβερνοεπίθεση. Ακολουθεί, η αναφορά στα εγκλήματα που διαπράττονται με ηλεκτρονικό υπολογιστή, ενώ στη συνέχεια αναλύονται οι μορφές κινδύνων που απειλούν τον Κυβερνοχώρο και οι πρακτικές που πρέπει να εφαρμοστούν για τη βελτίωση των συνθηκών λειτουργίας του Κυβερνοχώρου και της αποτελεσματικότερης δράσης της Κυβερνοασφάλειας. Στη συνέχεια, στο τέταρτο μέρος της εργασίας παρουσιάζονται ορισμένα εγκλήματα που διαπράττονται μέσω ηλεκτρονικού υπολογιστή καθώς και φαινόμενα, όπως ο διαδικτυακός εκφοβισμός και η ρητορική μίσους που εμφανίζονται όλο και πιο συχνά στο διαδίκτυο τελευταία, με τάσεις επικίνδυνα ανοδικές. Ακολουθεί ανάλυση του εσωτερικού νομοθετικού πλαισίου για την Κυβερνοασφάλεια , η ενεργοποίηση των κρατικών μηχανισμών αναφορικά με τα προβλήματα στο χώρο της Κυβερνοασφάλειας καθώς και οι δράσεις που έχουν αναληφθεί για τη διαχείριση και την αντιμετώπιση αυτών των προβλημάτων. Αντικείμενο του προτελευταίου κεφαλαίου αποτελεί το νομικό πλαίσιο για την Κυβερνοασφάλεια στην ΕΕ και οι ενέργειές της για την ενίσχυση της Κυβερνοασφάλειας μέσω της υιοθέτησης σχετικών προτάσεων. Τέλος, η εργασία καταλήγει με την αναφορά στην πανδημία κορονοϊού και πόσο αυτή έχει επηρεάσει τον τομέα της Κυβερνοασφάλειας, αλλά και τα νέα δεδομένα που έχουν προκύψει στο χώρο των επιχειρήσεων ειδικότερα και στο χώρο της εργασίας γενικότερα.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Συντομογραφίες

Συντομογραφίες

ΑΔΑΕ=Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

ΑΠ= Άρειος Πάγος

Αριθ. αριθμός

ΑΤΜ=Αυτόματη Ταμειολογιστική Μηχανή

Βλ.= βλέπε

Δευτ= δεύτερο

ΔΕΥ= Συμβούλιο Δικαιοσύνης και Εσωτερικών Υποθέσεων

Εδαφ.= εδάφιο

ΕΕΕυρΔ= Ελληνική Επιθεώρηση Ευρωπαϊκού Δικαίου

ΕΕ= Ευρωπαϊκή Ένωση

ΕΕΤΤ= Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων

ΕΚ= Ευρωπαϊκό Κοινοβούλιο

Εκδ.= έκδοση

Επιμ. επιμέλεια

Επ.= επόμενα

ΕΣΔΑ=Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου

Κλπ.= και λοιπά

ΚΠΑΑ= Κοινή Πολιτική Ασφάλειας και Άμυνας

Ν.= νόμο

ΟΛ.=ολομέλεια

Παρ.= παράγραφος

ΠΔ= Προεδρικό Διάταγμα

Περ. = περίπτωση

ΠοινΔικ.= Ποινική Δικαιοσύνη

ΠοινΧρ=Ποινικά Χρονικά

ΠΚ= Ποινικός Κώδικας

ΠοινΤμ= Ποινικό Τμήμα

ΣΕΒ= Σύνδεσμος επιχειρήσεων και βιομηχανιών

Σελ.= σελίδα

ΣΛΕΕ=Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης

Στοιχ. =στοιχείο

Σχ. =σχετικά

ΤΝΠ= Τράπεζα Νομικών Πληροφοριών

ΤΠΕ= Τεχνολογίες Πληροφορίας και Επικοινωνιών

ΦΕΚ= Φύλλο Εφημερίδας της Κυβέρνησης

Χ.χ.=χωρίς χρονολογία

CSIRT=Computer Security Incident Response Team

ENIISA= The European Union Agency for Cybersecurity

IoT=Internet of Things

N.d.= not dated

NIS= Directive on security of network and information systems

PIN= Personal Identified Number

RAM=Random access memory

SIM= Subscriber Identity Module

USB= Universal Serial Bus

ΕΙΣΑΓΩΓΗ

Οι τεχνολογίες δικτύων και πληροφοριών και ιδιαίτερα το διαδίκτυο, έχουν εισχωρήσει σχεδόν σε κάθε τομέα του κοινωνικού, προσωπικού και επαγγελματικού βίου. Η επίδρασή τους είναι τόσο καταλυτική που σε αρκετές περιπτώσεις μπορεί να γίνει λόγος για πραγματική εξάρτηση από αυτές και αντικειμενική αδυναμία λειτουργίας χωρίς την ύπαρξή τους.

Ειδικότερα όσον αφορά το διαδίκτυο, η αλματώδης εξέλιξή του και η ευρύτητα των εφαρμογών και λειτουργιών τους το έχουν καταστήσει απαραίτητο εργαλείο σε ένα μεγάλο φάσμα δραστηριοτήτων που σχετίζονται με την οικονομία, το εμπόριο, τις επιχειρήσεις και τους δημόσιους και ιδιωτικούς οργανισμούς.

Το διαδίκτυο, ωστόσο, χρησιμοποιείται ευρέως και επί καθημερινής βάσης και από τους πολίτες, είτε για ψυχαγωγικούς λόγους, είτε για ενημέρωση και εκπαίδευση, είτε για τραπεζικές συναλλαγές είτε τέλος για αλληλεπίδραση και επικοινωνία με άλλους χρήστες.

Η αλήθεια είναι, όμως, ότι όσο διευρύνονται οι υπηρεσίες που παρέχει το διαδίκτυο, τόσο μεγαλώνουν και οι κίνδυνοι που συνδέονται με την ασφαλή χρήση του. Κακόβουλο λογισμικό, διαδικτυακές απάτες, διακίνηση υλικού παιδικής πορνογραφίας, κυβερνοέγκλημα, υφαρπαγή προσωπικών δεδομένων προσώπων και οντοτήτων, είναι μερικοί μόνο από τους παράγοντες κινδύνου που ελλοχεύουν στο διαδίκτυο. Η προστασία των χρηστών και κατ' επέκταση του ίδιου του κυβερνοχώρου από τέτοιου είδους απειλές είναι αρμοδιότητα των πάροχων υπηρεσιών στον τομέα των δικτύων και πληροφοριών, οι οποίοι οφείλουν να εφαρμόζουν συστήματα Κυβερνοασφάλειας και να συμμορφώνονται με τους κανόνες ασφάλειας που αυτή θέτει.

Πλέον, η Κυβερνοασφάλεια αποτελεί πρώτη προτεραιότητα των αρμόδιων εθνικών και ευρωπαϊκών αρχών. Αυτό αποδεικνύεται και από τη σύσταση της Εθνικής Αρχής Κυβερνοασφάλειας στην Ελλάδα και του ENISA στην Ευρωπαϊκή Ένωση, έργο των οποίων αποτελεί ο σχεδιασμός και η εφαρμογή των αντίστοιχων στρατηγικών Κυβερνοασφάλειας. Επίσης, η θέσπιση

κανονιστικού πλαισίου στην Ελλάδα και ΕΕ για την Κυβερνοασφάλεια, καθώς και η συνεργασία και οι συντονισμένες ενέργειες όλων των εμπλεκόμενων μερών, παρέχουν εγγυήσεις για απρόσκοπτη, ομαλή λειτουργία του κυβερνοχώρου, ενώ παράλληλα διασφαλίζουν την προστασία των χρηστών απέναντι σε κυβερνοεπιθέσεις και παραβίαση των προσωπικών τους δεδομένων.

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

1.1 Τι είναι η Κυβερνοασφάλεια και ποιο το αντικείμενό της

Ο ρόλος των συστημάτων δικτύου και πληροφοριών είναι ιδιαίτερα σημαντικός για την κοινωνία. Αποφασιστικής σημασίας αποτελεί η ασφάλειά τους και η αξιοπιστία στη λειτουργία τους, για τη διεκπεραίωση των οικονομικών και κοινωνικών συναλλαγών. Ωστόσο, μεγάλη απειλή συνιστούν οι εσκεμμένες βλαβερές ενέργειες που έχουν στόχο να επιφέρουν βλάβες ή να διακόψουν τη λειτουργία αυτών των συστημάτων, προκαλώντας μεγάλες ζημίες στις οικονομικές δραστηριότητες και αβεβαιότητα στους χρήστες[1].

Η Κυβερνοασφάλεια, ήτοι η προστασία των συστημάτων δικτύου και των υπολογιστών καθώς και των δεδομένων από περιστατικά κυβερνοεπιθέσεων, είναι πρώτιστη προτεραιότητα για πολλές χώρες που έχουν συνειδητοποιήσει τη σημασία και το στόχο της. Προς επίτευξη αυτού του σκοπού, δημιουργήθηκαν και εξελίχθηκαν στρατηγικές Κυβερνοασφάλειας για την προστασία από τις απειλές κατά της ασφάλειας και την εξασφάλιση της ευημερίας σε κοινωνικό και οικονομικό επίπεδο. Οι στρατηγικές αυτές αποβλέπουν στην προώθηση και ενδυνάμωση της κυβερνητικής συνεργασίας και στην κατανομή αρμοδιοτήτων σχετικά με την καταπολέμηση του εγκλήματος στο διαδίκτυο, καθώς και στη σύμπραξη του δημόσιου και του ιδιωτικού τομέα, κυρίως παρόχων διαδικτυακών υπηρεσιών, αλλά και στη συνεργασία σε διεθνές φάσμα[2].

Ειδικότερα, όσον αφορά τον όρο της Κυβερνοασφάλειας αυτός περιλαμβάνει κάθε διασφάλιση και μέτρο που λαμβάνεται για την προστασία των πληροφοριακών συστημάτων και των χρηστών τους έναντι μη

---

[1] Βλ. Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 5ης Ιουλίου 2016 *σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου κα πληροφοριών σε ολόκληρη την Ένωση* ΕΕ L 194/1, 19.7.2016 [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016L1148 Πρόσβαση στις 7-11-2021

[2] Βλ. Ι. Ιγγλεζάκη (2021), *Δίκαιο Πληροφορικής*, Δ' Έκδοση, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη, σελ. 449

αδειοδοτημένης προσέγγισης, επιθέσεων και βλάβης, έτσι ώστε να διασφαλίζεται ότι τηρείται η «εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα» των δεδομένων[3].

Με την Κυβερνοασφάλεια προλαμβάνονται και εντοπίζονται συμβάντα που σχετίζονται με την ασφάλεια, ενώ προβλέπει τρόπους αντίδρασης έναντι αυτών καθώς και την πορεία ανάκαμψης έπειτα ένα τέτοιο περιστατικό. Στα συμβάντα αυτά, τα οποία ενδέχεται να είναι είτε σκόπιμα είτε όχι, συγκαταλέγονται, ενδεικτικώς αναφερόμενα, η τυχαία διάδοση πληροφοριών, οι επιθέσεις εναντίον επιχειρήσεων και σημαντικών οργανώσεων, η κλοπή προσωπικών δεδομένων, ή ακόμη και η παρεμβολή σε διαδικασίες δημοκρατικού χαρακτήρα. Τα αποτελέσματα αυτών των συμβάντων μπορούν να βλάψουν με ποικίλους τρόπους πρόσωπα, φορείς και κοινότητες[4].

Στο πολιτικό περιβάλλον της Ευρωπαϊκής Ένωσης, η χρήση του όρου της Κυβερνοασφάλειας δε συνδέεται μόνο με την ασφάλεια των συστημάτων δικτύου και πληροφοριών, αλλά καλύπτει και κάθε παράνομη ενέργεια που συντελείται μέσω της ψηφιακής τεχνολογίας στο χώρο του διαδικτύου. Συνεπώς, στην Κυβερνοασφάλεια μπορεί να εμπίπτουν κυβερνοεγκλήματα όπως η μόλυνση των υπολογιστών με ιούς ή η απάτη στα μέσα χρηματικών καταβολών, εκτός από τις πληρωμές με μετρητά και να έχουν στόχο όχι μόνο τα συστήματα αλλά και το περιεχόμενο, όπως και η διάδοση υλικού σεξουαλικού περιεχομένου ανηλίκων στο διαδίκτυο. Ακόμη, αντικείμενό της μπορεί να είναι ενέργειες παραπληροφόρησης για τη χειραγώγηση στο διάλογο μέσω διαδικτύου και εικασίες για παρεμβολές στις εκλογικές διαδικασίες[5].

---

[3] Βλ. Ευρωπαϊκό Ελεγκτικό Συνέδριο (2019) *Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια*. Λουξεμβούργο: Ευρωπαϊκό Ελεγκτικό Συνέδριο σελ. 8 [Διαδίκτυο] Διαθέσιμο στο: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EL.pdf Πρόσβαση στις 7-11-2021

[4] Βλ. Ευρωπαϊκό Ελεγκτικό Συνέδριο (2019) *Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια*. σελ. 8

[5] Βλ. Ευρωπαϊκό Ελεγκτικό Συνέδριο (2019) *Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια*. σελ. 8

1.2. Η κυβερνοασφάλεια και πως διακρίνεται από την ασφάλεια πληροφοριών και τις τεχνολογίες πληροφοριών

Στόχος της ασφάλειας των πληροφοριών είναι η διαφύλαξη των πληροφοριών και των πόρων ενός συστήματος πληροφοριών ευρύτερα, από ενδεχόμενες βλάβες που μπορεί να μειώσουν την αξία τους Επιπλέον, στοχεύει στη χορήγηση φερέγγυων πληροφοριών, στις οποίες οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση, όποτε είναι απαραίτητο [6].

Από πρακτικής πλευράς, η ασφάλεια πληροφοριών μπορεί να θεωρηθεί ως μια διαδικασία που χαρακτηρίζεται από τρία στάδια:

- Την πρόληψη στο πλαίσιο της οποίας λαμβάνονται μέτρα για την αποτροπή συνεπειών από ανεπιθύμητες ενέργειες
- Την ανίχνευση στο πλαίσιο της οποίας εντοπίζονται ενέργειες και διερευνούνται συμβάντα και πρόσωπα που ήταν υπαίτιοι αυτών των ενεργειών, όπως και συνέπειες αυτών των ενεργειών
- Την αντίδραση στο πλαίσιο της οποίας αποκαθίστανται οι πόροι που επλήγησαν και αντιμετωπίζονται οι υπό εξέλιξη επιθέσεις[7].

Όσον αφορά τις Τεχνολογίες Πληροφορίας και Επικοινωνιών αυτές αποσκοπούν:

α) «Προστασία Υπολογιστικών Συστημάτων (*Computer Security*): Διαφύλαξη υπολογιστικών πόρων συστήματος από μη εξουσιοδοτημένη χρήση και προστασία δεδομένων από ακούσια ή σκόπιμη αποκάλυψη ή τροποποίηση ή διαγραφή κατά την επεξεργασία και αποθήκευσή τους»

β) «Προστασία Επικοινωνιών (*Communication Security*): Διαφύλαξη δικτυακών πόρων και προστασία δεδομένων από ακούσια ή σκόπιμη αποκάλυψη ή τροποποίηση ή διαγραφή κατά τη μετάδοσή τους μέσω δικτύων υπολογιστών»[8].

Περαιτέρω η διαφύλαξη των πόρων και των δεδομένων στηρίζεται σε βασικά χαρακτηριστικά της Ασφάλειας Πληροφοριών, όπως:

---

[6] Βλ. Ι. Μαυρίδης (2015) *Ασφάλεια Πληροφοριών στο Διαδίκτυο*. Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών, σελ. 16

[7] Βλ. Ι. Μαυρίδη (2015) *Ασφάλεια Πληροφοριών στο Διαδίκτυο*. σελ. 16

[8] Βλ. Ι. Μαυρίδη *(2015) Ασφάλεια Πληροφοριών στο Διαδίκτυο.* σελ. 17

i) «Εμπιστευτικότητα»: σχετίζεται με τη διαφύλαξη της πληροφορίας από αποκάλυψή της για την οποία δεν έχει δοθεί σχετική εξουσιοδότηση

ii) «Ακεραιότητα»: σχετίζεται με τη διαφύλαξη της πληροφορίας από πιθανή αλλαγή , μεταβολή ή διαγραφή της, χωρίς προηγούμενη εξουσιοδότηση για αυτό το λόγο

iii) «Διαθεσιμότητα»: σχετίζεται με την προστασία της εξουσιοδοτημένης πρόσβασης, είτε για να γίνει κοινολόγηση είτε τροποποίηση, στην πληροφορία, χωρίς καθυστερήσεις ή κωλύματα[9].

Επιπρόσθετα, εκτός από τα ανωτέρω χαρακτηριστικά, η ασφάλεια στις ΤΠΕ συνδέεται με τη λειτουργία ορισμένων μηχανισμών που εφαρμόζονται με επιτυχία. Ειδικότερα, εφαρμόζεται ο μηχανισμός της «αναγνώρισης» που έχει ως αντικείμενο τη διαδικασία ταυτοποίησης ενός προσώπου ενώπιον του συστήματος, της «αυθεντικοποίησης» που έχει σχέση με την επαλήθευση των στοιχείων ενός προσώπου, τα οποία δηλώσει στο σύστημα ένα πρόσωπο. Ακολουθεί ο μηχανισμός της «εξουσιοδότησης» που αναφέρεται στη λήψη απόφασης σχετικά με τον εάν θα γίνει δεκτό ή θα απορριφθεί η αίτηση για πρόσβαση στο σύστημα ενός προσώπου του οποίου έχει γίνει αυθεντικοποίηση, στη βάση των δικαιωμάτων πρόσβασης τα οποία έχουν παραχωρηθεί ήδη και τη διαδικασία ως προς τον έλεγχο που αφορά την πρόσβαση στο σύστημα και τέλος, ο μηχανισμός της «αδυναμίας αποποίησης» η οποία σχετίζεται με τον πέραν πάσης αμφιβολίας καταλογισμό ευθύνης για την εκτέλεση μιας ενέργειας στο σύστημα[10].

1.3. Η σημασία της κυβερνοασφάλειας

Ο ρόλος της κυβερνοασφάλειας είναι σημαντικός διότι προστατεύει όλων των ειδών τα δεδομένα από κλοπή και βλάβη. Σε αυτά τα δεδομένα ανήκουν προσωπικές αναγνωρίσιμες πληροφορίες, οι προστατευόμενες πληροφορίες που

[9] Βλ. Ι. Μαυρίδη *(2015) Ασφάλεια Πληροφοριών στο Διαδίκτυο* σελ. 17-18

[10] Βλ. Ι. Μαυρίδη (2015) *Ασφάλεια Πληροφοριών στο Διαδίκτυο* σελ. 18

συνδέονται με την υγεία, οι προσωπικές πληροφορίες, τα δεδομένα που αφορούν την πνευματική ιδιοκτησία και τα δεδομένα που περιέχονται σε κυβερνητικά και βιομηχανικά πληροφοριακά συστήματα[11].

Χωρίς τη λειτουργία ενός συστήματος Κυβερνοασφάλειας οι οργανισμοί γίνονται ευάλωτοι απέναντι σε εκστρατείες διαρροών δεδομένων και συγχρόνως αποτελούν εύκολο στόχο για τους κυβερνοεγκληματίες. Τα λογισμικά προστασίας και τα τείχη προστασίας από ιούς δεν μπορούν να χρησιμοποιούνται πλέον ως οι μοναδικές λύσεις ασφάλειας, δεδομένου ότι οι εγκληματίες του διαδικτύου έχουν βελτιώσει τις πρακτικές τους, καθιστώντας αυτές πιο ανθεκτικές έναντι των παραδοσιακών συστημάτων προστασίας[12].

Είναι γεγονός ότι, ανεξάρτητα από το μέγεθος μιας επιχείρησης, αν είναι δηλαδή μικρή ή μεγάλη, όλες χρησιμοποιούν τα συστήματα των υπολογιστών σε καθημερινή βάση που σε συνδυασμό με τη χαμηλής ποιότητας υπηρεσία προστασίας τύπου "*cloud*", τα έξυπνα κινητά και το "*Internet of Things (IoT)*" έχουν προκαλέσει πολλά προβλήματα, ανύπαρκτα πριν από μερικά χρόνια, στο ζήτημα της ασφάλειας[13].

Μάλιστα, τα κυβερνοεγκλήματα έχουν προκαλέσει την προσοχή των αξιωματούχων των κυβερνήσεων σε ολόκληρο τον κόσμο. Η θέσπιση και η εφαρμογή του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων είναι ένα θετικό μέτρο για την αντιμετώπιση των εγκλημάτων στον κυβερνοχώρο, διότι με την αύξηση των συνεπειών από τις παραβιάσεις δεδομένων εξαναγκάζει τους οργανισμούς που το πεδίο δραστηριοτήτων τους βρίσκεται στο εντός του χώρου της ΕΕ:

- Να κάνουν γνωστές μεταξύ τους τις παραβιάσεις δεδομένων
- Να ορίσουν έναν υπεύθυνο για την προστασία των δεδομένων
- Να καθίσταται αναγκαία η συναίνεση του χρήστη για την επεξεργασία των πληροφοριών

[11] Βλ. A.T. Tunggal (2021) 'Why is Cybersecurity Important'?*UpGuard* [Διαδίκτυο] Διαθέσιμο στο: https://www.upguard.com/blog/cybersecurity-important Πρόσβαση στις 10-11-2021
[12] Βλ. A. T. Tungga (2021), *'Why is Cybersecurity Important'?...*
[13] Βλ. A. T. Tunggal (2021) '*Why is Cybersecurity Important?'...*

- Να προβαίνουν σε «ανωνυμοποίηση» των δεδομένων για τη διαφύλαξη της «ιδιωτικότητας».

1.4 Οι κυβερνοεπιθέσεις και οι κυβερνοαπειλές στον Κυβερνοχώρο

Με τον όρο κυβερνοαπειλή περιγράφεται κάθε κακόβουλη ενέργεια που έχει στόχο τη ζημία ή την κλοπή δεδομένων ή τη διατάραξη της ψηφιακής ασφάλειας γενικότερα. Μια κυβερνοαπειλή μπορεί να περιλαμβάνει επίθεση με ιούς σε υπολογιστές, παραβιάσεις δεδομένων, επιθέσεις που αφορούν την άρνηση υπηρεσιών και άλλες μορφές επίθεσης[14].

Επίσης, μια κυβερνοαπειλή μπορεί να αφορά μια κυβερνοεπίθεση που έχει στόχο την πρόσβαση άνευ προηγούμενης εξουσιοδότησης σε δεδομένα, τη βλάβη, τη διατάραξη ή την κλοπή πληροφοριών που αφορούν τεχνολογικά στοιχεία, λογισμικό υπολογιστών, πνευματική ιδιοκτησία ή οποιασδήποτε μορφής ευαίσθητων δεδομένων. Μάλιστα, μια κυβερνοαπειλή μπορεί να πραγματοποιείται εκ των έσω, από χρήστες δηλαδή που ενεργούν από το χώρο ενός οργανισμού, ή από άγνωστους χρήστες που ενεργούν από απομακρυσμένους προορισμούς[15].

Οι κυβερνοεπιθέσεις μπορεί να εκπορεύονται από διάφορους παράγοντες. Πιο αναλυτικά, οι κυβερνοεπιθέσεις μπορεί να προέρχονται από εχθρικά κράτη, τα οποία συνιστούν το μεγαλύτερο κίνδυνο, εξαιτίας της ικανότητάς τους να χρησιμοποιούν με αρκετά αποτελεσματικό τρόπο τα μέσα της τεχνολογίας εναντίον στόχων ιδιαίτερης δυσκολίας, όπως απόρρητα δίκτυα, δομές ζωτικής σημασίας, δίκτυα ηλεκτρικής ενέργειας και βαλδίδες ελέγχου αερίου[16].

Ακόμη, τρομοκρατικές ομάδες εξαπολύουν κυβερνοεπιθέσεις εναντίον κρατικών συμφερόντων, οι οποίες θα ενταθούν καθώς αυτές οι ομάδες ενισχύονται με πιο

[14] Βλ. A. T. Tunggal (2021) '*What is a Cyber Threat'?UpGuard* [Διαδίκτυο] Διαθέσιμο στο: https://www.upguard.com/blog/cyber-threat Πρόσβαση στις 10-12-2021
[15] Βλ. A. T. Tunggal (2021) ' *What is a Cyber Threat?'...*
[16] Βλ. A. T. Tunggal)2021) *'What is a Cyber Threat?'...*

καταρτισμένα τεχνολογικά άτομα. Ιδιαίτερη μορφή κυβεερνοεπιθέσεων είναι εκείνες που πραγματοποιούνται από εταιρικούς κατασκόπους και οργανωμένες εγκληματικές οργανώσεις μέσω της βιομηχανικής κατασκοπείας, προκειμένου να καρπωθούν εμπορικά μυστικά ή να διεξάγουν νομισματική κλοπή σε μεγάλη κλίμακα[17].

Επίσης, οι κυβερνοεπιθέσεις από ακτιβιστές αποβλέπουν κυρίως στη διάδοση προπαγανδιστικών ιδεών και όχι στη ζημία δομών ή διατάραξη υπηρεσιών, ενώ ένα πολύ συχνό φαινόμενο είναι οι κυβερνοεπιθέσεις από δυσαρεστημένους χρήστες, οι οποίοι γνωστοποιούν ευαίσθητα δεδομένα ίσως επειδή έχουν εξουσιοδοτημένη πρόσβαση σε αυτά. Περαιτέρω, οι κυβερνοεπιθέσεις μπορεί να προέρχονται από κακόβουλους χάκερς, οι οποίοι εκμεταλλευόμενοι ελαττώματα και ευπάθειες των συστημάτων αποκτούν πρόσβαση σε δεδομένα, χωρίς προηγούμενη εξουσιοδότηση. Θεωρούν την εισβολή τους στα συστήματα πληροφοριών ως ένα είδος πρόκλησης ή απλά καυχώνται για το κατόρθωμά τους. Μάλιστα, αν και παλιότερα τέτοιου τύπου επιθέσεις απαιτούσαν υψηλό επίπεδο επιδεξιότητας, σήμερα το διαδίκτυο περιέχει αυτοματοποιημένα σενάρια επιθέσεων και διάφορα πρωτόκολλα που κάνουν πολύπλοκες επιθέσεις να φαίνονται απλές[18].

Οι κυβερνοεπιθέσεις, ωστόσο, δεν οφείλονται πάντα σε ανθρώπινη ενέργεια, αλλά και σε φυσικές καταστροφές, διότι αυτές μπορούν να προκαλέσουν αναστάτωση στις βασικές δομές, όπως ακριβώς συμβαίνει και με μια κυβερνοεπίθεση. Τέλος, μια μορφή κυβερνοεπίθεσης αποτελούν οι τυχαίες πράξεις εξουσιοδοτημένων χρηστών, οι οποίοι ξεχνούν να ρυθμίσουν σωστά τα συστήματα ασφαλείας, με συνέπεια πιθανές διαρροές δεδομένων. Πράγματι, κάποιες από τις μεγαλύτερες διαρροές δεδομένων ήταν περισσότερο αποτέλεσμα ανεπαρκούς ρύθμισης, και όχι επίθεση από χάκερ ή δυσαρεστημένους χρήστες[19].

[17] Βλ. A. T. Tunggal (2021) 'What is a Cyber Threat?'...
[18] Βλ. A. T. Tunggal (2021) '*What is a Cyber Threat?'...*
[19] Βλ. A. T. Tunggal (2021) '*What is a Cyber Threat?'...*

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ

Ο ΗΛΕΚΤΡΟΝΙΚΟΣ ΥΠΟΛΟΓΙΣΤΗΣ ΚΑΙ Η ΤΕΛΕΣΗ ΕΓΚΛΗΜΑΤΩΝ

Κατηγορίες εγκλημάτων με χρήση ηλεκτρονικού υπολογιστή

Τα άλματα που σημειώθηκαν τις τελευταίες δεκαετίες στο χώρο της τεχνολογίας, είχαν ως αποτέλεσμα την εμφάνιση της ηλεκτρονικής εγκληματικότητας, η οποία δημιουργεί νέους προβληματισμούς στο πεδίο του ποινικού δικαίου. Σε πρώτο στάδιο, η αντιμετώπιση αυτών των προβλημάτων έγινε με το ν. 1805/1998[20], ο οποίος εισήγαγε νέα άρθρα στον ΠΚ[21], προκειμένου να αντιμετωπιστούν οι μορφές εγκλημάτων που σχετίζονται με τους ηλεκτρονικούς υπολογιστές και την πληροφορική[22].

Η εμφάνιση και η καθιέρωση του Διαδικτύου ως ενός νέου μέσου επικοινωνίας παγκόσμιας αποδοχής και απήχησης οδήγησε στην ανάδυση νέων προκλήσεων, καθώς αναδείχθηκαν νέοι τύποι εγκλημάτων που συνδέονται με αυτό. Γι' αυτό το λόγο η νομοθεσία σε ευρωπαϊκό και εθνικό επίπεδο εναρμονίστηκε με τα νέα δεδομένα, θεσπίζοντας σχετικές διατάξεις για την κύρωση των εγκλημάτων που τελούνται μέσω του Διαδικτύου[23]

Σημαντικό βήμα προς αυτή την κατεύθυνση αποτελεί η Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα[24], ενώ ιδιαίτερη μνεία πρέπει να γίνει στη Σύμβαση για το Έγκλημα στον «Κυβερνοχώρο» που υπογράφηκε

---

[20] Βλ. Νόμος 1805/1988 - ΦΕΚ 199/Α/31-8-1988, *Εκσυγχρονισμός τον θεσμού τον ποινικού μητρώου, τροποποίηση ποινικών διατάξεων και ρύθμιση άλλων σχετικών θεμάτων*. [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-dikasteria-dikaiosune/n-1805-1988.html Πρόσβαση 11-12-2021

[21] Προστέθηκε εδάφιο στην περίπτωση γ' το άρθρου 13, το άρθρο 370Β, 370Γ και 386Α.

[22] Βλ. Ι. Ιγγλεζάκη (2021)*Δίκαιο Πληροφορικής*... σελ.399

[23] Βλ. Ι. Ιγγλεζάκη (2021 *Δίκαιο Πληροφορικής*... σελ.399

[24] Βλ. Οδηγία 2010/0273 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου *για τις επιθέσεις κατά των συστημάτων πληροφοριών και την κατάργηση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου {SEC(2010)1122 final}{SEC(2010)1123 final}*, αιτιολογική έκθεση [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52010PC0517&from=EN Πρόσβαση στις 14-11-2021·Βλ. Ι. Αγγελής(2001) *Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο*, ΠοινΔικ σελ. 1218 επ.

στη Βουδαπέστη στις 23 Νοεμβρίου 2001[25]. Η εν λόγω Σύμβαση, γνωστή και ως Σύμβαση της Βουδαπέστης, στοχεύει στην ευθυγράμμιση των εσωτερικών διατάξεων του ουσιαστικού ποινικού δικαίου για τα αδικήματα που τελούνται στον κυβερνοχώρο, συγχρόνως, δε, περιλαμβάνει διατάξεις του δικονομικού ποινικού δικαίου που προβλέπονται ως αναγκαίες προκειμένου να διερευνηθούν και να τιμωρηθούν τέτοιας μορφής αδικήματα καθώς και αδικήματα που τελούνται με ηλεκτρονικό υπολογιστή, ενώ επίσης, δημιουργεί τις προϋποθέσεις για αποτελεσματική συνεργασία σε διεθνές επίπεδο[26] [27].

Τα αδικήματα που περιλαμβάνονται στη Σύμβαση καλύπτουν τέσσερις κατηγορίες και τα συμβαλλόμενα κράτη μέλη πρέπει να θεσμοθετήσουν τα σωστά μέτρα[28]. Πιο αναλυτικά, στην πρώτη κατηγορία, η οποία περιλαμβάνει τα αδικήματα σχετικά με την «εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα», ανήκουν τα κάτωθι εγκλήματα:

α) Η παράνομη πρόσβαση *(illegal access)*, δηλαδή η πρόσβαση που γίνεται σκόπιμα και άνευ δικαιώματος, συνολικά ή σε τμήμα ενός συστήματος υπολογιστή, η οποία πιθανόν να πραγματοποιείται παραβιάζοντας τα μέτρα ασφαλείας και αποσκοπεί στο να αποκτηθούν δεδομένα ηλεκτρονικού υπολογιστή, ή σε άλλο κακοπροαίρετο σκοπό[29]

β) η παράνομη υφαρπαγή δεδομένων(*illegal interception*) , δηλαδή η σκόπιμη και άνευ δικαιώματος υφαρπαγή «με τεχνικά μέσα μη δημόσιας διαβίβασης»

---

[25]Βλ. Εφημερίδα της Κυβερνήσεως (2016). *Convention on Cybercrime* [Διαδίκτυο] Διαθέσιμο στο: https://www.lawspot.gr/sites/default/files/annex_files/other/sumvasi_voudapestis_eng_fr.pdf Πρόσβαση στις 14-11-2021

[26] Βλ.Council of Europe (2001) *Explanatory Report to the Convention on Cybercrime*. Budapest: Council of Europe σελ. 3, [Διαδίκτυο] Διαθέσιμο στο: https://rm.coe.int/16800cce5b Πρόσβαση στις 10-12-2021

[27] Βλ. Council of Europe Portal Treaty Office (2021) *Chart of signatures and ratifications of Treaty 189, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)* Strasbourg: . Council of Europe Portal Treaty Office, όπου τη συγκεκριμένη Σύμβαση υιοθέτησαν και χώρες εκτός του Συμβουλίου της Ευρώπης, μεταξύ των οποίων η Αυστραλία, η Βραζιλία, το Ισραήλ, ο Καναδάς, η Ιαπωνία και οι Ηνωμένες Πολιτείες Αμερικής. [Διαδίκτυο] Διαθέσιμο στο: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=189 Πρόσβαση στις 10-12-2021

[28] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής*... σελ.400

[29] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής*... σελ.400-401

δεδομένων ηλεκτρονικού υπολογιστή, είτε προς σύστημα ηλεκτρονικού υπολογιστή, είτε από, είτε μέσα στο σύστημα ηλεκτρονικού υπολογιστή[30]

γ) η παρέμβαση σε δεδομένα (*data interference),* δηλαδή η εσκεμμένη και άνευ δικαιώματος καταστροφή, διαγραφή, παραποίηση, παραλλαγή ή αποσιώπηση δεδομένων

δ) η παρέμβαση σε σύστημα (*system intereference*), δηλαδή η σκόπιμη και άνευ δικαιώματος[31] παρακώλυση της λειτουργίας ενός συστήματος ηλεκτρονικού υπολογιστή, με την εισαγωγή, μεταφορά, καταστροφή, διαγραφή, νόθευση, αλλαγή ή αποσιώπηση δεδομένων ηλεκτρονικού υπολογιστή[32]

ε) κακή μεταχείριση συσκευών (*misuse of devices*), δηλαδή η σκόπιμη και άνευ δικαιώματος παραγωγή, πώληση, διανομή και άλλων ενεργειών συσκευής ηλεκτρονικού υπολογιστή ή κωδικών του ίδιου του ηλεκτρονικού υπολογιστή, ή κωδικών πρόσβασης ή σχετικών δεδομένων, με στόχο την τέλεση των εγκλημάτων που έχουν αναφερθεί ανωτέρω[33].

Στη δεύτερη κατηγορία εγκλημάτων περιλαμβάνονται αυτά που σχετίζονται με ηλεκτρονικούς υπολογιστές και πιο συγκεκριμένα:

α) η *πλαστογραφία αναφορικά με ηλεκτρονικό υπολογιστή (computer related forgery),* δηλαδή η σκόπιμη και άνευ δικαιώματος εισαγωγή, τροποποίηση, διαγραφή ή αποσιώπηση δεδομένων ηλεκτρονικού υπολογιστή, με συνέπεια μη ακριβή δεδομένα να εκλαμβάνονται ως γνήσια[34]

β) η απάτη με ηλεκτρονικό υπολογιστή (*computer related fraud),* δηλαδή η σκόπιμη και άνευ δικαιώματος ζημία στην περιουσία άλλου με στόχο να επωφεληθεί οικονομικά άλλο πρόσωπο, με την εισαγωγή, τροποποίηση, διαγραφή ή αποσιώπηση δεδομένων, ή η επέμβαση στο λειτουργικό σύστημα ενός ηλεκτρονικού υπολογιστή[35].

Στην επόμενη κατηγορία περιλαμβάνονται τα αδικήματα που έχουν σχέση με το περιεχόμενο του ηλεκτρονικού υπολογιστή. Σε αυτή την κατηγορία εμπίπτει το

---

[30] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής...* σελ. 401
[31] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής...* σελ. 401
[32] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής...* σελ. 401
[33] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής...* σελ. 401
[34] Βλ. Ι. Ιγγλεζάκη *(2021) Δίκαιο Πληροφορικής...* σελ. 401
[35] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής...* σελ. 401

αδίκημα της παιδικής πορνογραφίας, ενώ στην τελευταία κατηγορία εμπίπτουν τα αδικήματα που αφορούν τις παραβιάσεις δικαιωμάτων πνευματικής ιδιοκτησίας[36].

ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ
ΚΡΙΣΙΜΑ ΖΗΤΗΜΑΤΑ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

3.1 Κίνδυνοι και τάσεις της Κυβερνοασφάλειας

Η εξέλιξη στον ψηφιακό χώρο αποτελεί μια πραγματική επανάσταση, η οποία προσφέρει ευκαιρίες ανάπτυξης σε οργανισμούς και επιχειρήσεις, προσφέροντάς τους συγχρόνως αξία και προβάδισμα ανταγωνισμού. Για τη μελλοντική πρόοδο, ωστόσο, των οργανισμών σε ένα ψηφιακό περιβάλλον, είναι αναγκαίος ένας αποτελεσματικός σχεδιασμός κυβερνοασφάλειας που θα παρακινήσει τους οργανισμούς να γίνουν πιο ασφαλείς, προετοιμασμένοι και απρόσβλητοι απέναντι σε κυβερνοεπιθέσεις[37].

Περαιτέρω, οι οργανισμοί θα πρέπει να μπορούν να αντιλαμβάνονται τις ευκαιρίες και τους κινδύνους που συνδέονται με τον ψηφιακό καινοτόμο χώρο, να ισοσταθμίζουν την ανάγκη προάσπισής τους έναντι των υπαρκτών απειλών, καθώς και την ανάγκη να ενστερνίζονται νέου τύπου επιχειρηματικά πρότυπα και νέες πολιτικές που επωφελούνται από τις τεχνολογικές ψηφιακές εξελίξεις και θεμελιώνουν τους πυλώνες για ανάπτυξη[38]. Υπό αυτό το πρίσμα, είναι σημαντικό οι οργανισμοί να συνειδητοποιήσουν το είδος του κινδύνου τους, να εκτιμήσουν την κατάσταση που βρίσκονται τα συστήματα ασφαλείας και να

---

[36] Βλ. Ι. Ιγγλεζάκη *(2021) Δίκαιο Πληροφορικής...* σελ. 401

[37] Βλ. Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ (2020). *Κυβερνοασφάλεια*, σελ. 5, [Διαδίκτυο] Διαθέσιμο στο: https://www2.deloitte.com/content/dam/Deloitte/gr/Documents/risk/gr_SEV_Deloitte_Cybersecurity_noexp.pdf Πρόσβαση στις 20-12-2021

[38] Βλ. Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ (2020*). Κυβερνοασφάλεια* ...σελ. 5

σχεδιάσουν ένα πρόγραμμα για να ενισχύσουν την άμυνά τους απέναντι στους κινδύνους που εγκυμονεί ο Κυβερνοχώρος[39].

Η διαχειριστική αντιμετώπιση κινδύνων στον Κυβερνοχώρο είναι μια διαδικασία που βρίσκεται σε διαρκή ανάπτυξη και συνεχείς μεταβολές οι οποίες προσαρμόζονται ανάλογα στις εκάστοτε απειλές[40]. Για να είναι αποτελεσματική μια τέτοια διαδικασία, είναι απαραίτητο να δημιουργηθεί και να τεθεί σε εφαρμογή ένα πιστοποιημένο πλαίσιο που θα επιβάλλει και θα καθορίζει με σαφήνεια επιχειρηματικούς λόγους, οι οποίοι θα το υλοποιούν[41].

Ακολούθως, κατά την διαδικασία αξιολόγησης των κινδύνων, γίνεται αναγνώριση αυτών, ενώ παράλληλα προσδιορίζεται η πιθανότητα να προκύψει κίνδυνος, οι αρνητικές επιπτώσεις του και τα μέτρα ασφαλείας που θα πρέπει να εφαρμοστούν, ώστε να μειωθούν στο κατάλληλο επίπεδο τόσο ο κίνδυνος, αν αυτός προκύψει, όσο και οι αρνητικές επιπτώσεις του[42]. Όσον αφορά τη μέθοδο που ακολουθείται κατά τη διαδικασία αξιολόγησης των κινδύνων, αυτή περιλαμβάνει, καταρχήν, τον προσδιορισμό των πληροφοριών και το πόσο σημαντικό ρόλο έχουν για τον οργανισμό, ακόμη, τον προσδιορισμό των ελλείψεων στο σύστημα ασφαλείας και τις απειλές, τον υπολογισμό του κινδύνου και, τέλος, το σχεδιασμό δράσης για τον όσο το δυνατόν μεγαλύτερο περιορισμό των κινδύνων[43].

Η εξελικτική πορεία του περιβάλλοντος Κυβερνοασφάλειας τα δώδεκα προηγούμενα χρόνια αποδεικνύει ότι η προσέγγιση στο σύστημα Κυβερνοσασφάλειας πρέπει να είναι ολιστική, με το ζήτημα της πρόληψης να βρίσκεται στο επίκεντρο. Ειδικότερα, την περίοδο των ετών 2008-2012, η προσοχή επικεντρώθηκε στην Κυβερνοασφάλεια καθώς ισχυροποιήθηκαν τα πρώτα σημαντικά κανονιστικά μοντέλα που αποσκοπούν στον καθορισμό των

---

[39] Βλ. Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ (2020*). Κυβερνοασφάλεια*..σελ. 5

[40] Βλ. Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ (2020). Κυβερνοασφάλεια...σελ. 6

[41] Βλ. Ν. Ηλιόπουλο (2008), 'Περί κινδύνων ο λόγος... Διαχείριση και αντιμετώπισή τους', *it PROFESSIONAL security*, [Διαδίκτυο]Διαθέσιμο στο: https://www.itsecuritypro.gr/peri-kindynon-o-logos-diachirisi-ke-antimetopisi-tous-2/ Πρόσβαση στις 22-12-2021

[42] Βλ. Ν. Ηλιόπουλο (2008) 'Περί κινδύνων ο λόγος... Διαχείριση και αντιμετώπισή τους'...

[43] Βλ. Ν. Ηλιόπουλο (2008) 'Περί κινδύνων ο λόγος... Διαχείριση και αντιμετώπισή του'ς...

ελάχιστων απαιτήσεων αλλά και στο σωστό προσανατολισμό των οργανισμών αναφορικά με την ασφάλειά τους. Στη συνέχεια, την τετραετία 2012-2018, ήρθαν στο φως της δημοσιότητας τα πρώτα διεθνώς συμβάντα παραβίασης, εξαιτίας των οποίων η Κυβερνοασφάλεια προήχθη και σε πρόβλημα τεχνικό πλέον, εκτός από επιχειρησιακό, ενώ ιδιαίτερη σημασία δόθηκε στο διαχειριστικό πλαίσιο κινδύνων καθώς και στην αντοχή των οργανισμών. Από το 2018 και έκτοτε, οι καινοτόμες τεχνολογικές εφαρμογές, όπως η «ψηφιοποίηση, το υπολογιστικό νέφος, IoT, η τεχνητή νοημοσύνη», προκάλεσαν αβεβαιότητα στο χώρο της Κυβερνοασφάλειας, ενώ η στρατηγική μέχρι και το 2025 δίνει ιδιαίτερη βαρύτητα στη διαχείριση κινδύνων που βρίσκονται εκτός του χώρου ελέγχου των οργανισμών[44]

Κατά μια άποψη, ο ευρύτερος τεχνολογικός χώρος θα μπορούσε, να χαρακτηριστεί ως ένα « *πεδίο μάχης*», το μεγαλύτερο που υπήρξε ποτέ. Οι εγκληματίες που δρουν στον Κυβερνοχώρο, ανάλογα με τα κίνητρά τους, τα οποία δεν είναι μόνο οικονομικής φύσης, είναι διαφορετικοί και θέτουν σε εφαρμογή όλα τα μέσα για να πετύχουν τους στόχους τους, για τους οποίους εργάζονται προσεκτικά και με μεθοδικότητα. Επίσης, όσοι στοχοποιούν κακοπροαίρετα έναν οργανισμό, τον παρακολουθούν συνεχώς και επιδεικνύουν μεγάλη υπομονή, ώστε να ανακαλύψουν πιθανά μειονεκτήματα και να κάνουν την επίθεσή τους εγκαίρως. Απώτερος σκοπός τους είναι να εξασφαλίσουν μη εξουσιοδοτημένη πρόσβαση, μέσω της οποίας θα καταφέρουν να επιτύχουν τα κίνητρά τους, βλάπτοντας τη φήμη του οργανισμού[45]

Στους κινδύνους του Κυβερνοχώρου περιλαμβάνονται οι απειλές που προέρχονται από εσωτερικούς χρήστες, που ενεργούν είτε εκ προθέσεως είτε όχι, για λόγους εκδίκησης ή για την αποκόμιση οικονομικού οφέλους, με αποτέλεσμα να ζημιώνεται οικονομικά ο οργανισμός, να βλάπτεται η φήμη του και να διαρρέονται πληροφορίες. Ακόμη, στους κινδύνους που απειλούν τον Κυβερνοχώρο ανήκει το διεθνές οργανωμένο έγκλημα, το οποίο είναι δύσκολο να εντοπιστεί και το κίνητρό του είναι η απόκτηση προσωρινού οικονομικού

[44]Βλ. Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ (2020). *Κυβερνοασφάλεια*...σελ. 7
[45] Βλ. Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ (2020) *Κυβερνοασφάλεια,* ...σελ. 8

οφέλους. Πλήττει την οικονομική επιφάνεια και τη φήμη του οργανισμού, ενώ συνδέεται με διαρπαγή πληροφοριών[46]

Ακόμη, κίνδυνος θεωρείται και το κυβερνοέγκλημα που υποθάλπει το κράτος για λόγους κατασκοπείας, με κίνητρο οφέλη σε οικονομικό και πολιτικό επίπεδο. Οι επιπτώσεις αυτού του κινδύνου στον οργανισμό αφορούν την κλοπή πληροφοριών, την παύση λειτουργίας του και την οικονομική ζημία. Επίσης, η δράση των ανταγωνιστών που υποκινείται από την πρόθεση απόκτησης ανταγωνιστικού πλεονεκτήματος, πλήττει τη φήμη του οργανισμού, οδηγεί στη διαρροή εμπιστευτικών πληροφοριών και μειώνει την ανταγωνιστικότητά του. Έναν ακόμη κίνδυνο για τον Κυβερνοχώρο συνιστούν οι χάκερς που δρουν με σκοπό να κάνουν αισθητή την παρουσία τους στο χώρο ή να αυξήσουν τη δημοφιλία τους. Τα κίνητρά τους δεν είναι ξεκάθαρα, ενώ η δράση τους προκαλεί ζημία στην υπόληψη του οργανισμού, σταματά τη λειτουργία του και οδηγεί σε διαρροή πληροφοριών[47].

Σχετικά με τον προσδιορισμό της απειλής, αυτή αναφέρεται ως ένα σύνολο συμβάντων, τα οποία όταν εκδηλωθούν επηρεάζουν αρνητικά την ικανότητα του οργανισμού να ανταποκριθεί στους επιχειρηματικούς του στόχους[48]. Στις πιο σημαντικές κατηγορίες απειλών περιλαμβάνονται:

α) «Απώλεια εμπιστευτικότητας» των πληροφοριών κατά τη διακίνησή τους καθώς και εκείνων των πληροφοριών που σχετίζονται με δεδομένα προσωπικού χαρακτήρα πελατών ή συνεργατών

β) «Απώλεια ακεραιότητας» των πληροφορίων κατά τη διακίνησή τους, με πιθανή κατάληξη την άνευ προηγούμενης εξουσιοδότησης τροποποίησή τους[49]

---

[46] Βλ, Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ (2020) *Κυβερνοασφάλεια*...σελ. 8

[47] Βλ. Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ (2020) *Κυβερνοασφάλεια*,...σελ. 8

[48] Βλ. Ν. Ηλιόπουλο (2008) 'Διαχείριση Ασφάλειας Πληροφοριών: Η Σύγχρονη Επιχειρησιακή Αναγκαιότητα', *it PROFESSIONAL security*, [Διαδίκτυο]Διαθέσιμο στο: https://www.itsecuritypro.gr/diachirisi-asfalias-pliroforion-sygchroni-epichirisiaki-anagkeotita-2/ Πρόσβαση στις 22-12-2021

[49] Βλ. Ν. Ηλιόπουλο *(2008)* 'Διαχείριση Ασφάλειας Πληροφοριών: Η Σύγχρονη Επιχειρησιακή Αναγκαιότητα' , όπου η εν λόγω τροποποίηση μπορεί να αφορά για παράδειγμα χρηματικά ποσά ή αριθμό παραγγελιών, όπως και τους παραλήπτες ορισμένων πληρωμών.

γ) «Απώλεια διαθεσιμότητας» που οφείλεται σε κακή λειτουργία (εσκεμμένη ή μη) του δικτύου επικοινωνίας, ή σε συνειδητή ενέργεια, με στόχο την παύση παροχής αυτών των υπηρεσιών

δ) Εν νέου διεξαγωγή συναλλαγής που διενεργήθηκε με τη χρήση των ίδιων δεδομένων[50]

ε) Μη αποδεχόμενη συμμετοχή σε συναλλαγή ή διεξαγωγή αυτής από κάποια από τις συναλλασσόμενες πλευρές

στ) «Εξαπάτηση» του οργανισμού με τη μέθοδο της πλαστοπροσωπίας

ζ) «Απάτη» μέσω της χρησιμοποίησης για ίδιον όφελος των ελαττωμάτων στην ασφάλεια, με συνέπεια την εξαπάτηση συνεργατών ή πελατών από τρίτα πρόσωπα, ή την εξαπάτηση του οργανισμού από άτομα που ανήκουν στο περιβάλλον του[51].

Σε κάθε τομέα επιχειρηματικής δράσης υπάρχουν απειλές. Ωστόσο, για τη μη εμφάνισή τους σημαντικός παράγοντας αποτελεί η ύπαρξη και αποτελεσματικότητα των σωστών ασφαλιστικών δικλείδων, οι οποίες μειώνουν την πιθανή εμφάνιση αδυναμίας που θα οδηγήσει με τη σειρά της στην εμφάνιση της ανάλογης απειλής[52].

3. 2 Η χρήση βέλτιστων πρακτικών για την Κυβερνοασφάλεια

Ο προγραμματισμός και η εφαρμογή μιας ολιστικού τύπου στρατηγικής για την Κυβερνοασφάλεια είναι απαίτηση της σύγχρονης εποχής, προκειμένου να είναι αποτελεσματική η αντιμετώπιση των κινδύνων του Κυβερνοχώρου , μέσω της εφαρμογής κατάλληλων και τεχνολογικών μέτρων ασφαλείας[53].

---

[50] Βλ. Ν. Ηλιόπουλο (2008) 'Διαχείριση Ασφάλειας Πληροφοριών: Η Σύγχρονη Επιχειρησιακή Αναγκαιότητα', όπου αυτό σημαίνει ότι τα δεδομένα καταχωρούνται δύο φορές, το ίδιο και οι εγγραφές.

[51] Βλ. Ν. Ηλιόπουλο (2008) 'Διαχείριση Ασφάλειας Πληροφοριών: Η Σύγχρονη Επιχειρησιακή Αναγκαιότητα'...

[52] *Βλ. Ν. Ηλιόπουλο (2008)* 'Διαχείριση Ασφάλειας Πληροφοριών: Η Σύγχρονη Επιχειρησιακή Αναγκαιότητα'..

[53] Βλ. Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ (2020) *Κυβερνοασφάλεια* ...σελ. 20

Επιπρόσθετα, η προσέγγιση των οργανισμών θα πρέπει να λαμβάνει υπόψη τις επιχειρησιακές τους ανάγκες και τις απειλές που υφίστανται στο περιβάλλον λειτουργίας τους, με στόχο την αντιμετώπιση κινδύνων που συνδέονται με την Κυβερνοασφάλεια. Ακόμη, δεδομένης της μεγάλης σημασίας που έχουν για ένα οργανισμό οι λειτουργίες του και η προστασία των αγαθών του, καθίσταται αναγκαία η εφαρμογή των εννοιών της «προστασίας», της «επίγνωσης» και της «ανθεκτικότητας» απέναντι σε περιστατικά Κυβερνοεπιθέσεων[54'].

Η χρήση της ψηφιακής τεχνολογίας μπορεί να οδηγήσει σε βελτίωση της διαχείρισης των κινδύνων στον Κυβερνοχώρο, μέσω νέων εφικτών προοπτικών και δυνατοτήτων. Οι επενδυτικές κινήσεις σε ψηφιακές τεχνολογίες για την διαχειριστική αντιμετώπιση των κινδύνων που απειλούν την Κυβερνοασφάλεια μπορούν να οδηγήσουν σε υψηλότερα ποσοστά αποτελεσματικότητας και αποδοτικότητας, καθιερώνοντας νέους κανόνες, σύμφωνα με τους οποίους ορισμένοι κίνδυνοι θεωρούνται ξεπερασμένοι. Για τους οργανισμούς η ψηφιακή τεχνολογία μπορεί να αποτελέσει το μέσο για να αναβαθμιστούν οι πρακτικές αντιμετώπισης κινδύνων, να αυξήσουν την απόδοση των λειτουργιών τους και να προβούν πάλι σε επενδυτικές πρωτοβουλίες σχετικά με τον εκσυγχρονισμό της αντιμετώπισης του κινδύνου[55].

ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ
ΕΓΚΛΗΜΑΤΑ-ΠΡΟΚΛΗΣΕΙΣ ΠΟΥ ΑΝΤΙΜΕΤΩΠΙΖΕΙ Η ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

4.1 Η *απάτη* μέσω ηλεκτρονικού υπολογιστή

Σύμφωνα με το προϊσχύσαν δίκαιο, η πρόκληση περιουσιακής ζημίας σε τρίτο μέσω της χρήσης ηλεκτρονικού υπολογιστή δεν χαρακτηριζόταν ως απάτη,

[54] Βλ. Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ(2020) *Κυβερνοασφάλεια* ...σελ. 22
[55] Βλ. Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ (2020) Κυβερνοασφάλεια, ...σελ. 22

για το λόγο ότι η περιουσιακή ζημία που προκαλείται σε τρίτο με την παρέμβαση του δράστη σε σύστημα πληροφορικής δεν εμπίπτει στο άρθρο 386 ΠΚ[56] [57].

Όταν πρόκειται για απάτη με υπολογιστή, όπου ο δράστης εισάγει σε ένα σύστημα πληροφορικής ψεύτικα δεδομένα στα οποία εφαρμόζεται αυτοματοποιημένη επεξεργασία χωρίς ανθρώπινη επέμβαση, δεν θεμελιώνεται το έγκλημα της απάτης του άρθρου 86 ΠΚ, ενώ το ίδιο ισχύει και στην περίπτωση επέμβασης του δράστη στο υλικό ή στο λογισμικό ενός υπολογιστή, επηρεάζοντας την έκβαση που θα έχει η επεξεργασία της πληροφορίας, με επακόλουθο την επέλευση περιουσιακής ζημίας[58].

Το κενό στη νομοθεσία καλύφθηκε με την προσθήκη της διάταξης 386 Α ΠΚ[59] [60], η οποία λαμβάνει ως υπόδειγμα τη διάταξη του άρθρου 263a του γερμανικού Ποινικού Κώδικα, το οποίο αναφέρεται σε βλάβη της περιουσίας μέσω ηλεκτρονικού υπολογιστή, στην οποία δεν υφίσταται παραπλάνηση ανθρώπου, αλλά παρέμβαση όταν ο υπολογιστής βρίσκεται σε λειτουργία[61] [62].

---

[56] Βλ. Χ. Μυλωνόπουλο (1991) *Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο. Συμβολή στην ερμηνεία των άρθρων 13γ, 370Β, 370Γ και 386* Α Π.Κ. (άρθρ. 2-5 ν. 1805/88. σελ. 54·Ε. Βασιλάκη (1993) *Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών-Η αντιμετώπιση του προβλήματος μετά την εισαγωγή του ν. 1805/88*. σελ. 185

[57] Η συγκεκριμένη διάταξη κάνει λόγο για την πλάνη που προκαλείται σε φυσικό πρόσωπο, η οποία συμβαίνει όταν ο δράστης «προβαίνει στην εν γνώσει παράσταση ψευδών γεγονότων ως αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων».

[58] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής*...σελ. 405-406

[59] Βλ. Άρθρο 386 Α ΠΚ « Όποιος με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή: ... με τη χωρίς δικαίωμα παρέμβαση στη λειτουργία προγράμματος υπολογιστή... με τη χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων υπολογιστή.....με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση...τιμωρείται με φυλάκιση...» , Ν. 46/2019-ΦΕΚ 95/Α/11-6-2019- *Κύρωση του Ποινικού Κώδικα*, [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-kodikes-nomothesias/nomos-4619-2019-phek-95a-11-6-2019.html Πρόσβαση στις 27-12-2021

[60] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής*... σελ. 406, όπου για τη διάταξη του άρθρου 386 Α ΠΚ έχει χρησιμοποιηθεί η παράγραφος 263a του Γερμανικού Ποινικού Κώδικα. Για αυτό το λόγο, κατά την ερμηνεία της συγκεκριμένης διάταξης λαμβάνεται υπόψη η γερμανική θεωρία και νομολογία

[61] Βλ. Ε. Βασιλάκη (1993) *Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών...σελ. 201 επ.*· Χ. Μυλωνόπουλο (1991) *Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο*... σελ. 56·Α. Παπαδαμάκη (2020) *Τα περιουσιακά εγκλήματα*, 3η εκδ. 2020, σελ. 154

[62] Αρχικά, η διατύπωση της διάταξης ήταν η ακόλουθη: «Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη

Σκοπός του νομοθέτη ήταν να προστατεύσει τη περιουσία από προσβολές που πραγματοποιούνται μέσω της τεχνολογίας, η οποία, σε πολλές περιπτώσεις, υποκαθιστά τις ανθρώπινες ενέργειες[63].

Με το ν. 4411/2016[64] τροποποιήθηκε η διάταξη του άρθρου 386 Α ΠΚ, ώστε να συμπεριληφθεί σε αυτή και η περίπτωση χρήσης σωστών δεδομένων χωρίς δικαίωμα, όταν, για παράδειγμα ο δράστης αποκτά παράνομα το όνομα χρήστη και τον σχετικό κωδικό χρήσης[65]. Σύμφωνα με μια άποψη που έχει υποστηριχθεί, η ανωτέρω τροποποίηση επέτρεψε να θεωρείται ως απάτη που διενεργείται μέσω υπολογιστή, κάθε μεταφορά χρημάτων, η οποία πραγματοποιείται είτε με υποκλοπή και χρήση ξένων, ορθών ωστόσο, κωδικών, είτε με παράνομη εισαγωγή του δράστη στα πληροφοριακά συστήματα τραπεζικών οργανισμών ή χρηματιστηριακών εταιρειών[66].

Ως προς τη διατύπωσή της, η διάταξη του άρθρου 386 Α ΠΚ συμφωνεί με εκείνη του άρθρου 386 ΠΚ, ωστόσο, η διαφορά τους έγκειται στο ότι στο πραγματικό της πρώτης διάταξης δεν γίνεται αναφορά στην πράξη εξαπάτησης, αλλά σε συμπεριφορές που στοχεύουν στον «επηρεασμό» των στοιχείων του ηλεκτρονικού υπολογιστή, με αποτέλεσμα την εσφαλμένη επεξεργασία δεδομένων[67]. Επομένως, η απάτη με υπολογιστή δε συνιστά ειδικότερη μορφή απάτης, αλλά αποτελεί ιδιώνυμο έγκλημα όσον αφορά την απάτη[68].

περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση προγράμματος υπολογιστή είτε με επέμβαση κατά την εφαρμογή του είτε με τη χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων τιμωρείται...»

[63] Βλ. Α.Παπαδαμάκη (2020) *Τα περιουσιακά εγκλήματα...* σελ. 153

[64] Βλ. Ν. 4411/2016-ΦΕΚ 142/Α/3-8-2016: *Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών*, [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-nomothesia-genikou-endiapherontos/nomos-4411-2016.html Πρόσβαση στις 27-12-2021

[65] Βλ. Αιτιολογική έκθεση ν. 4411/2016, σελ. 6, [Διαδίκτυο] Διαθέσιμο στο: https://www.hellenicparliament.gr/UserFiles/2f026f42-950c-4efc-b950-340c4fb76a24/k-raxef-eis.pdf Πρόσβαση στις 27-12-2021

[66] Βλ. Ι. Μοροζίνη *Η μεταφορά χρημάτων με χρήση υπηρεσιών ηλεκτρονικής τραπεζικής ως ποινικώς κολάσιμη συμπεριφορά υπό το πρίσμα των εγκλημάτων κατά της ιδιοκτησίας και της περιουσίας, σε: Δαλακούρα*, σελ. 157 επ.

[67] Βλ. Χ. Μυλωνόπουλο (1991) *Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο Συμβολή στην ερμηνεία των άρθρων 13γ, 370Β, 370Γ και 386 Α Π.Κ. (άρθρ. 2-5 ν. 1805/88*, ελ. 56

[68] Βλ. Α.Παπαδαμάκη (2020) Τα περιουσιακά εγκλήματα, σελ. 154

Όπως προκύπτει, άλλα είδη απάτης που διενεργούνται μέσω του διαδικτύου, όπως η «Νιγηριανή επιστολή», όπου δηλαδή ο δράστης καταφέρνει, παραπλανώντας το θύμα και με την υπόσχεση κάποιου κέρδους, να αποσπά από αυτό χρηματικά ποσά, εμπίπτουν στην κατηγορία της κοινής απάτης, και όχι στο αδίκημα της απάτης με υπολογιστή[69].

Στο σημείο αυτό πρέπει να αναφερθεί ότι κατά την κρατούσα άποψη, το έννομο αγαθό που προστατεύεται με τη διάταξη του άρθρου 386 Α ΠΚ είναι η περιουσία, που είναι αποσυνδεδεμένη από το πρόσωπο του θύματος[70]. Βέβαια, ως άποψη υποστηρίζεται ότι η ανωτέρω διάταξη «κυρώνει τη συμπεριφορά με σκοπό παράνομου περιουσιακού οφέλους που κατατείνει σε παράνομες περιουσιακές μετατοπίσεις, προσβάλλοντας όμως αρχικά και ένα πρόγραμμα η/υ»[71].

Η διάταξη του άρθρου 386 Α ΠΚ αναφέρει περιοριστικά τους τρόπους με τους οποίους τελείται η απάτη με υπολογιστή. Ειδικότερα, τρόπος τέλεσης είναι η «η μη ορθή διαμόρφωση του προγράμματος»[72] και εδώ ανήκει η επεξεργασία ενός νέου προγράμματος και η συμπλήρωση ή παραποίηση «των λογικών βημάτων» του προγράμματος, όπως και οποιαδήποτε τροποποίηση στο αρχικό πρόγραμμα του υπολογιστή[73]. Παραπέρα, το αδίκημα τελείται με την παρέμβαση στην εξέλιξη του προγράμματος με τη χρήση του πληκτρολογίου *(console manipulation)*[74], όπως και η παρέμβαση στο υλικό (*hardware)* του

---

[69] Βλ. A.O. Salu (2004) 'Online crimes and advance fee fraud in Nigeria - are available legal remedies adequate?', *Journal of Money Laundering Control*, Vol. 8, No. 2, pp. 159-167 [Διαδίκτυο] Διαθέσιμο στο: https://doi.org/10.1108/13685200510621091 Πρόσβαση στις 10-12-2021

[70] Βλ. Ε. Βασιλάκη (1993) *Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών. -Η αντιμετώπιση του προβλήματος μετά την εισαγωγή του ν. 1805/88*. σελ. 201 επ.· Χ. Μυλωνόπουλο (1991) *Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο. Συμβολή στην ερμηνεία των άρθρων 13γ, 370Β, 370Γ και 386 Α Π.Κ. (άρθρ. 2-5 ν. 1805/88*, σελ. 59· Α.Παπαδαμάκη (2020) *Τα περιουσιακά εγκλήματα*.. σελ. 184

[71] Βλ. Γ. Νούσκαλη (2003) *Απάτη με ηλεκτρονικό υπολογιστή (η/υ): Το παρελθόν και το μέλλον του άρθρου 386 Α ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση*, ΠοινΔικ σελ. 178 επ.

[72] Βλ. Άρθ. 386Α ΠΚ, περ. α

[73] Βλ. Ε. Βασιλάκη (1993) *Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών-Η αντιμετώπιση του προβλήματος μετά την εισαγωγή του ν. 1805/88*..σελ.201 επ.

[74] Βλ. Βλ. Άρθ. 386Α ΠΚ, περ. β

ηλεκτρονικού υπολογιστή, όχι όμως και η παρέμβαση στην έξοδο των στοιχείων (*output manipulation)*[75].

Επίσης, η απάτη με υπολογιστή συντελείται κατά τη χρησιμοποίηση μη ορθών στοιχείων, όταν δηλαδή τα δεδομένα δεν αντιστοιχούν στα πραγματικά και κατά τη χρησιμοποίηση ελλιπών στοιχείων[76], όταν δηλαδή αυτά ανταποκρίνονται εν μέρει στην πραγματικότητα και η μη αναφορά τους είναι σημαντική για την επεξεργασία των δεδομένων. Χρησιμοποίηση μη ορθών στοιχείων υφίσταται όταν εισάγονται στον υπολογιστή στοιχεία που δεν ανταποκρίνονται σε υπαρκτά τέκνα, ώστε, για παράδειγμα, ο δράστης να λάβει επίδομα πολυτέκνου[77].

Στη συνέχεια, απάτη με υπολογιστή υφίσταται κατά την, άνευ σχετικού δικαιώματος, εισαγωγή, παραποίηση, διαγραφή ή εξαφάνιση δεδομένων του υπολογιστή, κυρίως σε δεδομένα που συνδέονται με την αναγνώριση ταυτότητας[78]. Εδώ, η περίπτωση αφορά στη χρησιμοποίηση κωδικών για την Ηλεκτρονική Τραπεζική *(e-banking*) ή στον κωδικό PIN, χωρίς να υπάρχει σχετικό δικαίωμα[79][80].

Ακόμη, το αδίκημα της απάτης με υπολογιστή τελείται και με την άνευ σχετικού δικαιώματος εκμετάλλευση λογισμικού που προορίζεται για τη μεταφορά χρημάτων[81]. Εδώ, περιλαμβάνονται μορφές απάτης, όπως η απάτη με την αλλαγή της κάρτας SIM κινητού τηλεφώνου, η οποία τελείται από τον

[75] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής*...σελ. 408
[76] Βλ. Βλ. Άρθ. 386Α ΠΚ, περ. γ
[77] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής*...σελ. 408
[78] Βλ. Βλ. Άρθ. 386Α ΠΚ, περ. δ
[79] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής*...σελ. 408-409
[80] Βλ. ΑΠ 813/2015 όπου κρίθηκε ότι το αδίκημα της απάτης με ηλεκτρονικό υπολογιστή, κατά το άρθρο 386 Α ΠΚ, τελείται κατά την ανάληψη χρημάτων από ΑΤΜ με την εισαγωγή πιστωτικής κάρτας, την οποία η κατηγορούμενη είχε στην κατοχή της με πλαστή εξουσιοδότηση, και την επιρροή στα στοιχεία του υπολογιστή των ΑΤΜ, διότι «εκ μέρους της χρήση της πιστωτικής κάρτας παρείχε στον υπολογιστή την συμπερασματικά συναγόμενη δήλωση ότι η χρήση γινόταν κάθε φορά από τον νόμιμο κάτοχο της πιστωτικής κάρτας, ενώ αυτό δε συνέβαινε» Τράπεζα Νομικών Πληροφοριών ΝΟΜΟΣ·ΑΠ 1726/2019 όπου κρίθηκε ότι η αντικειμενική υπόσταση της διάταξης του άρθρου 386 Α ΠΚ πραγματώνεται με την εισαγωγή της κάρτας ανάληψης μετρητών και την πληκτρολόγηση του κωδικού PIN, που είχαν αφαιρεθεί κατά παράνομο τρόπο από την κατοχή του θύματος, ΤΝΠ ΝΟΜΟΣ
[81] Βλ. Βλ. Άρθ. 386Α ΠΚ, περ. ε

δράστη με την χωρίς εξουσιοδότηση αλλαγή της κάρτας SIM τρίτου χρήστη και, έτσι ο δράστης έχει πρόσβαση στα δεδομένα του κατόχου του τηλεφώνου που είναι καταχωρημένα στη συσκευή, με συνέπεια ο τελευταίος να αποκτά παρανόμως περιουσιακό όφελος σε βάρος του συνδρομητή[82].

Στο σημείο αυτό πρέπει να γίνει αναφορά στην Οδηγία (ΕΕ) 2019/713[83], όπου η απάτη και η πλαστογράφηση υλικών και «άϋλων» μέσων πληρωμής, εκτός από τα μετρητά, τυποποιείται ως αδίκημα. Πιο συγκεκριμένα, η Οδηγία βρίσκει πεδίο εφαρμογής σε ηλεκτρονικής και εικονικής μορφής χρήμα, ενώ περιλαμβάνει: τις πιστωτικές κάρτες ή τους «δίσκους USB με κρυπτονομίσματα», δηλαδή υλικά μέσα πληρωμής, και β) τους «αριθμούς πιστωτικών και χρεωστικών καρτών, και τους κωδικούς ιδιωτικού κλειδιού «κρυπτονομίσματος», δηλαδή τα «άϋλα» μέσα πληρωμής[84].

4.2 Η πλαστογραφία ηλεκτρονικού εγγράφου

Σύμφωνα με τη διάταξη του άρθρου 13 γ' εδαφ. δευτ. ΠΚ «[...έγγραφο είναι και κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή αναπαραγωγή στοιχείων που δεν μπορούν να διαβαστούν άμεσα, πως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό...][85]. Στα πλαίσια του ανωτέρω ορισμού, ως έγγραφο νοείται και κάθε μέσο στο οποίο γίνεται εγγραφή ή αποθήκευση δεδομένων, όπως είναι για παράδειγμα σκληροί δίσκοι, μαγνητοταινίες, χαρτί που

[82] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής*...σελ. 410

[83] Βλ. Οδηγία (ΕΕ) 2019/713 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019 *για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών και την αντικατάσταση της απόφασης-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου*, ΕΕ L 123/18, 10.5.2019 [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX:32019L0713 Πρόσβαση στις 17-12-2021

[84] Βλ. Ι. Ιγγλεζάκη *(2021) Δίκαιο Πληροφορικής*...σελ. 410

[85] Άρθρο 13 ΠΚ, ν. 4619/2019

χρησιμοποιείται για εκτύπωση κλπ. Επιπλέον, στην έννοια του εγγράφου περιλαμβάνονται και «μαγνητικές ταινίες πιστωτικών καρτών, βάσεις δεδομένων και αρχεία», δεδομένου ότι αυτά είναι ηλεκτρονικά αρχεία[86]. Ωστόσο, δεν αποτελεί έγγραφο η απλή εγγραφή στη μνήμη RAM ενός ηλεκτρονικού υπολογιστή, αλλά η εγγραφή των δεδομένων πρέπει να έχει γίνει σε μια σταθερή μνήμη και να είναι «σταθερά ενσωματωμένα στους υλικούς φορείς τους», ενώ πρέπει να είναι δυνατόν να προκύψει ο εκδότης των δεδομένων[87]. Επισημαίνεται, ωστόσο, ότι η προστασία αφορά μόνο τα δεδομένα η προγράμματα που έχουν αξία ως αποδεικτικά, όπως για παράδειγμα οι εγγραφές στη μαγνητική ταινία των καρτών[88].

Στο πλαίσιο της ευρείας έννοιας του εγγράφου, είναι δυνατόν να εφαρμοστούν οι διατάξεις των άρθρων για «εγκλήματα σχετικά με τα υπομνήματα». Ιδίως οι διατάξεις των άρθρων για τα εγκλήματα της «πλαστογραφίας[89], της πλαστογραφίας πιστοποιητικών[90], της υφαρπαγής ψευδούς βεβαίωσης[91], της υπεξαγωγής εγγράφου[92], της ψευδούς βεβαίωσης»[93] εφαρμόζονται στα ηλεκτρονικά έγγραφα και στο λογισμικό[94]. Πιο συγκεκριμένα, αποτελεί πλαστογραφία η με παράνομο τρόπο αντιγραφή δεδομένων ή λογισμικού, στην περίπτωση που η πράξη του δράστη αποσκοπεί στην παραπλάνηση άλλου προσώπου με τη χρησιμοποίηση του αντιγράφου για γεγονός που μπορεί σημαντικό από νομικής πλευράς, ενώ επιβαρυντική περίπτωση αποτελεί η χρησιμοποίηση του λογισμικού που έχει αντιγραφεί[95].

---

[86] Βλ. Χ. Μυλωνόπουλου (1991) *Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο .Συμβολή στην ερμηνεία των άρθρων 13γ, 370Β, 370Γ και 386 Α Π.Κ. (άρθρ. 2-5 ν. 1805/88,* σελ. 43 επ.

[87] Βλ. Χ. Μυλωνόπουλου (1991) *Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο*. Συμβολή στην ερμηνεία των άρθρων 13γ, 370Β, 370Γ και 386 Α Π.Κ. (άρθρ. 2-5 ν. 1805/88. σελ. 4επ.

[88] Βλ. Χ. Μυλωνόπουλου (1991) *Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο*. Συμβολή στην ερμηνεία των άρθρων 13γ, 370Β, 370Γ και 386 Α Π.Κ. (άρθρ. 2-5 ν. 1805/88, σελ. 4επ.

[89] Άρθρο 216 ΠΚ, Ποινικός Κώδικας [Διαδίκτυο] Διαθέσιμο στο: https://www.legal-tools.org/doc/60f2e6/pdf/ Πρόσβαση στις 10-12-2021

[90] Άρθρο 217 ΠΚ

[91] Άρθρο 220 ΠΚ

[92] Άρθρο 222 ΠΚ

[93] Άρθρο 242 ΠΚ

[94] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής*...σελ. 419-420

[95] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής*...σελ. 420

4.3 Η αντιγραφή προγραμμάτων ηλεκτρονικού υπολογιστή και η χρησιμοποίησή τους χωρίς δικαίωμα

Με τη διάταξη του άρθρου 370 Δ[96] θεσπίζεται έννομη προστασία σε περίπτωση παράνομης αντιγραφής και χρήσης λογιστικού και της μη εξουσιοδοτημένης πρόσβασης σε δεδομένα ηλεκτρονικού υπολογιστή. Με τη συγκεκριμένη διάταξη, ενώ φαίνεται ότι δεν υφίσταται σύνδεση μεταξύ της προστασίας του λογισμικού που προβλέπει το δίκαιο της πνευματικής ιδιοκτησίας και του ποινικού δικαίου, δε συνεπάγεται ότι αποσυνδέονται οι κυρώσεις που προβλέπουν οι διατάξεις του ποινικού δικαίου από την παροχή προστασίας που προβλέπει το ανωτέρω δίκαιο. Στην εφαρμογή της διάταξης του άρθρου 370 Δ ΠΚ τίθενται περιορισμοί από το ν. 2121/1993[97], διότι διαφορετικά, το αξιόποινο θα ήταν ιδιαίτερα διευρυμένο[98].

Με την συγκεκριμένη διάταξη προβλέπεται η τιμωρία της αντιγραφής και χρησιμοποίησης ενός προγράμματος ηλεκτρονικού υπολογιστή χωρίς να υφίσταται σχετικό δικαίωμα. Το άρθρο αυτό συνιστά τη βάση για την προστασία του λογισμικού σύμφωνα με τις διατάξεις του Ποινικού Δικαίου[99]. Αντιστοίχως, η διάταξη του άρθρου 66 ν. 2121/1993[100] αποτελεί την κύρια διάταξη που προβλέπει την προστασία της πνευματικής ιδιοκτησίας.

---

[96] Άρθρο 370 Δ παρ. 1 ΠΚ «Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με χρηματική ποινή ή παροχή κοινωφελούς εργασίας»

[97] Ν. 2121/1993 - ΦΕΚ 25/Α/4-3-1993: *Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-pneumatike-idioktesia/n-2121-1993.html Πρόσβαση στις 20-12-2021

[98] Βλ. Χ. Μυλωνόπουλου (1991) *Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο*...σελ. 87-88·Μ.Μαρίνου, *Λογισμικό. Νομική προστασία και συμβάσεις* (Ι) 1992, σελ. 88

[99] Βλ. Ε. Βασιλάκη (1993) *Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών- Η αντιμετώπιση του προβλήματος μετά την εισαγωγή του ν. 1805/88*... σελ. 105

[100] Άρθρο 66 παρ. 1 ν. 2121/1993 «Όποιος χωρίς δικαίωμα και κατά παράβαση ίων διατάξεων του παρόντος νόμου ή διατάξεων των χυρωμένων με νόμο πολυμερών διεθνών συμβάσεων για την προστασία της πνευματικής ιδιοκτησίας εγγράφει, αναπαράγει στο πρωτότυπο ή σε μετάφραση ή διασκευή, θέτει σε κυκλοφορία ή κατέχει με σκοπό θέσης οε κυκλοφορία, χρησιμοποιεί κατά παράβαση περιοριστικών όρων, παρουσιάζει στο κοινό, εκτελεί δημόσια, μεταδίδει ραδιοτηλεοπτικά κατά οποιονδήποτε

Περαιτέρω, στον ν, 2121/1993 δεν προβλέπεται ορισμός για την αναπαραγωγή και την έλλειψη αυτή καλύπτει η επιστήμη, αναφέροντας ότι αναπαραγωγή είναι η «παραγωγή ενός ή περισσότερων σταθερών αντιτύπων ή αντιγράφων ενός έργου, η οποία το καθιστά προσιτό στις αισθήσεις άμεσα ή μέσω τεχνικών συσκευών»[101].

Περαιτέρω, από τον νόμο απαγορεύεται η χρησιμοποίηση ενός προγράμματος χωρίς σχετικό δικαίωμα. Εδώ περιλαμβάνεται για παράδειγμα ,η εκτέλεση του λογισμικού από το σύστημα επεξεργασίας που χρησιμοποιεί ο ηλεκτρονικός υπολογιστής, ενώ δεν περιλαμβάνεται η περίπτωση της απλής ανάληψης των υλικών φορέων του λογισμικού από τρίτο, καθώς θεωρείται προπαρασκευαστική πράξη που δεν τιμωρείται, όπως επίσης δεν τιμωρείται η μελέτη του υλικού που συνοδεύει το πρόγραμμα ή της περιγραφής του τελευταίου[102].

Βεβαίως, θα πρέπει να αναφερθεί ότι η τροποποίηση του λογισμικού αποτελεί παράνομη χρήση, καθώς προσβάλλεται έτσι το δικαίωμα του δημιουργού[103], εφόσον δεν έχει δώσει σχετική άδεια ο τελευταίος. Μάλιστα, σύμφωνα με μια άποψη, και η μεταβίβαση του λογισμικού θεωρείται ως έμμεση χρησιμοποίηση, η οποία προσβάλλει το περιουσιακό δικαίωμα του δημιουργού και ως εκ τούτου είναι παράνομη[104].

τρόπο και γενικά εκμεταλλεύεται έργο που είναι αντικείμενο πνευματικής ιδιοκτησίας ή εισάγει αντίτυπα ή οργανώνει δημόσια εκτέλεση τέτοιου έργου ή προσβάλλει το δικαίωμα του πνευματικού δημιουργού να αποφασίζει για την παρουσίαση του έργου στο κοινό και να το παρουσιάζει αναλλοίωτο χωρίς προσθήκες ή περικοπές, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή 1 έως 5 εκατομμυρίων δραχμών»

[101] Βλ. Μ.Θ. Μαρίνου (2004) *Πνευματική ιδιοκτησία* σελ. 152·Γ. Κουμάντου (2002) *Πνευματική ιδιοκτησία*, σελ. 218 σύμφωνα με τον οποίο «αναπαραγωγή είναι η παραγωγή νέων υλικών υποστρωμάτων όπου επαναλαμβάνεται η αρχική ενσωμάτωση του έργου»

[102] Ε. Βασιλάκη (1993) *Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών- Η αντιμετώπιση του προβλήματος μετά την εισαγωγή του ν. 1805/88*.. σελ. 116 επ.

[103] Άρθρο 3 παρ. 1 περ. γ' ν. 2121/1993 «Το περιουσιακό δικαίωμα δίνει οτο δημιουργό ιδίως την εξουσία να επιτρέπει ή να απαγορεύει:..γ) τη διασκευή, την προσαρμογή ή άλλες μετατροπές του έργου...»

[104] Ε. Βασιλάκη (1993) *Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών-Η αντιμετώπιση του προβλήματος μετά την εισαγωγή του ν. 1805/88*….σελ. 118 επ

4.4 Το « ηλεκτρονικό ψάρεμα» (*spear phishing*) μέσω ηλεκτρονικού υπολογιστή

Το «ηλεκτρονικό ψάρεμα» (*Spear phishing)* είναι μια διαδικασία που στοχεύει σε συγκεκριμένα άτομα ή ομάδες εντός ενός οργανισμού. Είναι μια μορφή παραλλαγής του «ψαρέματος» (*phishing),* μια κακόβουλη πρακτική που μέσω της αποστολής ηλεκτρονικών μηνυμάτων, των μέσων κοινωνικής δικτύωσης, της στιγμιαίας ανταλλαγής μηνυμάτων καθώς και μέσω άλλων μορφών πλατφόρμας αποσκοπεί να ωθήσει τους χρήστες να προβούν στην αποκάλυψη ιδιωτικών πληροφοριών ή να διενεργήσουν ˈάλλες πράξεις που θα προκαλέσουν υπονόμευση δικτύου, διαφυγή δεδομένων και οικονομικές απώλειες[105].

Επίσης, ενώ η τακτική του «ψαρέματος» (*phishing*) είναι η μαζική αποστολή ηλεκτρονικών μηνυμάτων σε τυχαίους αποδέκτες, στο «ηλεκτρονικό ψάρεμα» (*spear phishing*) η αποστολή γίνεται σε συγκεκριμένους αποδέκτες, αφού έχει προηγηθεί σχετική έρευνα[106].

Ένα τυπικό παράδειγμα «ηλεκτρονικού ψαρέματος» (*spear phishing*) περιλαμβάνει την αποστολή ηλεκτρονικού μηνύματος και συνημμένου κειμένου. Το ηλεκτρονικό μήνυμα περιέχει πληροφορίες που αφορούν τον αποδέκτη, συμπεριλαμβανομένου του ονόματός του και τη θέση του στην εταιρεία. Στη συνέχεια, το θύμα θα πραγματοποιήσει όλες τις ενέργειες που θα οδηγήσουν στη μόλυνση, θα ανοίξει δηλαδή το ηλεκτρονικό μήνυμα καθώς και το συνημμένο κείμενο[107].

Ουσιαστικά δηλαδή, στο «ηλεκτρονικό ψάρεμα» (*spear phishing*) οι χάκερς στοχεύουν εργαζόμενους, μέσω των ηλεκτρονικών ταχυδρομείων συναδέλφων των πρώτων, επιτρέποντας κατ' αυτό τον τρόπο στους εγκληματίες του

---

[105] Βλ. Trend Micro [n.d.] *Spear phishing* [Διαδίκτυο] Διαθέσιμο στο: https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing Πρόσβαση στις 20-12-2021

[106] Βλ. Trend Micro [n.d.] *Spear phishing*..

[107] Βλ. Trend Micro [n.d.] *Spear phishing*..

κυβερνοχώρου να υποκλέψουν δεδομένα προσωπικού χαρακτήρα[108]. Οι χάκερς συνήθως προσποιούνται ότι είναι υπάλληλοι της εταιρείας και στέλνουν μηνύματα μέσω ηλεκτρονικού ταχυδρομείου σε άλλους υπαλλήλους της εταιρείας, θέτοντας σε σοβαρό κίνδυνο την κυβερνοασφάλεια της εταιρείας. Οι χάκερς αποβλέπουν στη συγκέντρωση πληροφοριών προσωπικού χαρακτήρα του στόχου τους, ώστε τα ποσοστά. Η μέθοδος αυτή είναι πολύ επιτυχημένη και το 91% των επιθέσεων στο διαδίκτυο πραγματοποιείται με αυτή την τεχνική[109].

4.5 Ο εκφοβισμός μέσω του Διαδικτύου (*cyberbulling)*

Τα τελευταία χρόνια, το ζήτημα του «Διαδικτυακού εκφοβισμού» (*cybebulling)* έχει λάβει πολύ μεγάλες διαστάσεις. Σύμφωνα με πορίσματα ερευνών, η χρήση της τεχνολογίας και των μέσων του διαδικτύου αυξάνεται ολοένα και περισσότερο προκειμένου να ασκηθεί ψυχολογική βία, παρενόχληση, ακόμα και να δυσφημιστούν άτομα, με συνέπεια να διαταράσσεται η ψυχική υγεία και ηρεμία αυτών των ατόμων που είναι στόχοι περιστατικών « Διαδικτυακού εκφοβισμού» (*cyber bulling)* [110].

Ειδικότερα, ο διαδικτυακός εκφοβισμός υφίσταται όταν κάποιος κακόβουλα παρενοχλεί κάποιο άτομο χρησιμοποιώντας την τεχνολογία[111]. Τα περιστατικά παρενόχλησης μπορεί να λαμβάνουν χώρα είτε σε τακτικά είτε σε άτακτα

---

[108] Βλ. D. Stephenson, (2013) 'Spear Phishing: Who's Getting Caught?', Business 2 Community, [Διαδίκτυο] Διαθέσιμο στο: https://www.business2community.com/infographics/spear-phishing-attacks-whos-getting-caught-0505469 Πρόσβαση στις 20-12-2021

[109] Βλ. D. Stephenson (2013) *'Spear Phishing Who's Getting Caught?'...*

[110] N. Martin, J. Rice (2011) *'Cybercrime: understanding and addressing the concerns of stakeholders', Computers & Security*, [Διαδίκτυο] Διαθέσιμο στο: https://www.sciencedirect.com/science/article/pii/S016740481100085X Πρόσβαση στις 22-12-2021

[111] Βλ. SafeInternet4Kids.gr [χ.χ.] *Cyberbullying – Διαδικτυακός Εκφοβισμός* [χ.χ.] [Διαδίκτυο] Διαθέσιμο στο: https://saferinternet4kids.gr/hot-topics-ef/cyberbullying-ef/ Πρόσβαση στις 30-11-2021

χρονικά διαστήματα μέσω πράξεων εκφοβισμού και εκδήλωσης επιθετικής ή καταπιεστικής συμπεριφοράς[112].

Ο διαδικτυακός εκφοβισμός πραγματοποιείται, μεταξύ άλλων, μέσω της αποστολής μηνυμάτων άσεμνου περιεχομένου, της απαγόρευσης πρόσβασης ατόμων σε εφαρμογές συνομιλιών, της δημοσίευσης δυσάρεστων φωτογραφιών, της κυκλοφορίας δυσφημιστικών σχολίων[113].

Αποτέλεσμα των ανωτέρω είναι , τα θύματα του διαδικτυακού εκφοβισμού να βιώνουν έντονο συναισθηματικό άγχος, καθώς, συνήθως, ο αποστολέας των κακόβουλων μηνυμάτων είναι ανώνυμος και συνεπώς δεν είναι εύκολο τα θύματα να γνωρίζουν ποιος είναι ο δράστης. Ακόμη, ο διαδικτυακός εκφοβισμός μπορεί να συμβεί κάθε στιγμή της ημέρας και από οποιαδήποτε τοποθεσία. Σε περίπτωση που τα μηνύματα ή οι φωτογραφίες αναρτηθούν στο διαδίκτυο, πολλοί χρήστες έχουν άμεση πρόσβαση σε αυτές και το θύμα βιώνει μια πολύ αγχωτική κατάσταση, καθώς διαπιστώνει την ταχύτητα με την οποία μια φωτογραφία ή μια κακόβουλη φήμη διασπείρεται στο διαδίκτυο[114].

Πρέπει να τονιστεί ότι, ο διαδικτυακός εκφοβισμός μπορεί να εκδηλώνεται είτε με άμεσο είτε με έμμεσο τρόπο και να εμπλέκονται και άλλα άτομα, τα οποία πιθανόν να μη γνωρίζουν ή να μην έχουν σχέση με το θύμα[115].
Άλλες τύποι διαδικτυακού εκφοβισμού περιλαμβάνουν τη «Διαδικτυακή παρακολούθηση» (*cyberstalking*) όπου ο εισβολέας προσπαθεί επίμονα να επικοινωνήσει με το θύμα, και, συνήθως, όσοι παρακολουθούν μέσω διαδικτύου κάποιο άτομο τρέφουν βαθιά αισθήματα, θετικά ή αρνητικά, για το θύμα τους[116].
Ακολούθως, η «διαρροή απόρρητων στοιχείων» (*doxing)* συνιστά μορφή διαδικτυακού εκφοβισμού κατά την οποία ένα άτομο ή ακόμη και ομάδα ατόμων διαρρέουν στα μέσα κοινωνικής δικτύωσης ή σε ανοιχτούς τόπους συζητήσεων, προσωπικά στοιχεία του θύματος, όπως η διεύθυνση του σπιτιού του, ο αριθμός

[112] *Βλ.* SafeInternet4Kids.gr [χ.χ.] *Cyberbullying – Διαδικτυακός Εκφοβισμός...*
[113] *Βλ.* SafeInternet4Kids.gr [χ.χ.] *Cyberbullying – Διαδικτυακός Εκφοβισμός...*
[114] Βλ. . SafeInternet4Kids.gr [χ.χ.] *Cyberbullying – Διαδικτυακός Εκφοβισμός...*
[115] *Βλ.* SafeInternet4Kids.gr *[χ.χ.] Cyberbullying* – Διαδικτυακός Εκφοβισμός...
[116] Βλ. The Cybersmile foundation [n.d] '*What is cyberbulling*?' [Διαδίκτυο] Διαθέσιμο στο: https://www.cybersmile.org/advice-help/category/what-is-cyberbullying Πρόσβαση στις 30-11-2021

του κινητού τηλεφώνου του, ή ο τόπος εργασίας του, χωρίς το ίδιο το θύμα να έχει δώσει σχετική άδεια για αυτό[117].

Σοβαρή μορφή διαδικτυακού εκφοβισμού αποτελεί και «εκδικητική πορνογραφία» (*revenge porn)* όπου υλικό ενός ατόμου με σεξουαλικό περιεχόμενο έχει διαρρεύσει στα μέσα κοινωνικής δικτύωσης ή έχει διαμοιρασθεί σε συγκεκριμένες σελίδες εκδικητικής πορνογραφίας, χωρίς το ίδιο το θύμα να έχει δώσει την άδειά του για μια τέτοια ενέργεια. Συνήθως, τέτοιου είδους υλικό αναρτάται από πρώην συντρόφους, οι οποίοι επιθυμούν να βλάψουν την υπόληψη του θύματος και να το ταπεινώσουν[118].

Ως διαδικτυακός εκφοβισμός θεωρείται και η δημιουργία « ψεύτικων προφίλ» (*false profiles*) όπου στα μέσα κοινωνικής δικτύωσης δημιουργούνται ψεύτικα προφίλ, με στόχο να προκληθεί βλάβη στην υπόληψη ενός ατόμου ή ακόμη και εταιρείας. Αυτό επιτυγχάνεται αρχικά με την απόκτηση οπτικού υλικού του θύματος ,το οποίο βρίσκεται διαθέσιμο δημόσια και ακολουθεί στη συνέχεια η δημιουργία ενός λογαριασμού, όσο το δυνατόν πιο γνήσιου[119].

4. 6 Το έγκλημα της κλοπής ταυτότητας

Ο όρος «*κλοπή ταυτότητας*» καλύπτει ένα ευρύ φάσμα εγκλημάτων ταυτοπροσωπίας και ταυτοποίησης. Πιο αναλυτικά, μπορεί να συνδέεται με τη χρησιμοποίηση των προσωπικών δεδομένων ενός ατόμου, προκειμένου να αποκτηθούν οικονομικά οφέλη σε βάρος του, την χωρίς άδεια είσοδο στην προσωπική του ζωή ή ακόμη να αφορά σε συγκάλυψη άλλων εγκληματικών πράξεων[120].

---

[117] Βλ. The Cybersmile foundation [n.d.] *What is cyberbulling?...*
[118] Βλ. The Cybersmile foundation [n.d.] *'What is cyberbulling?'...*
[119] Βλ. 'The Cybersmile foundation [n.d.] *'What is cyberbulling?'...*
[120] Βλ. C. J. Hoofnagle (2007) *'Identity Theft: Making the Known Unknowns Known'*, Harvard Journal of Law and Technology, Vol. 21 [Διαδίκτυο] Διαθέσιμο στο: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=969441 Πρόσβαση στις 30-11-2021

Περαιτέρω, σημειώνεται ότι η κλοπή ταυτότητας προκαλεί οικονομικές απώλειες σε καταναλωτές, σε χρηματοπιστωτικούς οργανισμούς, σε εμπορικές επιχειρήσεις και στο σύνολο της οικονομίας γενικότερα[121].

Προκειμένου να γίνει ταυτοποίηση των παρεμβάσεων και να γίνει κατάλληλη κατανομή πόρων, απαιτείται συνολική μελέτη δεδομένων σχετικά με το σκοπό και την επίδραση της κλοπής ταυτότητας. Ένας τρόπος για να συγκεντρωθούν αυτά τα δεδομένα είναι να απαιτηθεί από τους χρηματοπιστωτικούς οργανισμούς να δημοσιεύσουν εκθέσεις στοιχείων σχετικά με την κλοπή ταυτότητας. Μέσω αυτών των δημόσιων εκθέσεων θα ταυτοποιηθούν οι παρεμβάσεις και η πιθανή απόδοση αυτών των παρεμβάσεων[122].

Αυτή η γνωστοποίηση των εκθέσεων είναι αναγκαία προκειμένου να δημιουργηθεί ένα σταθερό υπόβαθρο για τις επενδύσεις των επιχειρήσεων καθώς και για την ανάληψη δράσης από μέρους των ρυθμιστών. Εξάλλου, το τίμημα της κλοπής ταυτότητας το πληρώνουν οι πολίτες, είτε άμεσα, στις περιπτώσεις που είναι τα θύματα, είτε έμμεσα, μέσω υψηλότερων εισφορών και επιτοκίων[123].

4. 7 Το έγκλημα της πορνογραφίας και η πορνογραφία ανηλίκων

Σύμφωνα με τα οριζόμενα στο άρθρο 29 ν. 5060/1931[124] αποτελεί παράνομη ενέργεια και ο νομοθέτης προβλέπει ποινή φυλάκισης ενός μηνός και

[121] Βλ. C. J. Hoofnagle (2007) *'Identity Theft: Making the Known Unknowns Known'*...
[122] Βλ. C. J. Hoofnagle (2007) *'Identity Theft: Making the Known Unknowns Known'*...
[123] Βλ. C. J. Hoofnagle (2007)*'Identity Theft: Making the Known Unknowns Known'*...
[124] Άρθρο 29 ν. 5060/1931 «Οστις προς τον σκοπόν εμπορίας, ή διανομής, ή δημοσία εκθέσεως, παρασκευάζει, αποκτά, κατέχει, μεταφέρει, εισάγει εις το Κράτος ή εξάγει, ή καθ` οιονδήποτε τρόπον τίθησιν εις κυκλοφορίαν έγγραφα, έντυπα, συγγράμματα, σχέδια εικόνας, ζωγραφίας, εμβλήματα, φωτογραφίας, κινηματογραφικάς ταινίας, ή άλλα αντικείμενα άσεμνα, οιουδήποτε είδους, όστις μεταχειρίζεται, οιονδήποτε μέσον δημοσιότητος προς διευκόλυνσιν της κυκλοφορίας ή τού εμπορίου των αυτών ασέμνων αντικειμένων, τιμωρείται δια φυλακίσεως τουλάχιστον ενός μηνός και δια χρηματικής ποινής... » [Διαδίκτυο] Διαθέσιμο στο: https://www.kodiko.gr/nomothesia/document/579264/nomos-5060-1931 Πρόσβαση στις 22-11-2021

χρηματική ποινή, σε όποιον κατασκευάζει, αποκτά στην κατοχή του, μεταφέρει, εισάγει στη χώρα ή εξάγει από αυτή εικόνες με πορνογραφικό υλικό, με στόχο την εμπορική εκμετάλλευση αυτού του υλικού, την κυκλοφορία του ή τη δημοσιοποίησή του. Ακόμη, όπως ορίζει το άρθρο 30 ν. 5060/1931[125], άσεμνα χαρακτηρίζονται και τα έντυπα καθώς και οι εικόνες που είναι προσβλητικές για το κοινό αίσθημα, δηλαδή θίγουν την αιδώ.

Πρέπει να επισημανθεί ότι, η ανωτέρω διάταξη εφαρμόζεται και στις περιπτώσεις κατοχής και δημοσίευσης εικόνων πορνογραφίας στο διαδίκτυο, εφόσον στόχος είναι η εμπορία[126] [127].

Ωστόσο, εκτός από την πορνογραφία, το διαδίκτυο αποτελεί το κύριο μέσο δια του οποίου διαδίδεται η παιδική πορνογραφία και μάλιστα διεθνώς[128].

Το άρθρο 384 Α ΠΚ που προστέθηκε με το άρθρο 6 ν. 3064/2002[129], κατέτασσε την πορνογραφία κατά ανηλίκων στα εγκλήματα, ενώ με το ν.

---

[125] Άρθρο 30 ν. 5060/1931 «Άσεμνα κατά τις περιπτώσεις του προηγούμενου άρθρου θεωρούνται τα χειρόγραφα, έντυπα εικόνες και λοιπά αντικείμενα, όταν, σύμφωνα με το κοινό αίσθημα, προσβάλλουν την αιδώ...»

[126] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής*...σελ. 427

[127] Σημειώνεται ότι οι ανωτέρω διατάξεις εφαρμόζονταν και σε περιπτώσεις παιδικής πορνογραφίας, πριν θεσπιστεί νομοθεσία για την τελευταία· Βλ. ΑΠ 2087/2003 (Ε' ΠοινΤμ) ΝΟΜΟΣ ΤΝΠ

[128] Βλ. Ίδρυμα Μαραγκοπούλου, *Η παιδική πορνογραφία στο διαδίκτυο*, 2007, σελ. 5 επ·Κ. Θεοδωρίδη, *Πορνογραφία ανηλίκων στο Διαδίκτυο*, ΕΕΕυρΔ, 2207, σελ. 673 επ. **ε**

[129] Βλ. J. Hoofnagle (2007)*'Identity Theft: Making the Known Unknowns Known'*...

[129] Άρθρο 29 ν. 5060/1931 «Οστις προς τον σκοπόν εμπορίας, ή διανομής, ή δημοσία εκθέσεως, παρασκευάζει, αποκτά, κατέχει, μεταφέρει, εισάγει εις το Κράτος ή εξάγει, ή καθ` οιονδήποτε τρόπον τίθησιν εις κυκλοφορίαν έγγραφα, έντυπα, συγγράμματα, σχέδια εικόνας, ζωγραφίας, εμβλήματα, φωτογραφίας, κινηματογραφικάς ταινίας, ή άλλα αντικείμενα άσεμνα, οιουδήποτε είδους, όστις μεταχειρίζεται, οιονδήποτε μέσον δημοσιότητος προς διευκόλυνσιν της κυκλοφορίας ή τού εμπορίου των αυτών ασέμνων αντικειμένων, τιμωρείται δια φυλακίσεως τουλάχιστον ενός μηνός και δια χρηματικής ποινής... » [Διαδίκτυο] Διαθέσιμο στο: https://www.kodiko.gr/nomothesia/document/579264/nomos-5060-1931 Πρόσβαση στις 22-11-2021

[129] Άρθρο 30 ν. 5060/1931 «Άσεμνα κατά τις περιπτώσεις του προηγούμενου άρθρου θεωρούνται τα χειρόγραφα, έντυπα εικόνες και λοιπά αντικείμενα, όταν, σύμφωνα με το κοινό αίσθημα, προσβάλλουν την αιδώ...»

[129] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής*...σελ. 427

[129] Σημειώνεται ότι οι ανωτέρω διατάξεις εφαρμόζονταν και σε περιπτώσεις παιδικής πορνογραφίας, πριν θεσπιστεί νομοθεσία για την τελευταία· Βλ. ΑΠ 2087/2003 (Ε' ΠοινΤμ) ΝΟΜΟΣ ΤΝΠ

[129] Βλ. Ίδρυμα Μαραγκοπούλου, *Η παιδική πορνογραφία* Άρθρο 6 «1.Όποιος από κερδοσκοπία παρασκευάζει, κατέχει, προμηθεύεται, αγοράζει, μεταφέρει, διακινεί,

3625/2007[130] τροποποιήθηκε η ανωτέρω διάταξη. Η τροποποίηση της εν λόγω διάταξης κρίθηκε ως αναγκαία, διότι έθετε ως προϋπόθεση για την επιβολή τιμωρίας της πορνογραφίας ανηλίκων να διαπράττεται αυτή για «κερδοσκοπία», όρος που έπρεπε να διαγραφεί[131].

Στη συνέχεια, νέα τροποποίηση του άρθρου 349 Α ΠΚ έγινε με τον άρθρο 8[132] ν. 4267/2014, για να κυρωθεί η Οδηγία 2011/92/ΕΕ[133] κα να ενσωματωθούν οι

διαθέτει, πωλεί ή θέτει με οποιονδήποτε τρόπο σε κυκλοφορία πορνογραφικό υλικό τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή δέκα χιλιάδων έως εκατό χιλιάδων ευρώ.

2.Πορνογραφικό υλικό κατά την έννοια της προηγούμενης παραγράφου συνιστά κάθε περιγραφή ή πραγματική ή εικονική αποτύπωση, σε οποιονδήποτε υλικό φορέα, του σώματος ανηλίκου που αποσκοπεί στη γενετήσια διέγερση, καθώς και η καταγραφή ή αποτύπωση, σε οποιονδήποτε υλικό φορέα, πραγματικής, προσποιητής ή εικονικής ασελγούς πράξης που ενεργείται για τον ίδιο σκοπό από ή με ανήλικο», ν. 3064/2002 - ΦΕΚ 248/Α/15-10-2002: Νόμος 3064/2002 :*Καταπολέμηση της εμπορίας ανθρώπων, των εγκλημάτων κατά της γενετήσιας ελευθερίας, της πορνογραφίας ανηλίκων και γενικότερα της οικονομικής εκμετάλλευσης της γενετήσιας ζωής και αρωγή στα θύματα των πράξεων αυτών* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-egklema-organomeno/n-3064-2002.html Πρόσβαση στις 20-12-2021

[130] Βλ. Νόμος 3625/2007 - ΦΕΚ 290/Α/24-12-2007: *Κύρωση, εφαρμογή του Προαιρετικού Πρωτοκόλλου στη Σύμβαση για τα Δικαιώματα του Παιδιού σχετικά με την εμπορία παιδιών, την παιδική πορνεία και παιδική πορνογραφία και άλλες διατάξεις.*[Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-anilikoi/n-3625-2007.html Πρόσβαση στις 22-12-2021

[131] Βλ. Ίδρυμα Μαραγκοπούλου (2006) *Η παιδική πορνογραφία*..σελ. 62 επ.·Γ. Νούσκαλη (2006) *Πορνογραφία ανηλίκων: τα κρίσιμα ζητήματα του άρθρου 348 Α ΠΚ*, Ποιν Δικ σελ. 908 επ.·Κ. Θεοδωρίδη, *Πορνογραφία ανηλίκων*...σελ. 674·Γ. Καρανικόλα (2005) *Παιδική Πορνογραφία στο Διαδίκτυο: προβληματισμοί γύρω από τη νέα ρύθμιση του άρθρου348 Α ΠΚ*, ΠοινΔικ σελ. 964 επ.

[132] Άρθρο 8 «*1.Οι παράγραφοι 2, 3 και 4 του άρθρου 348Α του Ποινικού Κώδικα αντικαθίστανται ως εξής:*

«*2.* Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιονδήποτε τρόπο διαθέτει, διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, μέσω της τεχνολογίας των πληροφοριών και επικοινωνιών, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή πενήντα χιλιάδων έως τριακοσίων χιλιάδων ευρώ.

3.Υλικό παιδικής πορνογραφίας, κατά την έννοια των προηγούμενων παραγράφων, συνιστά η αναπαράσταση ή η πραγματική ή εικονική αποτύπωση, σε ηλεκτρονικό ή άλλο υλικό φορέα, των γεννητικών οργάνων ή του σώματος εν γένει του ανηλίκου, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και της πραγματικής ή εικονικής ασελγούς πράξης που διενεργείται από ή με ανήλικο.

4.Οι πράξεις των παραγράφων 1 και 2 τιμωρούνται με κάθειρξη μέχρι δέκα ετών και χρηματική ποινή εκατό χιλιάδων έως πεντακοσίων χιλιάδων ευρώ:...», ν. 4267/2014 - ΦΕΚ 137/Α/12-6-2014: *Καταπολέμηση της σεξουαλικής κακοποίησης και* εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και άλλες διατάξεις [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-anilikoi/n-4267-2014.html Πρόσβαση στις 22-11-2021

διατάξεις στην ελληνική έννομη τάξη. Τέλος, η παρ. του άρθρου 348 Α[134] ΠΚ αντικαταστάθηκε με το ν. 4619/2019.

Με τη διάταξη του άρθρου 348 Α ΠΑΡ. 2 ΠΚ τυποποιείται αρχικά ένα έγκλημα κατά της γενετήσιας ελευθερίας του ανθρώπου, αλλά και ένα έγκλημα κατά της παιδικής ηλικίας, το οποίο συνιστά έγκλημα «αφηρημένης διακινδύνευσης»[135], τυποποιείται, ωστόσο, και ένα έγκλημα κατά ανηλίκων που είναι θύματα των πράξεων εμφανίζονται στο πορνογραφικό υλικό[136].

Επισημαίνεται εδώ ότι, ως προς την έννοια της «κατοχής» πορνογραφικού υλικού ανηλίκων, από τη νομολογία γίνεται δεκτό ότι ως τέτοια « νοείται η φυσική εξουσία του δράστη ώστε να μπορεί να εξακριβώσει με δική του θέληση την ύπαρξη του υλικού και να τη διαθέσει πραγματικά και αν ακόμη προορίζεται για προσωπική χρήση του δράστη[137].

Επιπλέον, αναφέρεται ότι δεν υφίσταται αξιόποινη πράξη όταν το συγκεκριμένο υλικό εμφανίζεται στην οθόνη του υπολογιστή ή όταν «ανοίγει» ένα μήνυμα ηλεκτρονικού ταχυδρομείου, εφόσον δεν προκύπτει ότι το υλικό βρίσκεται υπό τη «φυσική εξουσίαση» του χρήστη του ηλεκτρονικού υπολογιστή. Βέβαια, η επίσκεψη σε ιστοσελίδες, όπως και η πρόσβαση σε σχετικό υλικό που έχει αποθηκευτεί σε άλλους ηλεκτρονικούς υπολογιστές, συνιστά αξιόποινη πράξη, διότι στην περίπτωση αυτή το υλικό αυτό αποθηκεύεται προσωρινά στη μνήμη του υπολογιστή[138]. Παραπέρα, η έννοια της διάθεσης του υλικού

---

[133] Βλ. Οδηγία 2011/93/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 2011 *σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου*, L335/1, 17.12.2011, [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32011L0093 Πρόσβαση στις 28-12-2021

[134] Βλ. Άρθρο 348 Α παρ. 2 ΠΚ «Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιονδήποτε τρόπο διαθέτει, διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, μέσω πληροφοριακών συστημάτων, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή»

[135] Βλ. Β Πολυζωϊδου (2016) *Το αξιόποινο της πορνογραφίας ανηλίκων* σελ. 129 επ

[136] Βλ. Γ. Νούσκαλη (2006) *Πορνογραφία ανηλίκων. τα κρίσιμα ζητήματα του άρθρου 348 Α ΠΚ.. ·* Ίδρυμα Μαραγκοπούλου, Η *παιδική πορνογραφία*...σελ 55

[137] Βλ. ΑΠ 628/2006, ΑΠ 810/2007, ΑΠ 770/2015 ΝΟΜΟΣ ΤΝΠ

[138] Βλ. Γ. Νούσκαλη (2020) *Κατοχή και διανομή/διάθεση πορνογραφικού υλικού ανηλίκων (άρθρο 348 Α ΠΚ): Η νομολογιακή προσέγγιση κρίσιμων ζητημάτων ουσιαστικού και*

καλύπτει, εκτός από την πώληση του υλικού ,και τη μεταφορά του, ή τη διάδοσή του στο κοινό[139].

Όσον αφορά τον ορισμό του πορνογραφικού υλικού της διάταξης του άρθρου 348 Α παρ. 3[140] ΠΚ, είναι πιο περιοριστικός σε σχέση με τον ορισμό του άρθρου 1 περ. β' της 2004/68/ΕΕ[141] απόφασης-πλαίσιο, καθώς ορίζει ως προϋπόθεση την πρόκληση «γενετήσιας» διέγερσης, η οποία δεν αποτελεί προϋπόθεση σύμφωνα με την ανωτέρω απόφαση-πλαίσιο[142][143].

4.8 Ο διαδικτυακός μισαλλόδοξος λόγος ή η ρητορική μίσους (*hatespeech)*

δικονομικού δικαίου, Επιθεώρηση Δικαίου Πληροφορικής [Διαδίκτυο] Διαθέσιμο στο: https://ejournals.lib.auth.gr/infolawj/article/view/7783 Πρόσβαση στις 12-11-2021 ε

[139] Βλ. Γ. *Νούσκαλη* (2020*) Κατοχή και διανομή/διάθεση πορνογραφικού υλικού ανηλίκων…*

[140] Άρθρο 348 Α παρ. 3 ΠΚ «Υλικό παιδικής πορνογραφίας, κατά την έννοια των προηγούμενων παραγράφων συνιστά η αναπαράσταση ή η πραγματική ή η εικονική αποτύπωση σε ηλεκτρονικό ή άλλο υλικό φορέα των γεννητικών οργάνων ή του σώματος εν γένει του ανηλίκου, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και της πραγματικής ή εικονικής γενετήσιας πράξης που διενεργείται από ή με ανήλικο»

[141] Βλ. Άρθρο 1 περ.β' «"παιδική πορνογραφία": το πορνογραφικό υλικό στο οποίο απεικονίζεται ή παριστάνεται: i) πραγματικό παιδί που συμμετέχει ή επιδίδεται σε πράξη με σαφή σεξουαλικό χαρακτήρα, συμπεριλαμβανομένης της άσεμνης επίδειξης των γεννητικών οργάνων ή της ηβικής χώρας παιδιού, ή ii) πραγματικό πρόσωπο που εμφανίζεται ως παιδί το οποίο συμμετέχει ή επιδίδεται στις αναφερόμενες στο σημείο i) πράξεις, ή iii) ρεαλιστικές εικόνες μη πραγματικού παιδιού που συμμετέχει ή επιδίδεται στις αναφερόμενες στο σημείο i) πράξεις», ·απόφαση-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου, της 22ας Δεκεμβρίου 2003, *για την καταπολέμηση της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας*, L 013 της 20/01/2004 [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32004F0068 Πρόσβασης στις 20-12-2021

[142] Βλ. Γ. Νούσκαλη (2020) *Κατοχή και διανομή/διάθεση πορνογραφικού υλικού ανηλίκων…*

[143] Επίσης ο ορισμός της παρ. 3 του άρθρου 348 Α ΠΚ σχετικά με το υλικό παιδικής πορνογραφίας αναφέρει και την αναπαράσταση εικονικής ασέλγειας, η οποία δεν αναφέρεται στον ανάλογο ορισμό του άρθρου 2 στοιχ. γ' της οδηγίας 2011/93/ ΕΕ, σύμφωνα με τον οποίο: « παιδική πορνογραφία»:i) κάθε υλικό στο οποίο απεικονίζεται παιδί να επιδίδεται σε πραγματική ή προσομοιωμένη πράξη σαφούς σεξουαλικού χαρακτήρα, ii) κάθε απεικόνιση, προς σεξουαλικούς κυρίως σκοπούς, των γεννητικών οργάνων παιδιού, iii) κάθε υλικό στο οποίο απεικονίζεται πρόσωπο που εμφανίζεται ως παιδί να επιδίδεται σε πραγματική ή προσομοιωμένη πράξη σαφούς σεξουαλικού χαρακτήρα ή κάθε απεικόνιση των γεννητικών οργάνων οποιουδήποτε προσώπου εμφανίζεται ως παιδί, προς σεξουαλικούς κυρίως σκοπούς, ή iv) ρεαλιστικές εικόνες παιδιού στις οποίες απεικονίζεται να επιδίδεται σε πράξη σαφούς σεξουαλικού χαρακτήρα ή ρεαλιστικές εικόνες των γεννητικών οργάνων παιδιού, προς σεξουαλικούς κυρίως σκοπούς·» …

Το διαδίκτυο μέσω του παγκόσμιου χαρακτήρα του συμβάλλει στην άμεση διάδοση και ανταλλαγή απόψεων και ιδεών ανάμεσα σε ανθρώπους σε βρίσκονται σε διαφορετικές περιοχές του κόσμου, η ανωνυμία, ωστόσο, που παρέχει εγκυμονεί απειλές και κινδύνους[144].

Ένας από τους μεγαλύτερους κινδύνους που απειλεί το διαδίκτυο αποτελεί η διασπορά του μισαλλόδοξου λόγου (*hatespeech*) από υπέρμαχους ακραίων ιδεολογικών προσεγγίσεων και απόψεων και η χωρίς έλεγχο πρόσβαση σε αυτόν από χρήστες όλων των ηλικιών, λόγω της έλλειψης ουσιαστικών ελεγκτικών μηχανισμών στον Κυβερνοχώρο[145].

Ο ορισμός για τον μισαλλόδοξο λόγο (*hatespeech*) που έχει αποδοθεί από την Επιτροπή Υπουργών του Συμβουλίου της Ευρώπης είναι ο εξής: « κάθε μορφή έκφρασης που διαδίδει, υποκινεί, προωθεί ή δικαιολογεί το ρατσιστικό μίσος, την ξενοφοβία, τον αντισημιτισμό ή άλλες μορφές μίσους που βασίζονται στη μισαλλοδοξία, συμπεριλαμβανομένων αυτής που εκφράζεται μέσω του επιθετικού εθνικισμού και εθνοκεντρισμού, των διακρίσεων και της εχθρότητας κατά των μειονοτήτων, των μεταναστών και των ανθρώπων με καταγωγή από την αλλοδαπή». Με τον όρο αυτό μπορεί να περιγραφεί μια συμπεριφορά ιδιαζόντως προσβλητική που μπορεί να θεωρηθεί μέχρι και απειλητική, όπως και σχόλια που τις περισσότερες φορές είναι χλευαστικά και υποτιμητικά[146].

Ο νόμος 4285/2014[147] ενσωμάτωσε στο ελληνικό δίκαιο την απόφαση-πλαίσιο 2008/913/ΔΕΥ[148], ενώ τροποποίησε τις διατάξεις του ν. 927/1979[149] στις οποίες

---

[144] Βλ. SafeInternet4Kids.gr [χ.χ.] Hate Speech, *Ρητορική Μίσους στο Διαδίκτυο*, [Διαδίκτυο] Διαθέσιμο στο: https://saferinternet4kids.gr/wp-content/uploads/2018/05/hate-speech-per-page.pdf Πρόσβαση στις 22-11-2021

[145] Βλ. SafeInternet4Kids.gr [χ.χ.] Hate Speech, *Ρητορική Μίσους στο Διαδίκτυο*...

[146] Βλ. SafeInternet4Kids.gr [χ.χ.] Hate Speech, *Ρητορική Μίσους στο Διαδίκτυο*...

[147]Βλ. Νόμο 4285/2014 - ΦΕΚ 191/Α/10-9-2014: *Τροποποίηση του ν. 927/1979 (Α' 139) και προσαρμογή του στην απόφαση πλαίσιο 2008/913/ΔΕΥ της 28ης Νοεμβρίου 2008, για την καταπολέμηση ορισμένων μορφών και εκδηλώσεων ρατσισμού και ξενοφοβίας μέσω του ποινικού δικαίου (L 328) και άλλες διατάξεις*[Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-anthropina-dikaiomata/n-4285-2014.html Πρόσβαση στις 20-12-2021

[148] Βλ. Απόφαση-Πλαίσιο 2008/913/ΔΕΥ του Συμβουλίου της 28ης Νοεμβρίου 2008 *για την καταπολέμηση ορισμένων μορφών και εκδηλώσεων ρατσισμού και ξενοφοβίας μέσω του ποινικού δικαίου* [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX:32008F0913 Πρόσβαση στις 22-12-2021

υπήρχε πρόβλεψη ποινικής τιμωρίας για πράξεις που ενδέχεται να οδηγήσουν σε διάκριση, εκδήλωση βίας ή μίσους εναντίον προσώπων εξαιτίας, μεταξύ άλλων, της φυλετικής τους καταγωγής ή της εθνικότητάς τους[150].

Η πλήρωση της αντικειμενικής υπόστασης του συγκεκριμένου εγκλήματος επέρχεται όταν κάποιος παρακινεί δημοσίως άλλο ή άλλα πρόσωπα να προβούν σε πράξεις που ενδεχομένως οδηγήσουν σε διακρίσεις εκδήλωση μίσους ή βίας «κατά προσώπου ή ομάδας προσώπων, που προσδιορίζονται με βάση τη φυλή, το χρώμα, τη θρησκεία, τις γενεαλογικές καταβολές, την εθνική ή εθνοτική καταγωγή, το σεξουαλικό προσανατολισμό, την ταυτότητα φύλου ή την αναπηρία»[151].

Περαιτέρω, η παρακίνηση πρέπει να γίνεται δημόσια, δηλαδή να μπορεί να ακούγεται και να έχει επιρροή σε οποιονδήποτε την ακούει, είτε σε δημόσιο είτε σε ιδιωτικό χώρο, να μπορεί να συμβεί με τη χρήση του διαδικτύου, ενώ δεν θεωρείται παρακίνηση η εκφορά γνώμης, ακόμη και επικριτικής ή μη ευπρόσδεκτης που αφορά τα ανωτέρω πρόσωπα[152].

Ακόμη, σχετικά με την υποκειμενική υπόσταση του εν λόγω εγκλήματος αυτή πληρούται με «τη γνώση και θέληση των στοιχείων της αντικειμενικής υπόστασης», σύμφωνα με το 'άρθρο 27 παρ. 1[153] ΠΚ[154]. Οι διατάξεις του ν. 927/1979 προστατεύουν το έννομο αγαθό που είναι το κατοχυρωμένο εκ του

---

[149] Νόμος 927/1979 - ΦΕΚ 139/Α/28-6-1979: *Περί κολασμού πράξεων ή ενεργειών αποσκοπουσών εις φυλετικάς διακρίσεις* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-anthropina-dikaiomata/n-927-1979.html Πρόσβαση στις 12-12-2021

[150] Βλ. Χ. Νάϊντου [χ.χ.] *Ιδιαιτερότητες στην ποινική αντιμετώπιση του ρατσισμού που εκδηλώνεται μέσω του διαδικτύου, σε :Δαλακούρα (επιμ.), Ηλεκτρονικό έγκλημα*, σελ. 113 επ.· Μ. Καϊάφα-Γκπάντι (2016) *Η ποινική καταστολή της ρατσιστικής ρητορίας, των εγκλημάτων ρατσισμού και της ρατσιστικής διάκρισης: προς μια ουσιαστική προστασία της αξίας του ανθρώπου* ΠοινΔικ σελ. 102 επ·Ε. Συμεωνίδου-Καστανίδου (2015*) Η ποινική αντιμετώπιση του ρατσισμού και της ξενοφοβίας στην Ελλάδα* ΠοινΧρ. σελ. 731 επ.·Ι. Ιγγλεζάκη (2015) *Ο μισαλλόδοξος λόγος στο διαδίκτυο και η ποινική αντιμετώπισή του με τον Ν.4285/2014* Συνήγορος 109/σελ. 64 επ.

[151] Βλ. ΑΠ 858/2020 ΝΟΜΟΣ ΤΝΠ

[152] Βλ. ΑΠ 858/2020 ΝΟΜΟΣ ΤΝΠ

[153] Άρθρο 27 παρ. 1 ΠΚ «*Με δόλο (με πρόθεση) πράττει όποιος θέλει την παραγωγή των περιστατικών που κατά το νόμο απαρτίζουν την έννοια κάποιας αξιόποινης πράξης· επίσης όποιος γνωρίζει ότι από την πράξη του ενδέχεται να παραχθούν αυτά τα περιστατικά και το αποδέχεται*»

[154] Βλ. Ολ. ΑΠ 3/2010 ΝΟΜΟΣ ΤΝΠ

Συντάγματος[155] δικαίωμα κάθε Έλληνα να απολαμβάνει ίση μεταχείριση, να αναπτύσσει ελεύθερα την προσωπικότητά του και να απαγορεύεται κάθε διάκρισης που σχετίζεται με το άτομό του (άρθρα 4 παρ. 1 και 5 παρ. 1 και 2 του Συντάγματος), ενώ και στο άρθρο 14[156] της ΕΣΔΑ υπάρχει πρόβλεψη για απαγόρευση διακρίσεων κατά την απόλαυση εκ μέρους των προσώπων των δικαιωμάτων και των ελευθεριών, οι οποίες έχουν αναγνωριστεί και αποτελούν αντικείμενο προστασίας από την εν λόγω Σύμβαση[157].

Με το μισαλλόδοξο λόγο (*hatespeech)* προωθείται η βία ή το μίσος που κατευθύνεται εναντίον ατόμων ή ομάδων με βάση συγκεκριμένα χαρακτηριστικά αυτών των προσώπων και κυρίως με τη φυλή, την προέλευση, το θρησκευτικό και σεξουαλικό προσανατολισμό, την ηλικία και το φύλο. Με τον μισαλλόδοξο λόγο, η επίθεση στρέφεται κατά του θύματος για κάτι που είναι ,και όχι για κάτι που κάνει[158].

Η κοινωνική αποξένωση και απομάκρυνση και οι διακρίσεις είναι κάποιες από τις επιπτώσεις του μισαλλόδοξου λόγου (*hatespeech)* που ως φαινόμενο πλήττει όλες τις κοινωνικές ομάδες, τόσο προσωπικά όσο και κοινωνικά. Επίσης, προκαλεί καταθλιπτική συμπεριφορά, αγχώδη διαταραχή, θυμό, επικίνδυνες για τη ζωή του θύματος ενέργειες, ενώ οδηγεί στην αναπαραγωγή της βίας. Ακόμη,

---

[155] Βλ. Άρθρο 4 παρ. 1 του Συντάγματος «Οι Έλληνες είναι ίσοι ενώπιον του νόμου» και άρθρο 5 παρ. 1 «Καθένας έχει δικαίωμα να αναπτύσσει ελεύθερα την προσωπικότητά του και να συμμετέχει στην κοινωνική, οικονομική και πολιτική ζωή της Χώρας, εφόσον δεν προσβάλλει τα δικαιώματα των άλλων και δεν παραβιάζει το Σύνταγμα ή τα χρηστά ήθη» και παρ. 2 «Όλοι όσοι βρίσκονται στην Ελληνική Επικράτεια απολαμβάνουν την απόλυτη προστασία της ζωής, της τιμής και της ελευθερίας τους, χωρίς διάκριση εθνικότητας, φυλής, γλώσσας και θρησκευτικών ή πολιτικών πεποιθήσεων. Εξαιρέσεις επιτρέπονται στις περιπτώσεις που προβλέπει το διεθνές δίκαιο. Απαγορεύεται η έκδοση αλλοδαπού που διώκεται για τη δράση του υπέρ της ελευθερίας» [Διαδίκτυο] Διαθέσιμο στο: https://www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/ Πρόσβαση στις 20-12-2021

[156] Βλ. Άρθρο 14 ΕΣΔΑ «Η χρήσις των αναγνωριζομένων εν τη παρούση Συμβάσει δικαιωμάτων και ελευθεριών δέον να εξασφαλισθή ασχέτως διακρίσεως φύλου, φυλής, χρώματος, γλώσσης, θρησκείας, πολιτικών ή άλλων πεποιθήσεων, εθνικής ή κοινωνικής προελεύσεως, συμμετοχής εις εθνικήν μειονότητα, περιουσίας, γεννήσεως ή άλλης καταστάσεως" [Διαδίκτυο] Διαθέσιμο στο: https://www.echr.coe.int/documents/convention_ell.pdf Πρόσβαση στις 28-11-2021

[157] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής*...σελ. 438

[158] Βλ. SafeInternet4Kids.gr [χ.χ.] *Hate Speech, Ρητορική Μίσους στο Διαδίκτυο...*

η ένταση που προκαλείται από τη ρητορική μίσους, έχει επιπτώσεις και στο κοινωνικό σύνολο, εκτός από τη βλάβη σε ατομικό επίπεδο[159].

Η απουσία κατάλληλης εκπαίδευσης σχετικά με τα ανθρώπινα δικαιώματα καθώς και η μη αποδοχή και η έλλειψη σεβασμού απέναντι στο διαφορετικό σαν κάτι που πρέπει να αντιμετωπίζεται ως ισότιμο, είναι οι βασικοί λόγοι εμφάνισης του μισαλλόδοξου λόγου[160].

ΚΕΦΑΛΑΙΟ ΠΕΜΠΤΟ

Η ΔΙΑΧΕΙΡΙΣΗ ΤΟΥ ΖΗΤΗΜΑΤΟΣ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΕΛΛΑΔΑ

5. 1 Το νομοθετικό πλαίσιο για την Κυβερνοασφάλεια

Στις διατάξεις του ν. 4070/2012[161] ρυθμίζονται οι υποχρεώσεις των παρόχων δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, σχετικά με την προστασία και την άρτια λειτουργία των τελευταίων. Ειδικότερα, όπως ορίζεται στο άρθρο 37 του ανωτέρω νόμου, οι πάροχοι έχουν υποχρέωση να λαμβάνουν όλα τα πρόσφορα μέτρα, τεχνικού και οργανωτικού χαρακτήρα, προκειμένου να διασφαλιστεί ότι η διαχείριση των κινδύνων γίνεται με τον καταλληλότερο τρόπο, αναφορικά με την ασφάλεια των δικτύων και των υπηρεσιών[162]. Επίσης, το επίπεδο ασφαλείας που παρέχουν αυτά τα μέτρα πρέπει να είναι αντίστοιχα

---

[159] Βλ. . SafeInternet4Kids.gr [χ.χ.] *Hate Speech, Ρητορική Μίσους στο Διαδίκτυο...*

[160] Βλ. SafeInternet4Kids.gr [χ.χ.] *Hate Speech*, Ρητορική Μίσους στο Διαδίκτυο...

[161] Νόμος 4070/2012 - ΦΕΚ 82 Α/10-4-2012: *Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/n-4070-2012.html Πρόσβαση στις 28-12-2021

[162] Βλ. Law&Tech (2020) *Το Νομικό Πλαίσιο για την Ασφάλεια των Δικτύων / Υπηρεσιών Ηλεκτρονικών Επικοινωνιών* [Διαδίκτυο] Διαθέσιμο στο: https://lawandtech.eu/2020/04/27/%CF%80%CE%BF%CE%B9%CE%BF-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-%CE%BD%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C-%CF%80%CE%BB%CE%B1%CE%AF%CF%83%CE%B9%CE%BF-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B7%CE%BD-%CE%B1%CF%83/ Πρόσβαση στις 28-12-2021

με τον υφιστάμενο κίνδυνο, ενώ τα μέτρα αυτά να πρέπει είναι τόσο μέτρα αποτροπής των κινδύνων όσο και ελαχιστοποίησης των συνεπειών από συμβάντα ασφαλείας που έχουν επιπτώσεις στους χρήστες και στα δίκτυα[163].

Στη συνέχεια, οι πάροχοι πρέπει να λαμβάνουν τα αναγκαία μέτρα που θα εξασφαλίσουν την αρτιότητα των δικτύων, ώστε η παροχή των υπηρεσιών αυτών των δικτύων να μην παρακωλύεται και να παραμένει συνεχής. Μάλιστα, η οποιασδήποτε μορφής παραβίαση της ασφάλειας ή της ακεραιότητας των δικτύων που επηρέασε σημαντικά τη λειτουργία τους θα πρέπει να αναφέρεται από τους παρόχους στην ΕΕΤΤ, η οποία ακολούθως οφείλει να γνωστοποιεί κάθε παράβαση σχετικά με την ασφάλεια ή την ακεραιότητα στην Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών[164].

Παραπέρα, στις αρμοδιότητες της ΑΔΑΕ, η οποία συστάθηκε με το άρθρο 1 ν. 3115/2003[165] περιλαμβάνεται ο τακτικός και έκτακτος έλεγχος των επιχειρήσεων, ο έλεγχος τήρησης της νομοθεσίας για την άρση του απορρήτου, η επιβολή διοικητικών κυρώσεων σε περίπτωση παραβιάσεων της σχετικής νομοθεσίας, ο έλεγχος καταγγελιών που αφορούν την παραβίαση του απορρήτου των επικοινωνιών, η έκδοση κανονιστικών διοικητικών πράξεων σχετικά με την προστασία του απορρήτου των επικοινωνιών καθώς και η έκδοση γνωμοδοτήσεων και συστάσεων που άπτονται της αρμοδιότητάς της[166].

---

[163] Βλ. Law&Tech (2020) *Το Νομικό Πλαίσιο για την Ασφάλεια των Δικτύων / Υπηρεσιών Ηλεκτρονικών Επικοινωνιών*..

[164] Βλ. Law&Tech (2020) *Το Νομικό Πλαίσιο για την Ασφάλεια των Δικτύων / Υπηρεσιών Ηλεκτρονικών Επικοινωνιών*..

[165] Βλ. Άρθρο 1 «Συνιστάται, κατά την παράγραφο 2 του άρθρου 19 του Συντάγματος, Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.), με σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου", ν. 3115/2003-ΦΕΚ 47/Α/2722003: *Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/n-3115-2003.html Πρόσβαση στις 28-12-2021

[166] Βλ. Law&Tech (2020) *Το Νομικό Πλαίσιο για την Ασφάλεια των Δικτύων / Υπηρεσιών Ηλεκτρονικών Επικοινωνιών*...

Το 2013 η ΑΔΑΕ με την απόφασή της 205/2013[167] εξειδίκευσε το περιεχόμενο των διατάξεων του άρθρου 37 ν. 4070/2012 που αφορούν την ασφάλεια και την ακεραιότητα των δικτύων και των υπηρεσιών ηλεκτρονικών επικοινωνιών, προβλέποντας τις υποχρεώσεις που οφείλουν να εκπληρώνουν οι πάροχοι[168].

Στη συνέχεια, ακολούθησε, ο ν. 4577/2018[169] που ενσωμάτωσε την Οδηγία 2016/1148/ΕΕ , με την οποία θεσπίστηκε το νομικό πλαίσιο για την εξασφάλιση υψηλού επιπέδου προστασία στα συστήματα δικτύου και πληροφοριών, με στόχο τη βελτίωση της εσωτερικής αγοράς της ΕΕ. Σύμφωνα με όσα ορίζει η διάταξη του άρθρου 3 παρ. 2[170], αντικείμενο του ανωτέρω νόμου αποτελεί η ασφαλής λειτουργία και προστασία των συστημάτων δικτύου και πληροφοριών.

---

[167] Βλ. Απόφαση Α.Δ.Α.Ε. 205/2013 - ΦΕΚ 1742/Β/15-7-2013: *Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/apophase-adae-205-2013.html Πρόσβαση στις 28-12-2021

[168] Βλ. Law&Tech (2020) *Το Νομικό Πλαίσιο για την Ασφάλεια των Δικτύων / Υπηρεσιών Ηλεκτρονικών Επικοινωνιών*, όπου μεταξύ των υποχρεώσεων αυτών περιλαμβάνονται: «Κατάρτιση/Σχεδιασμός και τήρηση πολιτικής ασφάλειας δικτύων και υπηρεσιών, διορισμός υπευθύνου ασφάλειας δικτύων και υπηρεσιών, κατάρτιση/δημιουργία και τήρηση σχεδίου έκτακτων αναγκών, συμμόρφωση με πρότυπα ασφαλείας, τεχνικές διεπαφές και στοιχεία λειτουργίας δικτύων που συμφωνούνται σε Ενωσιακό επίπεδο, ανάλυση επιχειρησιακών επιπτώσεων και αξιολόγησης επικινδυνότητας αναφορικά με την ασφάλεια και την ακεραιότητα των δικτύων, κατάρτιση/δημιουργία/οργάνωση και τήρηση σχεδίου επιχειρησιακής συνέχειας/αδιάλειπτης λειτουργίας, Διεξαγωγή ελέγχων αποτελεσματικότητας και κατάρτιση σχετικών σχεδίων και διαδικασιών (δοκιμών, penetration tests, vulnerability assessments), τήρηση κατάλληλων μέτρων φυσικής και λογικής/πληροφοριακής? ασφάλειας, σχεδιασμός/ Επιλογή και τήρηση διαδικασίας διαχείρισης περιστατικών ασφαλείας, Σχεδιασμός/ επιλογή και τήρηση διαδικασίας εσωτερικού ελέγχου για την ασφάλεια και την ακεραιότητα των δικτύων / υπηρεσιών, τήρηση σχετικών αρχείων»

[169] Νόμος 4577/2018 - ΦΕΚ 199/Α/3-12-2018: *Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-nomothesia-genikou-endiapherontos/nomos-4577-2018-phek-199a-3-12-2018.html Πρόσβαση στις 28-12-2021

[170] Βλ. Άρθρο 3 παρ. 2 «ασφάλεια συστημάτων δικτύου και πληροφοριών»: η ικανότητα συστημάτων δικτύου και πληροφοριών να ανθίστανται, με δεδομένο βαθμό αξιοπιστίας, σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών»

Περαιτέρω, στις διατάξεις του ν. 4577/2018 γίνεται αναφορά σε απαιτήσεις ασφαλείας και κοινοποίησης με τις οποίες πρέπει να συμμορφώνονται αποκλειστικά οι φορείς που εκμεταλλεύονται την παροχή βασικών υπηρεσιών, και όσοι παρέχουν υπηρεσίες ψηφιακής τεχνολογίας σε υψηλής σημασίας φορείς. Δεν απαιτείται συμμόρφωση με αυτές τις απαιτήσεις από επιχειρήσεις που είναι πάροχοι δημόσιων δικτύων ή δημόσιες υπηρεσίες ηλεκτρονικών επικοινωνιών, είτε στην Ελλάδα είτε σε άλλη χώρα μέλος της ΕΕ, ή είναι πάροχοι υπηρεσιών «εμπιστοσύνης» και καλύπτονται από τη διάταξη του άρθρου 19 του Κανονισμού (ΕΕ) 910/2014[171][172].

Επίσης, σε ισχύ βρίσκεται το Π.Δ. 39/2011[173] με το οποίο θεσπίστηκε «διαδικασία προσδιορισμού των ευρωπαϊκών υποδομών ζωτικής σημασίας και αξιολόγησης της ανάγκης προστασίας των υποδομών αυτών», καθώς και οι διατάξεις σχετικά με το έγκλημα της παιδικής πορνογραφίας και του ν.4360/2016[174].

Το 2019 με την Υπουργική Απόφαση 1027/04-10-2019[175] τέθηκαν αντικειμενικά κριτήρια για τον «ορισμό «των υπόχρεων φορέων βασικών υπηρεσιών» που προβλέπει ο ν. 4577/2018 και ορίζει τις υποχρεώσεις αυτών των

---

[171] Βλ. Ι. Ιγγλεζάκη (2021) *Δίκαιο Πληροφορικής*.. σελ. 452

[172] Βλ. Κανονισμός (ΕΕ) αριθ.910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 *σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ,* [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32014R0910 Πρόσβαση στις 28-12-2021

[173] Βλ. Προεδρικό Διάταγμα υπ' αριθμ. 39, τεύχος πρώτο, αρ. φύλλου 104, 6 Μαΐου 2011: *Προσαρμογή της ελληνικής νομοθεσίας προς τις διατάξεις της Οδηγίας 2008/114/ΕΚ του Συμβουλίου της 8ης Δεκεμβρίου 2008 «σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους»(L 345/23–12–2008*) [Διαδίκτυο] Διαθέσιμο στο: http://www.kemea.gr/images/documents/pd39-2011.pdf Πρόσβαση στις 28-12-2021

[174] Βλ. Νόμος 4360/2016 - ΦΕΚ 9/Α/29-1-2016: *Ενσωμάτωση στην εθνική νομοθεσία: της Οδηγίας 2011/99/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 2011, περί της ευρωπαϊκής εντολής προστασίας, της απόφασης πλαίσιο 2009/315/ΔΕΥ του Συμβουλίου της 26ης Φεβρουαρίου 2009,* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-dikasteria-dikaiosune/nomos-4360-2016.html Πρόσβαση στις 28-12-2021

[175] Βλ. Υπουργική Απόφαση 1027/2019 - ΦΕΚ 3739/Β/8-10-2019:*Θέματα εφαρμογής και διαδικασιών του ν. 4577/2018 (Α 199)* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/upourgike-apophase-1027-2019-phek-3739b-8-10-2019.html Πρόσβαση στις 28-12-2021

παρόχων. Ειδικότερα, προβλέπεται : α)ευθύνη των οργανισμών για τις πράξεις ή παραλείψεις των συνεργατών που αυτοί οι οργανισμοί χρησιμοποιούν για διάφορες λειτουργίες των συστημάτων τους, β) υποχρέωση των οργανισμών για σχεδιασμό στρατηγικής ασφάλειας, γ) υποχρέωση των οργανισμών για σχεδιασμό ενός πλαισίου βασικών αναγκών ασφάλειας, προσανατολισμένο στις συγκεκριμένες ανάγκες και κινδύνους, δ) υποχρέωση των οργανισμών αντιμετώπισης των περιστατικών ασφάλειας και γνωστοποίησης αυτών στο CSIRT, στην Εθνική Αρχή Κυβερνοασφάλειας και στο κοινό[176].

5.2 Η ίδρυση της Εθνικής Αρχής Κυβερνοασφάλειας

Με το Προεδρικό Διάταγμα 82/2017[177] συστάθηκε η Εθνική Αρχή Κυβερνοασφάλειας που διαθέτει διευρυμένες αρμοδιότητες, παρακολουθεί και θέτει σε εφαρμογή και είναι υπεύθυνη για την Εθνική Στρατηγική Κυβερνοασφάλειας[178].

Στο έργο της η Εθνικής Αρχής Κυβερνοασφάλειας υποστηρίζεται από ένα «Εθνικό Συμβουλευτικό Όργανο, το οποίο απαρτίζεται από δημόσιους και ιδιωτικούς φορείς, ενώ προβλέπεται και συνεργασία με το εθνικό *Computer Emergency Response Team*[179].

[176] Βλ. Law&Tech (2020) *Το Νομικό Πλαίσιο για την Ασφάλεια των Δικτύων / Υπηρεσιών Ηλεκτρονικών Επικοινωνιών...*

[177] Βλ. Προεδρικό Διάταγμα 82/2017 - ΦΕΚ 117/Α/10-8-2017: *Οργανισμός του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/enemerose-tupos-radiophono-teleorase/proedriko-diatagma-82-2017-fek-117a-10-8-2017.html Πρόσβαση στις 28-12-2021

[178] Βλ. Υπουργική Απόφαση 3218/2018 ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας,* [Διαδίκτυο] Διαθέσιμο στο: https://mindigital.gr/wp-content/uploads/2020/01/NCSSGR.pdf Πρόσβαση στις 15-12-2021

[179] Βλ. Υπουργική Απόφαση 3218/2018,ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας...

Η Εθνική Αρχή Κυβερνοασφάλειας είναι αρμόδια για την παρακολούθηση, τη διεύθυνση και την αξιολόγηση του έργου των φορέων που εμπλέκονται στην υλοποίηση των στρατηγικών σχεδιασμών[180].

Ειδικότερα, στα πλαίσια των αρμοδιοτήτων της η Εθνική Αρχή Κυβερνοασφάλειας: α) παρακολουθεί και αξιολογεί την εφαρμογή του ν. 4577/2018 από τις επιχειρήσεις που οφείλουν να συμμορφώνονται με αυτόν, β) απαιτεί από τις ανωτέρω επιχειρήσεις να παράσχουν τα αναγκαία στοιχεία, συμπεριλαμβανομένων των στρατηγικών που αφορούν την ασφάλεια, γ) απαιτεί από τις συγκεκριμένες επιχειρήσεις να προβαίνουν σε διορθωτικές κινήσεις σχετικά με οποιαδήποτε παράλειψή τους να συμμορφωθούν, δ) διενεργεί επί τόπου ελέγχους στις εν λόγω επιχειρήσεις[181].

5.3 Ο σχεδιασμός και οι στόχοι της Εθνικής Στρατηγικής Κυβερνοασφάλειας

Βασικός πυλώνας στήριξης της εθνικής οικονομίας αποτελεί η ανάπτυξη και προστασία των υπηρεσιών ψηφιακής τεχνολογίας, η οποία κινείται σε ανταγωνιστικό πλαίσιο σε εθνικό και Ευρωπαϊκό επίπεδο[182].

Στους βασικούς κανόνες της Εθνικής Στρατηγικής Κυβερνοασφάλειας περιλαμβάνονται:

1)Η ανάπτυξη και η σταθεροποίηση ενός Κυβερνοχώρου που θα λειτουργεί με ασφάλεια και υπό το πλαίσιο εθνικών, ευρωπαϊκών και διεθνών αρχών, και κατάλληλων πρακτικών, και στον οποίο τόσο οι πολίτες όσο και οι ιδιωτικοί και δημόσιοι φορείς θα αναπτύσσουν τις δραστηριότητές τους και θα αλληλεπιδρούν με ασφάλεια, συμμορφούμενοι με τις αρχές του κράτους δικαίου

[180] Βλ. Υπουργική Απόφαση 3218/2018,. ΑΔΑ:*Ψ4Ρ7465ΧΘ0-Ζ6Ω: Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας…*

[181] Βλ. Law&Tech (2020) *Το Νομικό Πλαίσιο για την Ασφάλεια των Δικτύων / Υπηρεσιών Ηλεκτρονικών Επικοινωνιών…*

[182] Βλ. Υπουργική Απόφαση 3218/2018, ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας…*

2) Η διαρκής βελτίωση των ικανοτήτων για παροχή προστασίας έναντι κυβερνοεπιθέσεων, εστιάζοντας στις βασικές υποδομές και στην εξασφάλιση της επιχειρησιακής διάρκειας

3) Η ενισχυμένη θεσμική προστασία του εθνικού πλαισίου Κυβερνοασφάλειας, για την αποτελεσματικότερη διαχείριση των κυβερνοεπιθέσεων και την μείωση των συνεπειών από κυβερνοαπειλές

4) Η καλλιέργεια παιδείας σχετικά με την προστασία των πολιτών, του ιδιωτικού και δημόσιου τομέα, αξιοποιώντας τις ικανότητες ατόμων από τον ακαδημαϊκό χώρο καθώς και άλλων φορέων από τον ιδιωτικό και δημόσιο τομέα[183].

Η εφαρμογή της Εθνικής Στρατηγικής Κυβερνοασφάλειας υλοποιείται μέσα από ένα πλέγμα δράσεων:

1) Καθορισμός των φορέων, του δημόσιου και ιδιωτικού τομέα, που λαμβάνουν μέρος στην Εθνική Στρατηγική Κυβερνοασφάλειας και θα συμβάλλουν στην πραγμάτωση της εθνικής στρατηγικής[184]

2) Καθορισμός των κρίσιμων υποδομών και στο δημόσιο όσο και στον ιδιωτικό χώρο και εντοπισμός των εξαρτήσεων αναμεσά τους[185]

3) Αξιολόγηση της επικινδυνότητας σε εθνικό επίπεδο, μέσω πραγματοποίησης μελέτης σχετικά με την εκτίμηση της ανωτέρω επικινδυνότητας, η οποία στηρίζεται στην αναγνώριση, ερμηνεία και εκτίμηση των συνεπειών που απορρέουν από τους κινδύνους και καταλήγει στον σχεδιασμό ενός πλάνου προστασίας των κρίσιμων υποδομών ανά φορέα[186]

4) Καταγραφή, εκτίμηση και αναβάθμιση του νομοθετικού πλαισίου για την Κυβερνοασφάλεια, το οποίο επισημαίνει τα σημεία που δεν είναι επαρκώς

[183] Βλ. Υπουργική Απόφαση 3218/2018, ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας...*

[184] Βλ. Υπουργική Απόφαση 3218/2018, ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας...*

[185] Βλ. Υπουργική Απόφαση 3218/2018, ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας...*

[186] Βλ. Υπουργική Απόφαση 3218/2018, ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας...*

καλυμμένα, αλλά και εκείνα που πρέπει να βελτιωθούν και να συντονιστούν πιο αποτελεσματικά[187]

5) Κατάρτιση σχεδίου έκτακτης ανάγκης για τον Κυβερνοχώρο, το οποίο θα προσδιορίζει τα μέτρα για τη διαχείριση των σημαντικών συμβάντων που τελούνται σε κρίσιμα συστήματα πληροφορικής και επικοινωνιών των φορέων που είναι μέλη της Εθνικής Στρατηγικής Κυβερνοασφάλειας και θα αποκαθιστά τις παροχές αυτών των φορέων στο κοινωνικό σύνολο[188]

6) Προσδιορισμός των βασικών απαιτήσεων που αφορούν την ασφάλεια, όπου οι φορείς της Εθνικής Στρατηγικής Κυβερνοασφάλειας πρέπει να προβαίνουν στη λήψη των τεχνικών και οργανωτικών μέτρων που εξασφαλίζουν ότι η λειτουργία των συστημάτων πληροφοριών και επικοινωνίας είναι προστατευμένη και ανεμπόδιστη και να μειώνουν στο ελάχιστο τις συνέπειες ενός συμβάντος ασφαλείας[189]

7) Διαχείριση συμβάντων ασφαλείας, στο πλαίσιο της οποίας οι φορείς της Εθνικής Στρατηγικής Κυβερνοασφάλειας πρέπει να παραμένουν σε ετοιμότητα να προχωρήσουν σε δραστικές κινήσεις[190]

8) Οργάνωση ασκήσεις ετοιμότητας σε εθνικό επίπεδο, οι οποίες λειτουργούν ως ένα μέσο αξιολόγησης του επιπέδου εγρήγορσης των εμπλεκόμενων φορέων και εντοπίζουν τα αδύναμα σημεία των συστημάτων[191]

9) Ευαισθητοποίηση των χρηστών όσον αφορά τις απειλές και τις αδυναμίες της Κυβερνοασφάλειας, μέσω προγραμμάτων ενημέρωσης για τους χρήστες των εμπλεκόμενων φορέων της Εθνικής Στρατηγικής Κυβερνοασφάλειας, αλλά και για τους πολίτες γενικά, στα οποία ισχυροποιούνται οι γνώσεις γύρω από τους κινδύνους που υποκρύπτει ο χώρος του διαδικτύου, με αποτέλεσμα την ενίσχυση

---

[187] Βλ. Υπουργική Απόφαση 3218/2018, ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας...*

[188] Βλ. Υπουργική Απόφαση 3218/2018, ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας...*

[189] Βλ. Υπουργική Απόφαση 3218/2018, ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας...*

[190] Βλ. Υπουργική Απόφαση 3218/2018, ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας...*

[191] Βλ. Υπουργική Απόφαση 3218/2018, ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας...*

της ασφάλειας έναντι κοινών απειλών, κάτι που θα οδηγήσει σε αύξηση του επιπέδου Κυβερνοασφάλειας στη χώρα[192]

10) Προσδιορισμός μηχανισμών φερεγγυότητας κατά την ανταλλαγή των πληροφοριών, όπου, καταρχήν, οι φορείς του ιδιωτικού τομέα ανταλλάσσουν πληροφορίες σχετικά με τη λειτουργία των συστημάτων επικοινωνιών και πληροφορικής, τη στρατηγική προστασίας που έχουν εφαρμόσει, τα τρωτά σημεία, τις απειλές και τα συμβάντα ασφαλείας που καλούνται να διαχειριστούν, και κατά δεύτερον, οι φορείς του δημόσιου τομέα ανταλλάσσουν πληροφορίες που έχουν συλλεγεί από τους ίδιους και οι οποίες πιθανόν να είναι επικίνδυνες για την Κυβερνοασφάλεια[193]

11) Συνδρομή σε ερευνητικά και αναπτυξιακά προγράμματα και εκπαιδευτικά προγράμματα, με τα οποία ενισχύεται ο τομέας της Κυβερνοασφάλειας της χώρας, ο οποίος βρίσκεται υπό διαρκή εξέλιξη, από πλευράς υψηλών τεχνικών γνώσεων[194]

12) Σύναψη συνεργασιών σε διεθνές επίπεδο, στο πλαίσιο των οποίων ανταλλάσσονται εμπειρίες και τεχνικές και εξετάζεται η πιθανότητα κοινής ανάπτυξης πρόσφορων μέσων, με στόχο τη διαχείριση των απειλών που σχετίζονται με την προστασία του Κυβερνοχώρου[195]

13) Εκτίμηση και τροποποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας όπου την πραγματοποίηση των στόχων της εποπτεύει η Εθνική Αρχή Κυβερνοασφάλειας που παρακολουθεί τα διεθνή μοντέλα, ώστε να εφαρμόζει καλύτερες πρακτικές τις οποίες αργότερα προτείνει να εφαρμόσουν οι φορείς αργότερα[196] .

Το Μάριο του 2018, έπειτα από σχετική πρόταση της Εθνικής Αρχής

---

[192] Βλ. Υπουργική Απόφαση 3218/2018, ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας…*

[193] Βλ. Υπουργική Απόφαση 3218/2018, ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας…*

[194] Βλ. Υπουργική Απόφαση 3218/2018, ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας…*

[195] Βλ. Υπουργική Απόφαση 3218/2018, ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας…*

[196] Βλ. Υπουργική Απόφαση 3218/2018, ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας…*

Κυβερνοασφάλειας αναθεωρήθηκε η Εθνική Στρατηγική Κυβερνοασφάλειας[197]. Τα κύρια σημεία της νέας Εθνικής Στρατηγικής Κυβερνοασφάλειας αναφέρουν μεταξύ άλλων ότι οι δράσεις της Εθνικής Στρατηγικής έχουν στόχο να προστατεύσουν τους πολίτες και τις υποδομές των φορέων, αποτελώντας το θεμέλιο για την ψηφιακή διακυβέρνηση και την πρόοδο της χώρας. Επιπλέον, οι κυβερνοαπειλές που πιθανόν έχουν αντίκτυπο στην επιχειρησιακή διάρκεια και πορεία της Δημόσιας Διοίκησης και άλλων φορέων που εμπλέκονται, εντοπίζονται, καταγράφονται, κατατάσσονται σε κατηγορίες και αντιμετωπίζονται επιμελώς. Ακόμη, η νέα Στρατηγική αντιμετωπίζει με ιδιαίτερη προσοχή τα ανθρώπινα δικαιώματα και προστατεύει την ανθρώπινη ζωή. Επίσης, τα μέτρα που λαμβάνει η Αρχή Κυβερνοασφάλειας και οι εμπλεκόμενοι φορείς αποσκοπούν στην εξασφάλιση της προστασίας των πολιτών σε συνάρτηση με την τήρηση των υφιστάμενων κανόνων και ρυθμίσεων[198].

Υπό την προοπτική των ανωτέρω αρχών, το όραμα για τη νέα Εθνική Στρατηγική Κυβερνοασφάλειας διατυπώνεται ως εξής: «Ένα σύγχρονο και ασφαλές ψηφιακό περιβάλλον πληροφοριακών και δικτυακών υποδομών, εφαρμογών και υπηρεσιών προς όφελος της οικονομικής και κοινωνικής ευημερίας, με την εγγύηση της προστασίας των θεμελιωδών δικαιωμάτων των πολιτών, την ανάπτυξη κουλτούρας ασφαλούς χρήσης των ψηφιακών υπηρεσιών και εφαρμογών, και την επαύξηση της εμπιστοσύνης των πολιτών και επιχειρήσεων στις ψηφιακές τεχνολογίες.»[199].

---

[197] Βλ. Ελληνική Δημοκρατία. Υπουργείο Ψηφιακής Διακυβέρνησης (2020) Εθνική Αρχή Κυβερνοασφάλειας, *Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025* σελ. 16 [Διαδίκτυο]Διαθέσιμο στο: https://mindigital.gr/wp-content/uploads/2020/12/%CE%95%CE%B8%CE%BD%CE%B9%CE%BA%CE%B7%CC%81-%CE%A3%CF%84%CF%81%CE%B1%CF%84%CE%B7%CE%B3%CE%B9%CE%BA%CE%B7%CC%81-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%B1%CC%81%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf Πρόσβαση στις 10-11-2021

[198] Βλ. Ελληνική Δημοκρατία. Υπουργείο Ψηφιακής Διακυβέρνησης (2020) Εθνική Αρχή Κυβερνοασφάλειας *Εθνική Στρατηγική Κυβερνοασφάλειας* σελ. 18...

[199] Βλ. Ελληνική Δημοκρατία. Υπουργείο Ψηφιακής Διακυβέρνησης (2020) Εθνική Αρχή Κυβερνοασφάλειας, *Εθνική Στρατηγική Κυβερνοασφάλειας* σελ. 18...

5.4 Η Ελλάδα αντιμέτωπη με νέες προκλήσεις στον τομέα της Κυβερνοασφάλειας

Καθώς η τεχνολογία εξελίσσεται συνεχώς, η επικινδυνότητα του κυβερνοχώρου αυξάνεται. Ο κίνδυνος ελλοχεύει όχι μόνο για τα συστήματα που περιέχουν πληροφορίες που αφορούν ένα κράτος, αλλά και για τους πολίτες. Οι νέες απειλές που εμφανίζονται κάθε χρόνο συνιστούν μια πρόκληση για την κυβερνοασφάλεια, η οποία πρέπει να αντιμετωπιστεί[200].

Μια μορφή απάτης που έχει κατακλύσει σχεδόν τον Κυβερνοχώρο είναι τα deepfakes. Πρόκειται για ψεύτικες ειδήσεις ή κατασκευασμένες αναρτήσεις, ακόμα και μέσω μοντάζ ή Τεχνητής Νοημοσύνης, που χρησιμοποιούνται για να πειστούν όλοι ότι ένα αναγνωρίσιμο πρόσωπο προκρίνει μια συγκεκριμένη υπηρεσία. Τελευταία, τέτοιας μορφής απάτες έκαναν την εμφάνισή τους και στην Ελλάδα από τα μέσα κοινωνικής δικτύωσης, σχετικά με γνωστούς ηθοποιούς, παρουσιαστές και άλλα πρόσωπα που πλούτισαν μέσω «κρυπτονομισμάτων»[201].

Ακόμη, προβληματισμό έχει προκαλέσει στους ειδικούς η άνοδος του 5G, την οποία αναγνωρίζουν ως μια αφορμή για την εκδήλωση νέων απειλών από κακόβουλους χρήστες[202]. Είναι γνωστό ότι, τα δίκτυα 5G είναι σημαντικά όχι μόνο για την ψηφιακή επικοινωνία, αλλά και για τομείς ζωτικής σημασίας, όπως ο τομέας της ενέργειας, των μεταφορών, των χρηματοπιστωτικών υπηρεσιών και

---

[200] Βλ. Ε. Μεϊμάρογλου (2020), 'Η κυβερνοασφάλεια στην Ελλάδα: Αποσαφήνιση όρων και νέες,προκλήσει'ς', *ΟΔΕΘ*, 9 Σεπτεμβρίου. [Διαδίκτυο] Διαθέσιμο στο: https://odeth.eu/%CE%B7-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1-%CF%83%CF%84%CE%B7%CE%BD-%CE%B5%CE%BB%CE%BB%CE%AC%CE%B4%CE%B1-%CE%B1%CF%80%CE%BF%CF%83%CE%B1%CF%86/ Πρόσβαση στις 22-12-2021

[201] Βλ. Ε. Μεϊμάρογλου (2020), 'Η κυβερνοασφάλεια στην Ελλάδα: Αποσαφήνιση όρων και νέες,προκλήσεις'...

[202] Βλ. Ε. Μεϊμάρογλου (2020), 'Η κυβερνοασφάλεια στην Ελλάδα: Αποσαφήνιση όρων και νέες,προκλήσεις'...

των υπηρεσιών υγείας. Επομένως, είναι αποφασιστικής σημασίας να επιτευχθεί η ανθεκτικότητα αυτών των δικτύων[203].

Τέλος, έντονη ανησυχία επικρατεί από τη διάδοση του *ransomware,* το οποίο σχετίζεται με μια μορφή κακόβουλου λογισμικού που απειλεί να ανακοινώσει δημοσίως τα δεδομένα του θύματος ή του απαγορεύει την πρόσβαση σε αυτά, αν δεν καταβληθούν λύτρα. Μάλιστα, σε επίπεδο επιχειρήσεων, το *ransomware* ενδεχομένως να υφαρπάζει ευαίσθητα δεδομένα που μια εταιρεία δεν επιθυμεί να γνωρίζουν τρίτοι[204].

ΚΕΦΑΛΑΙΟ ΕΚΤΟ
Η ΕΥΡΩΠΑΙΚΗ ΕΝΩΣΗ ΑΠΕΝΑΝΤΙ ΣΤΗΝ ΠΡΟΚΛΗΣΗ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

6.1 Οι πρωτοβουλίες της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια

Η εποχή της ψηφιοποίησης είναι πλέον πραγματικότητα, καθώς η ψηφιακή τεχνολογία βρίσκει εφαρμογή σε όλο και περισσότερους τομείς του σύγχρονου πολιτισμού. Αν και τα οφέλη της «ψηφιοποίηση»ς είναι πολλά και σημαντικά για πολλούς χώρους όπως η υγεία, η εκπαίδευση και η οικονομία, η έκθεση αυτών σε κυβερνοαπειλές παραμένει και απαιτείται συντονισμένη προσπάθεια αντιμετώπισής τους[205]. Στο ίδιο πλαίσιο κινείται και η Ευρωπαϊκή Ένωση, η οποία λαμβάνοντας υπόψη τις εξελίξεις στο διεθνή χώρο, λαμβάνει

---

[203] Βλ. Ευρωπαϊκό Συμβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης. [χ.χ.] *Κυβερνοασφάλεια: Πώς αντιμετωπίζει η ΕΕ τις κυβερνοαπειλές*, [Διαδίκτυο] Διαθέσιμο στο: https://www.consilium.europa.eu/el/policies/cybersecurity/ Πρόσβαση στις 29-12-2021

[204] Βλ. Ε. Μεϊμάρογλου (2020 Η κυβερνοασφάλεια στην Ελλάδα: Αποσαφήνιση όρων και νέες, προκλήσεις'...

[205] Βλ. Μ. Γερονικολού (2021), 'Η εξέλιξη της κυβερνοασφάλειας στην ΕΕ',*ΟΔΕΘ*, 15 Ιουλίου. [Διαδίκτυο] Διαθέσιμο στο: https://odeth.eu/%CE%B7-%CE%B5%CE%BE%CE%AD%CE%BB%CE%B9%CE%BE%CE%B7-%CF%84%CE%B7%CF%82-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82-%CF%83%CF%84%CE%B7%CE%BD-%CE%B5/ Πρόσβαση στις 20-11-2021

μέτρα υπέρ της Κυβερνοασφάλειας, θέτοντάς την ως κύρια προτεραιότητα στον καθορισμό των πολιτικών της[206].

Πιο συγκεκριμένα, ήδη από τις αρχές του 2000, η ασφάλεια έναντι κυβερνοεπιθέσεων ήταν ένας τομέας ενδιαφέροντος για την ΕΕ, η οποία, ωστόσο, άρχισε να δραστηριοποιείται πιο ενεργά προς αυτή την κατεύθυνση από το 2004 και έπειτα. Τότε, με τον Κανονισμό 460/2004 συστάθηκε ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, γνωστός ως ENIISA Στη συνέχεια, η πρώτη πρωτοβουλία της ΕΕ σχετικά με την ασφάλεια των δικτύων εκδόθηκε δύο δυο χρόνια αργότερα, την οποία αντικατέστησε η «Στρατηγική για την Κυβερνοασφάλεια», το 2013. Η τελευταία ήταν αποτέλεσμα μιας μακρόχρονης πορείας διαβουλεύσεων και χρησιμοποίησε ως βάση την «Ψηφιακή Ατζέντα για την Ευρώπη» του 2010. Η στρατηγική, η οποία έθεσε τα θεμέλια για την ευρωπαϊκή Κυβερνοασφάλεια, ήταν η πρόληψη και η διαχείριση των αδυναμιών και ελλείψεων των ευρωπαϊκών συστημάτων τηλεπικοινωνιών[207].
Παράλληλα, οι πέντε αρχές σχετικά με τον κυβερνοχώρο στις οποίες στηρίζεται η στρατηγική αφορούν την ικανότητα διαχείρισης των κυβερνοεπιθέσεων, την ελαχιστοποίηση των κυβερνοεγκλημάτων, την πρόοδο σε θέματα πολιτικής «κυβερνοάμυνας» και δυνατοτήτων που συνδέονται με την Κοινή Πολιτική Ασφάλειας και Άμυνας (ΚΠΑΑ), την ανάπτυξη πόρων, βιομηχανικών και τεχνολογικών, για την προστασία του Κυβερνοχώρου, και, τέλος, την υιοθέτηση μιας κοινής ευρωπαϊκής στρατηγικής για τον κυβερνοχώρο, προωθώντας ταυτόχρονα τις βασικές αρχές της ΕΕ[208].

Ορόσημο για τη δράση της ΕΕ στον τομέα της Κυβερνοασφάλειας θεωρείται η ψήφιση της Οδηγίας 2016/1148 αναφορικά με κοινώς αποδεκτά μέτρα ασφάλειας υψηλού επιπέδου για συστήματα δικτύου και πληροφοριών σε ολόκληρη την Ευρωπαϊκή Ένωση. Επιπρόσθετα, η Οδηγία επεσήμαινε την αναγκαιότητα ανάπτυξης ειδικών ομάδων στα κράτη-μέλη, τις *Computer Security Incident Teams/CSIRTs* ,στόχος των οποίων θα είναι η προαγωγή της

[206] Βλ. Μ. Γερονικολού (2021), 'Η εξέλιξη της κυβερνοασφάλειας στην ΕΕ'...
[207] Βλ. Μ. Γερονικολού (2021), ' Η εξέλιξη της κυβερνοασφάλειας στην ΕΕ'...
[208] Βλ. Μ. Γερονικολού (2021), 'Η εξέλιξη της κυβερνοασφάλειας στην ΕΕ'...

εμπιστοσύνης και η αποδοτική συνεργασία σε επιχειρησιακό επίπεδο εντός της ΕΕ[209].

Στη συνέχεια, ακολούθησε το ίδιο έτος, το 2016, η ψήφιση του Γενικού Κανονισμού για την Προστασία των Δεδομένων των πολιτών εντός της Ένωσης, άμεσος στόχος του οποίου δεν είναι η ασφάλεια του Κυβερνοχώρου, αν και τον επηρεάζει αρκετά. Με τον εν λόγω Κανονισμό παρατηρείται σημαντική πρόοδος στο χώρο της Κυβερνοασφάλειας, όσον αφορά τις οικονομικές και κοινωνικές δραστηριότητες που εφαρμόζουν την ψηφιακή τεχνολογία, ενώ χαρακτηριστικό σημείο του είναι η αυστηρότητα των κυρώσεων που προβλέπονται για την παραβίασή του[210].

Ένα χρόνο αφού τέθηκε σε ισχύ η Οδηγία 2016/1148, η Στρατηγική του 2013 αναθεωρήθηκε με τον Κανονισμό 2019/881 [211], ο οποίος άρχισε να ισχύει από το 2019. Κύριοι στόχοι της νέας στρατηγικής ήταν η ανάπτυξη ενός ευρωπαϊκού μηχανισμού πιστοποίησης που παρέχει εγγυήσεις ασφαλούς χρησιμοποίησης προϊόντων και υπηρεσιών ψηφιακής τεχνολογίας σε όλη την ΕΕ καθώς και η ενίσχυση του ρόλου του ENISA.

Υπό το πρίσμα του σχεδιασμού της ΕΕ να προετοιμάσει την Ευρώπη για τον ψηφιακό κόσμο, το Φεβρουάριο του 2020 αναθεωρήθηκε η Οδηγία NIS. Η νέα Οδηγία NIS2 εντείνει τις απαιτήσεις προς τις επιχειρήσεις σχετικά με ζητήματα ασφάλειας, εισάγει πιο αυστηρά ελεγκτικά μέτρα για τις εθνικές αρχές και αποσκοπεί στην ευθυγράμμιση του πλαισίου κυρώσεων στα κράτη-μέλη. Επίσης, υποστηρίζει την ανταλλαγή πληροφοριών και τη συνεργατική αντιμετώπιση των προβλημάτων του Κυβερνοχώρου, τόσο σε επίπεδο εθνικό όσο και Ευρωπαϊκής Ένωσης[212].

---

[209] Βλ. Μ. Γερονικολού (2021),' Η εξέλιξη της κυβερνοασφάλειας στην ΕΕ'...

[210] Βλ. Μ. Γερονικολού (2021),' Η εξέλιξη της κυβερνοασφάλειας στην ΕΕ'...

[211] Βλ. Κανονισμός (ΕΕ) 1019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019 *σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια)* [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/eli/reg/2019/881/oj?locale=el Πρόσβαση στις 29-11-2021

[212] Βλ. Μ. Γερονικολού (2021), 'Η εξέλιξη της κυβερνοασφάλειας στην ΕΕ'...

Ακολούθως, το 2020 αναθεωρήθηκε η Στρατηγική για την Κυβερνοασφάλεια. Βασικοί στόχοι της νέας στρατηγικής είναι η ασφάλεια κρίσιμων υποδομών της ΕΕ και όλων των πολιτών έναντι απειλών του Κυβερνοχώρου καθώς και η ισχυροποίηση της ψηφιακής ασφάλειας της ΕΕ απέναντι σε τρίτες χώρες. Υπό αυτό το πρίσμα, τέθηκε υπό συζήτηση η ανάπτυξη ενός «δικτύου κέντρων επιχειρήσεων ασφαλείας», σε ολόκληρο τον ενωσιακό χώρο, υποστηριζόμενο από την τεχνητή νοημοσύνη, ενώ στα πλάνα της Ευρωπαϊκής Επιτροπής βρίσκεται η δημιουργία μιας «Κοινής Κυβερνομονάδας» που θα εντείνει τις συνεργασίες ανάμεσα στους θεσμούς της ΕΕ και τις εθνικές αρχές που είναι υπεύθυνες για την πρόληψη και διαχείριση κυβερνοεπιθέσεων[213].

Όπως συνάγεται από τα ανωτέρω, η ΕΕ δίνει ιδιαίτερη βαρύτητα στην Κυβερνοασφάλεια θέτοντάς τη ως προτεραιότητα, όπως άλλωστε προκύπτει και από τον προγραμματισμό της (2021-2027) , διατηρώντας για την ίδια βασικό ρόλο στην προώθηση ενός κυβερνοχώρου, ανοιχτού, με σταθερή λειτουργία και ασφάλεια, στηριζόμενη στις αξιακές αρχές της ΕΕ και στο κράτος δικαίου[214]

Σύμφωνα με τα λεχθέντα ανωτέρω, ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) ιδρύθηκε με τον Κανονισμό 460/2004[215] και το έργο του είναι να παρέχει συνδρομή στην ΕΕ και τα κράτη μέλη της ώστε να θωρακίζονται και να προετοιμάζονται καλύτερα, προκειμένου να διαχειρίζονται τα ζητήματα που ανακύπτουν σχετικά με την ασφάλεια των πληροφοριών[216].

Περαιτέρω, αρμοδιότητες του ENISA είναι να αναπτύσσει σε πανευρωπαϊκό επίπεδο δοκιμασίες διαχείρισης κρίσεων στον Κυβερνοχώρο, εθνικές πολιτικές που αφορούν τον Κυβερνοχώρο ,να προάγει τη συνεργασία μεταξύ ομάδων

[213] Βλ. Μ. Γερονικολού (2021), 'Η εξέλιξη της κυβερνοασφάλειας στην ΕΕ'...

[214] Βλ. Μ. Γερονικολού (2021), 'Η εξέλιξη της κυβερνοασφάλειας στην ΕΕ'...

[215] Βλ. Κανονισμός (ΕΚ) αριθ. 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαρτίου 2004, *για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών* [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32004R0460 Πρόσβαση στις 29-11-2021

[216]Βλ. Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) [χ.χ.] Enisa. [Διαδίκτυο]Διαθέσιμο στο: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/enisa_el Πρόσβαση στις 29-11-2021

διαχείρισης έκτακτων περιστατικών στο τομέα της πληροφορικής και να προωθεί την ανάπτυξη δεξιοτήτων[217].

Ακόμη, ο ENISA παρέχει υπηρεσίες σε εθνικές κυβερνήσεις της ΕΕ, στους θεσμούς της καθώς και σε φορείς από τον τομέα των Τεχνολογιών Πληροφορικής κα Επικοινωνιών (ΤΠΕ), δηλαδή πάροχους τηλεπικοινωνιών και διαδικτύου, σε επιχειρήσεις μικρού μεγέθους, σε ειδικούς που ασχολούνται με την προστασία των δικτύων και των πληροφοριών και σε ανώτατα εκπαιδευτικά ιδρύματα[218].

Μάλιστα, στα πλαίσια της νέας στρατηγικής για την κυβερνοασφάλεια, ο ρόλος του ENISA ενισχύθηκε και αποτελεί τον κύριο φορέα της ΕΕ για την παρακολούθηση της πορείας και της εφαρμογής της ευρωπαϊκής νομοθεσίας για την κυβερνοασφάλεια[219].

6.2 Η πρόταση για τη δημιουργία της «Κοινής Κυβερνομονάδας»

Στα πλαίσια της αντιμετώπισης του μεγάλου αριθμού των συμβάντων στον κυβερνοχώρο και των επιπτώσεών τους στους πολίτες και τις επιχειρήσεις σε ολόκληρη την Ένωση, η Ευρωπαϊκή Επιτροπή μελετά τη δημιουργίας μιας νέας «Κοινής Κυβερνομονάδας»[220][221]

---

[217] Βλ. Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA)...

[218] Βλ. Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA)...

[219] Βλ. Μ. Γερονικολού (2021), 'Η εξέλιξη της κυβερνοασφάλειας στην ΕΕ'...

[220] Βλ. Ένωση Ελλήνων Νομικών e-Θέμις (2021). *Κυβερνοασφάλεια της ΕΕ: Η Επιτροπή προτείνει τη δημιουργία μιας Κοινής Κυβερνομονάδας*, [Διαδίκτυο] Διαθέσιμο στο: https://www.ethemis.gr/2021/06/24/%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1-%CF%84%CE%B7%CF%82-%CE%B5%CE%B5-%CE%B7-%CE%B5%CF%80%CE%B9%CF%84%CF%81%CE%BF%CF%80%CE%AE-%CF%80%CF%81%CE%BF%CF%84%CE%B5%CE%AF%CE%BD%CE%B5%CE%B9-%CF%84%CE%B7-%CE%B4%CE%B7%CE%BC%CE%B9%CE%BF%CF%85%CF%81%CE%B3%CE%AF%CE%B1-%CE%BC%CE%B9%CE%B1%CF%82-%CE%BA%CE%BF%CE%B9%CE%BD%CE%AE%CF%82-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%BC%CE%BF%CE%BD%CE%AC%CE%B4%CE%B1%CF%82.html Πρόσβαση στις 25=11-2021

[221] Βλ. Ένωση Ελλήνων Νομικών e-Θέμις (2021), *Κυβερνοασφάλεια της ΕΕ:* «Η Επιτροπή προτείνει τη δημιουργία μιας Κοινής Κυβερνομονάδας...όπου αξιωματούχος της ΕΕ δηλώνει: «Η κυβερνοασφάλεια αποτελεί ακρογωνιαίο λίθο της ψηφιακής και

Στόχος της «Κοινής Κυβερνομονάδας» είναι η συλλογή των πόρων[222] και των εμπειρικών γνώσεων της ΕΕ και των κρατών μελών για την πρόληψη, παρεμπόδιση και αντιμετώπιση ομαδικών συμβάντων και κρίσεων στον κυβερνοχώρο. Η αλήθεια είναι ότι, συνήθως, οι εμπλεκόμενοι φορείς, είτε προέρχονται από το δημόσιο τομέα είτε από τον ιδιωτικό, αδυνατούν να συνεννοηθούν μεταξύ τους για τη διαχείριση των προβλημάτων που αφορούν τον κυβερνοχώρο[223]. Με τη δημιουργία της «Κοινής Κυβερνομονάδας», θα αναπτυχθεί από τους θεσμικούς φορείς της ΕΕ και τα κράτη μέλη μια ευρωπαϊκή βάση παροχής βοήθειας και υποστήριξης για τη διαχείριση κυβερνοεπιθέσεων μεγάλης έκτασης. Επίσης, θα προωθηθεί περαιτέρω η τελική διαμόρφωση του πλαισίου αντιμετώπισης των κινδύνων Κυβερνοασφάλειας στην ΕΕ. Άλλωστε, η δημιουργία της «Κοινής Κυβερνομονάδας» αποτελεί αυταπόδεικτη συνέπεια της λειτουργίας της στρατηγικής για την Κυβερνοασφάλεια στο ενωσιακό χώρο και της αντίστοιχης στρατηγικής της ΕΕ για *την «Ένωση Ασφάλειας»*[224].

Περαιτέρω, η «Κοινή Κυβερνομονάδα» θα συντονίζει σε ευρωπαϊκό επίπεδο την αντίδραση απέναντι σε μεγάλης έκτασης περιστατικά και διαταραχές στον κυβερνοχώρο, καθώς και την παροχή συνδρομής και υποστήριξης για την επαναφορά και ανάρρωση από τις επιθέσεις. Επιπρόσθετα, λαμβάνοντας υπόψη ότι σήμερα οι τομείς δράσης τόσο των φορέων της ΕΕ όσο και των κρατών μελών είναι ποικίλοι και διαφορετικοί, συχνά οι απειλές είναι

συνδεδεμένης Ευρώπης. Στη σημερινή κοινωνία, η συντονισμένη αντιμετώπιση των απειλών είναι υψίστης σημασίας. Η Κοινή Κυβερνομονάδα θα συμβάλει στην επίτευξη αυτού του στόχου. Μαζί μπορούμε πραγματικά να κάνουμε τη διαφορά».

[222] Βλ. Ένωση Ελλήνων Νομικών e-Θέμις (2021), *Κυβερνοασφάλεια της ΕΕ: Η Επιτροπή προτείνει τη δημιουργία μιας Κοινής Κυβερνομονάδας*...όπου με τη δήλωση του αξιωματούχου της ΕΕ συνοψίζεται η σημασία της Κοινής Κυβερνομονάδας: «Η Κοινή Κυβερνομονάδα αποτελεί δομικό στοιχείο για την προστασία μας από αυξανόμενες και ολοένα και πιο περίπλοκες κυβερνοαπειλές. Έχουμε θέσει σαφή ορόσημα και χρονοδιαγράμματα που θα μας επιτρέψουν –σε συνεργασία με τα κράτη μέλη– να βελτιώσουμε αισθητά τη συνεργασία για τη διαχείριση κρίσεων στην ΕΕ, να εντοπίζουμε απειλές και να αντιδρούμε ταχύτερα. Είναι το επιχειρησιακό σκέλος της ευρωπαϊκής κυβερνοασπίδας.»

[223] Βλ. Ένωση Ελλήνων Νομικών e-Θέμις *(2021), Κυβερνοασφάλεια της ΕΕ: Η Επιτροπή προτείνει τη δημιουργία μιας Κοινής Κυβερνομονάδας*...

[224] Βλ. Ένωση Ελλήνων Νομικών e-Θέμις (2021), *Κυβερνοασφάλεια της ΕΕ: Η Επιτροπή προτείνει τη δημιουργία μιας Κοινής Κυβερνομονάδας*...

κοινές και ως εκ τούτου είναι απαραίτητη η συντονισμένη δράση, η ανταλλαγή γνώσεων και ενδεχομένως η προειδοποιητική ενημέρωση[225][226].

6.3 Η πρόκληση του κυβερνοεγκλήματος στην Ευρωπαϊκή Ένωση

Σύμφωνα με τον ορισμό της Ευρωπαϊκής Επιτροπής,το κυβερνοέγκλημα συνίσταται σε «εγκληματικές πράξεις που διαπράττονται διαδικτυακά με τη χρήση δικτύων ηλεκτρονικών επικοινωνιών και πληροφοριακών συστημάτων»[227]. Η νομοθεσία και η στρατηγική που έχει θεσμοθετήσει και έχει θέσει σε εφαρμογή η Ευρωπαϊκή Επιτροπή σχετικά με το κυβερνοέγκλημα, καλύπτει τύπους παραδοσιακών εγκλημάτων, όπως για παράδειγμα η απάτη και η κλοπή, όταν διαπράττονται μέσω συστημάτων ηλεκτρονικών επικοινωνιών, εγκλήματα σχετικά με παράνομο περιεχόμενο, εδώ περιλαμβάνονται το έγκλημα της παιδικής πορνογραφίας, η παρακίνηση σε εγκληματικές ενέργειες, η προώθηση του ρατσισμού και τη ξενοφοβίας και τέλος, τα εγκλήματα μέσω ηλεκτρονικών δικτύων, όπως η υποκλοπή δεδομένων και πληροφορίων και οι παράνομες παρεμβολές[228]. Παράλληλα, από το διασυνοριακό χαρακτήρα του κυβερνοεγκλήματος συνάγεται ότι για την προώθηση των ερευνών και την

---

[225] Βλ. Ένωση Ελλήνων Νομικών e-Θέμις (2021), *Κυβερνοασφάλεια της ΕΕ: Η Επιτροπή προτείνει τη δημιουργία μιας Κοινής Κυβερνομονάδας...*

[226] Βλ. Ένωση Ελλήνων Νομικών e-Θέμις (2021), *Κυβερνοασφάλεια της ΕΕ: Η Επιτροπή προτείνει τη δημιουργία μιας Κοινής Κυβερνομονάδας...*, 'όπου σύμφωνα με δήλωση ευρωπαίου αξιωματούχου: «Η Κοινή Κυβερνομονάδα αποτελεί δομικό στοιχείο για την προστασία μας από αυξανόμενες και ολοένα και πιο περίπλοκες κυβερνοαπειλές. Έχουμε θέσει σαφή ορόσημα και χρονοδιαγράμματα που θα μας επιτρέψουν –σε συνεργασία με τα κράτη μέλη– να βελτιώσουμε αισθητά τη συνεργασία για τη διαχείριση κρίσεων στην ΕΕ, να εντοπίζουμε απειλές και να αντιδρούμε ταχύτερα. Είναι το επιχειρησιακό σκέλος της ευρωπαϊκής κυβερνοασπίδας.»

[227] Βl. European Commission Migration and Home Affairs [n. d.] *Cybercrime.* European Commission Migration and Home Affairs [Διαδίκτυο] Διαθέσιμο στο: https://ec.europa.eu/home-affairs/what-we-do/cybercrime_en Πρόσβαση στις 28-11-2021

[228] Βλ. European Parliament Directorate-General for Internal Policies, Policy Department Citizens' Rights and Constitutional Affairs (2015) *The law enforcement challenge of cybercrime: area we really playing catch-up.?* European Parliament Directorate-General for Internal Policies σελ. 24 [Διαδίκτυο] Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536471/IPOL_STU(2015)536471_EN.pdf Πρόσβαση στις 28-12-2021

επιβολή κυρώσεων, είναι αναγκαία η άρση των εμποδίων που θέτουν φραγμούς στη συνεργασία, εξαιτίας της εφαρμογής διαφορετικών δικαιοδοτικών κανόνων και νομοθετικών πλαισίων που διέπουν το σύστημα συλλογής και χρήσης των ηλεκτρονικών στοιχειών[229].

Πρέπει να αναφερθεί ότι ο σκοπός και η πολυπλοκότητα της ευρωπαϊκής πολιτικής για το κυβερνοέγκλημα υπήρξαν η αιτία για την πρόκληση διαφόρων εντάσεων μεταξύ των στόχων της πολιτικής και των νομικών δεσμεύσεων[230]. Οι Ευρωπαϊκές Συνθήκες και το μεταγενέστερο παράγωγο δίκαιο συνιστούν την εντολή για λήψη μέτρων που θα παρέχουν υψηλού επιπέδου ασφάλεια και προστασία για τα συστήματα τηλεπικοινωνιών και την ομαλή λειτουργία της ενιαίας αγοράς γενικότερα[231]. Περαιτέρω, οι διατάξεις αποτέλεσαν το νομικό υπόβαθρο για την ευρωπαϊκή νομοθεσία σε τομείς όπως η Κυβερνοασφάλεια και η προστασία υποδομών ζωτικής σημασίας[232]. Άλλωστε, η αντιμετώπιση του κυβερνοεγκλήματος αποτελεί πρωταρχικό στόχο για τη δημιουργία ενός χώρου ελευθερίας , ασφάλειας και δικαιοσύνης μέσα στην ΕΕ[233].

Ειδικότερα, ΣΛΕΕ στο άρθρο 83 προβλέπει την υιοθέτηση κοινών κανόνων σχετικά με τον ορισμό του ποινικού αδικήματος και των κυρώσεων στο χώρο του εγκλήματος μέσω υπολογιστή καθώς και άλλα σοβαρά αδικήματα[234]. Επισημαίνεται, ωστόσο, ότι η λήψη οποιονδήποτε νομοθετικών και επιχειρησιακών μέτρων που αφορούν το κυβερνοέγκλημα θα πρέπει να είναι

---

[229] Βλ. European Parliament Directorate-General for Internal Policies, Policy Department Citizens' Rights...σελ.24

[230] Βλ. European Parliament Directorate-General for Internal Policies, Policy Department Citizens' Rights …σελ.25

[231] Βλ. Άρθρο 114 Ενοποιημένη απόδοση της Συνθήκης για την Ευρωπαϊκή Ένωση και της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης - Ενοποιημένη απόδοση της Συνθήκης για την Ευρωπαϊκή Ένωση [Διαδίκτυο]Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:12012E/TXT Πρόσβαση στις 30-12-2021

[232] Βλ. European Parliament Directorate-General for Internal Policies, Policy Department Citizens' Rights …σελ.25

[233] Βλ. Άρθρο 4 παρ. 2, περ. α, *Ενοποιημένη απόδοση της Συνθήκης για την Ευρωπαϊκή Ένωση και της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης - Ενοποιημένη απόδοση της Συνθήκης για την Ευρωπαϊκή Ένωση - Ενοποιημένη απόδοση της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης*

[234] Βλ. European Parliament Directorate-General for Internal Policies, Policy Department Citizens' Rights...σελ.25

σύμφωνη με τον Ευρωπαϊκό Χάρτη Θεμελιωδών Δικαιωμάτων και άλλες ανάλογες διεθνείς πράξεις που αφορούν ανθρώπινα δικαιώματα, όπως είναι η Ευρωπαϊκή Σύμβαση για τα Ανθρώπινα Δικαιώματα και το Διεθνές Σύμφωνο για τα Πολιτικά και Κοινωνικά Δικαιώματα[235].

Περαιτέρω, η ευρωπαϊκή νομοθεσία κήρυξε παράνομες τις τρομοκρατικές οργανώσεις και ποινικοποίησε πολλές τρομοκρατικές πράξεις που διαπράττονται μέσω του διαδικτύου, συμπεριλαμβανομένης της οικονομικής βοήθειας σε άτομα και οργανώσεις που έχουν διαπράξει τρομοκρατικές πράξεις, της στρατολόγησης σε τρομοκρατικές ομάδες, της διάδοσης τρομοκρατικής προπαγάνδας και της υποκίνησης τέλεσης τρομοκρατικών πράξεων[236].

Ακόμη, στα πλαίσια της απόφασης-πλαίσιο 2001/41/ΔΕΥ[237] εναρμονίστηκαν και ποινικοποιήθηκαν αδικήματα σχετικά με την καταπολέμηση της απάτης και της παραχάραξης των μέσων πληρωμής, πλην των μετρητών, κυρίως των πιστωτικών και των χρεωστικών καρτών. Επίσης, στο Σχέδιο Δράσης για την εφαρμογή της Συντονισμένης Στρατηγικής που υιοθετήθηκε το 2010 καθορίζονται τα επιχειρησιακά μέτρα που στρέφονται κατά των δραστών τέτοιων πράξεων[238].

6.4 Η ψηφιακή τεχνολογία στη διάθεση της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια

6.4.1 *Η κρυπτογράφηση στην κυβερνοασφάλεια*

[235] Βλ. European Parliament Directorate-General for Internal Policies, Policy Department Citizens' Rights …σελ.26

[236] Βλ. European Parliament Directorate-General for Internal Policies, Policy Department Citizens' Rights …σελ.34-35

[237] Βλ. 2001/413/ΔΕΥ: Απόφαση-πλαίσιο του Συμβουλίου, της 28ης Μαΐου 2001, *για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών* [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32001F0413 Πρόσβαση στις 3-1-2022

[238] Βλ. Council of the Europoean Union (2010) *Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime.*,Luxembourg: Council of the Europoean Union [Διαδίκτυο] Διαθέσιμο στο: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/114028.pdf Πρόσβαση στις 30-12-2021

Το σύστημα της κρυπτογράφησης θεωρείται ένας αποτελεσματικός τρόπος διασφάλισης της προστασίας της Κυβερνοασφάλειας, των δεδομένων και της ιδιωτικότητας. Συνδράμει στην υπεράσπιση των πολιτών και των επιχειρήσεων έναντι της εκμετάλλευσης από τις τεχνολογίες πληροφορίας, όπως για παράδειγμα, η υποκλοπή, η κλοπή ταυτότητας και προσωπικών δεδομένων, η απάτη και η αθέμιτη γνωστοποίηση εμπιστευτικών πληροφοριών. Ωστόσο, κρυπτογράφηση μπορούν να χρησιμοποιήσουν και οι εγκληματίες για να συγκαλύψουν τις πράξεις τους και να αποφύγουν την επιβολή του νόμου. Έτσι, παρεμποδίζεται η νόμιμη πρόσβαση σε σημαντικά ηλεκτρονικά στοιχεία, το έργο των αρχών κατά την επιβολή του νόμου γίνεται πιο δύσκολο και περιπλέκεται η διαδικασία της ποινικής έρευνας[239].

Η Ευρωπαϊκή Επιτροπή, σε μια προσπάθεια να βοηθήσει τις αρχές να ξεπεράσουν τις δυσκολίες που θέτει η κρυπτογράφηση κατά την εφαρμογή του νόμου ,υπέβαλλε, στην 11η έκθεση προόδου για μια πιο αποτελεσματική και γνήσια Ένωση Ασφάλειας[240], συγκεκριμένα μη νομοθετικά μέτρα που αφορούν την περιφρούρηση μιας ισχυρής κρυπτογράφησης, η οποία είναι αναγκαία για τη λειτουργία της ψηφιακής ενιαίας αγοράς και τα οποία σε καμία περίπτωση δεν εμποδίζουν, περιορίζουν ή αποδυναμώνουν την κρυπτογράφηση. Πρέπει να τονιστεί ότι, η κρυπτογράφηση εξακολουθεί να παραμένει μια πρόκληση για την Ευρωπαϊκή Επιτροπή, την οποία η τελευταία θα συνεχίσει να αντιμετωπίζει. Ο διάλογος με τους ειδικούς και τους βασικούς εμπλεκόμενους παρέχει μια διαφορετική οπτική και θεώρηση των νέων εξελίξεων και δυνατότητα για μακροπρόθεσμη στρατηγική, υπό το πρίσμα της αυξανόμενης εξειδίκευσης και της ευρείας χρήσης των μηχανισμών κρυπτογράφησης στην επικοινωνίας, καθώς και την ανάγκη προστασίας των προσωπικών δεδομένων των χρηστών[241].

---

[239] Βλ. European Commission Migration and Home Affairs [n.d.] *Cybercrime.*.

[240] Βλ. European Commission (2017) *Communication from the Commission to the European Parliament, the European Council and the Council, Eleventh progress report towards an effective and genuine Security Union.* Brussels: European Commission [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0608 Πρόσβαση στις 29-12-2021

[241] Βλ. European Commission Migration and Home Affairs [n.d.] *Cybercrime.*.

6.4.2 *Η διατήρηση δεδομένων στην Κυβερνοασφάλεια*

Η σημασία της πρόσβασης σε ηλεκτρονικά δεδομένα είναι μεγάλη δεδομένου ότι δίνει τη δυνατότητα στην αστυνομία και στις δικαστικές αρχές να διεξάγουν έρευνα για εγκλήματα, συμπεριλαμβανομένων των εγκλημάτων που διαπράττονται διαδικτυακά ή είναι εφικτά με τη χρήση του διαδικτύου ή των δικτύων τηλεπικοινωνίας. Από την άλλη πλευρά, η πρόσβαση σε δεδομένα που δεν αφορούν το περιεχόμενο εξαρτάται από τη διαθεσιμότητα και τη διατήρησή τους από τους πάροχους υπηρεσιών επικοινωνίας[242].

Επισημαίνεται, όμως, ότι οι κανόνες διατήρησης δεδομένων πρέπει να σέβονται τα θεμελιώδη δικαιώματα της ιδιωτικότητας και της προστασίας δεδομένων, όπως αυτά έχουν κατοχυρωθεί αυτά στον Ευρωπαϊκό Χάρτη Θεμελιωδών Δικαιωμάτων. Προς το σκοπό αυτό, η Ευρωπαϊκή Επιτροπή παρακολουθεί τις εξελίξεις σε εθνικό επίπεδο, με στόχο να καλύψει τα γνωσιακά κενά και να συλλέξει πληροφορίες σχετικά με τις προκλήσεις των νομικών και θεμελιωδών δικαιωμάτων κατά την υποχρεωτική διατήρηση δεδομένων για ποινικές έρευνες και διώξεις, ζητήματα του παραδεκτού των αποδεικτικών στοιχείων και τις επιπτώσεις στους παρόχους υπηρεσιών ηλεκτρονικής επικοινωνίας και των χρηστών τους[243].

Σύμφωνα με τα όσα αναφέρθηκαν ανωτέρω, η νομοθεσία της Ευρωπαϊκής Ένωσης για το κυβερνοέγκλημα έχει στόχο να επιφέρει βελτιώσεις στις μεθόδους πρόληψης, στην έρευνα και τη δίωξη του κυβερνοεγκλήματος, να οδηγήσει στην ανάπτυξη ικανοτήτων καθώς και στο δικαστικό σύστημα και να συνεργαστεί με τις επιχειρήσεις για να ενισχύσει τη θέση των πολιτών και να τους προστατέψει[244].

---

[242]Βλ. European Commission Migration and Home Affairs [n.d.] *Cybercrime..*

[243] Βλ. European Commission Migration and Home Affairs [n.d.]*Cybercrime..*

[244]Βλ. European Commission Migration and Home Affairs [n.d.]*Cybercrime..*

6.5 Η αντίδραση της Ευρωπαϊκής Ένωσης σε περιστατικά παραβίασης της Κυβερνοασφάλειας

Το πλαίσιο που θεσπίστηκε το Μάϊο του 2019 από το Συμβούλιο της ΕΕ, δίνει τη δυνατότητα στην τελευταία να επιβάλλει κυρώσεις ως έναν τρόπο πρόληψης και αντίστασης σε περιστατικά κυβερνοεπιθέσεων που θεωρούνται εξωτερική απειλή για την ίδια την ΕΕ ή τις χώρες μέλη της[245].

Ειδικότερα, υπό το πλαίσιο αυτό, είναι η πρώτη φορά που στην ΕΕ επιτρέπεται η επιβολή κυρώσεων σε πρόσωπα ή οργανισμούς που φέρουν την ευθύνη για κυβερνοεπιθέσεις ή απόπειρες κυβερνοεπιθέσεων, στηρίζουν οικονομικά, τεχνικά ή υλικά τέτοιες επιθέσεις ή είναι εμπλεκόμενοι σε αυτές με άλλους τρόπους. Οι κυρώσεις μπορεί να έχουν τη μορφή απαγόρευσης ταξιδίου προς την ΕΕ και δέσμευσης περιουσιακών στοιχείων είτε προσώπων είτε οργανισμών[246].

Σημαντικό βήμα για τη διαχείριση ζητημάτων που σχετίζονται με την Κυβερνοασφάλεια στην ΕΕ αποτελεί η συμφωνία που επιτεύχθηκε το Δεκέμβριο του 2020 μεταξύ του Συμβουλίου και του Ευρωπαϊκού Κοινοβουλίου για την ίδρυση «Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλεια»ς, το οποίο θα στοχεύει να βελτιώσει την «κυβερνοανθεκτικότητα», να συντείνει στη διάδοση των σύγχρονων λύσεων που παρέχει η τεχνολογία όσον αφορά την Κυβερνοασφάλεια, να υποστηρίξει νέες επιχειρήσεις με αντικείμενο δραστηριοποίησης την Κυβερνοασφάλεια, να ενισχύσει την έρευνα και την πρωτοπορία στο χώρο της Κυβερνοασφάλειας και να συνδράμει στη διαχείριση της ελλιπούς κατάρτισης στο πεδίο της Κυβερνοασφάλειας[247].

---

[245] Βλ. Ευρωπαϊκό Συμβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης [χ.χ.] *Κυβερνοασφάλεια: Πώς αντιμετωπίζει η ΕΕ τις κυβερνοαπειλές…*

[246] Βλ. Ευρωπαϊκό Συμβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης [χ.χ.] *Κυβερνοασφάλεια: Πώς αντιμετωπίζει η ΕΕ τις κυβερνοαπειλές…*

[247] Βλ. Ευρωπαϊκό Συμβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης [χ.χ.] *Κυβερνοασφάλεια: Πώς αντιμετωπίζει η ΕΕ τις κυβερνοαπειλές…*

ΚΕΦΑΛΑΙΟ ΕΒΔΟΜΟ

ΚΟΡΟΝΟΙΟΣ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

7.1 Η πανδημία του κορονοϊου και τα νέα δεδομένα στην κυβερνοασφάλεια

Η πανδημία του κορονοϊού στάθηκε αφορμή για πολλές εταιρείες να εξετάσουν εκ νέου τις στρατηγικές τους σχετικά με την προστασία του απορρήτου. Σε όλους τους τομείς της οικονομίας παγκοσμίως, η Κυβερνοασφάλεα αντιπροσωπεύει έναν παράγοντα που υποκρύπτει μεγάλους κινδύνους που συνδέονται με την πανδημία του κορονοϊού[248].

Παγκοσμίως, η εφαρμογή περιοριστικών μέτρων ήταν η αιτία που πολλές επιχειρήσεις υιοθέτησαν μορφές εργασίας με πιο ευέλικτα χαρακτηριστικά, με την εφαρμογή τεχνολογιών που κάνουν εφικτή την εργασία από το χώρο του σπιτιού. Γι' αυτό το σκοπό, πολλοί οργανισμοί προκειμένου να ανταποκριθούν στα νέα δεδομένα της αγοράς, αναδιοργάνωσαν τα συστήματά τους για τη μετάβαση στην τηλεργασία σε πιο σύντομο χρονικό διάστημα. Κατόπιν τούτου, η ανωτέρω άμεση αναδιοργάνωση λειτουργίας που συνήθως ελέγχεται λεπτομερώς πριν πραγματοποιηθεί, πιθανόν να οδηγήσει σε ελλιπή ασφάλεια στον κυβερνοχώρο, την οποία κακοπροαίρετοι χρήστες θα μπορούσαν να αξιοποιήσουν προς όφελός τους[249].

Στο σημείο αυτό πρέπει να τονιστεί ότι, το συνεχώς εξελισσόμενο πεδίο επιθέσεων για τους κυβενροεγκληματίες δημιουργεί νέες προκλήσεις για τις επιχειρήσεις, τόσο σε θέματα ασφάλειας όσο και συμμόρφωσης. Επίσης, κατά το πρόσφατο χρονικό διάστημα, παρατηρήθηκε μια αύξηση στη συχνότητα εκδήλωσης κυβερνοεπιθέσεων, όχι μόνο σε υπηρεσίες χρηματοοικονομικού ενδιαφέροντος, αλλά και σε επιχειρήσεις με αντικείμενο ευαίσθητα ή σημαντικά

[248] Βλ Σ. Αγγελοπούλου (2020), 'Covid-19 και κυβερνοασφάλεια: Ποια είναι τα μέτρα που μπορούν να λάβουν οι επιχειρήσεις', *GrantThornton*, 25 Σεπτεμβρίου. [Διαδίκτυο] Διαθέσιμο στο: https://www.grant-thornton.gr/insights/article/covid-19-and-cybersecurity-gr/ Πρόσβαση στις 30-12-2021

[249] Βλ Σ. Αγγελοπούλου (2020) 'Covid-19 και κυβερνοασφάλεια: Ποια είναι τα μέτρα που μπορούν να λάβουν οι επιχειρήσεις'...

δεδομένα. Παρόλα αυτά, κατά την παρούσα χρονική περίοδο έχει γίνει φανερό ότι, ακόμα και οργανισμοί που διατηρούν ολοκληρωμένους μηχανισμούς που επιτρέπουν τη συνεχή και χωρίς κωλύματα λειτουργία τους, δεν έχουν εφαρμόσει αυτά τα συστήματα σε πραγματικό περιβάλλον, με συνέπεια οι κυβερνοεγκληματίες να έχουν μεγαλύτερο εύρος δράσης[250].

Εντούτοις, οι κίνδυνοι για την Κυβερνοασφάλεια στο χώρο των επιχειρήσεων δεν είναι μόνο εξωτερικοί. Υφίστανται κίνδυνοι και εκ των έσω, πρόκειται δηλαδή είτε για απειλές από χρήστες που ενεργούν κακόβουλα είτε για ανθρώπινα λάθη. Η πανδημία του κορονοϊού επέφερε αλλαγές στον τόπο και τον τρόπο εργασίας, απαιτώντας συγχρόνως από μεγάλο αριθμό προσωπικού να ανταποκριθεί σε νέες συνθήκες εργασίας για τις οποίες η πλειονότητα αυτού δεν είχε την κατάλληλη εκπαίδευση, με συνέπεια οι συνθήκες που προκύπτουν να ευνοούν την εκμετάλλευση της ανεπαρκούς ασφάλειας. Επιπλέον, ένα ακόμη στοιχείο που πρέπει να αναφερθεί είναι ότι, ενώ πριν το ξέσπασμα της πανδημίας οι αρμόδιες ρυθμιστικές αρχές μπορεί να εμφανίζονταν ικανοποιημένες με υψηλού επιπέδου πληροφορίες σχετικά με παροχή λύσεων στον κυβερνοχώρο, τώρα η προσοχή επικεντρώνεται στο τι προσφέρει η τεχνολογία και αν υπάρχουν αποδείξεις ότι είναι αποτελεσματική, και αυτή η προσοχή πρόκειται να ενταθεί εξαιτίας της παρούσας κρίσης[251].

7.2 Η κυβερνοασφάλεια στην τηλεργασία την εποχή της πανδημίας του κορονοϊού

Είναι αλήθεια ότι η τηλεργασία ως μορφή εργασίας εφαρμοζόταν από αρκετές εταιρείες, ωστόσο, με το ξέσπασμα της πανδημίας του κορονοϊού, είναι η πρώτη φορά που έχουν τόσο μεγάλο αριθμών χρηστών που είναι ταυτόχρονα συνδεδεμένοι εξ' αποστάσεως και για τόσο μεγάλη χρονική περίοδο. Βέβαια, για

[250] Βλ Σ. Αγγελοπούλου (2020), 'Covid-19 και κυβερνοασφάλεια: Ποια είναι τα μέτρα που μπορούν να λάβουν οι επιχειρήσεις'...
[251] Βλ Σ. Αγγελοπούλου (2020), '*Covid-19 και κυβερνοασφάλεια: Ποια είναι τα μέτρα που μπορούν να λάβουν οι επιχειρήσεις*'...

πολλές εταιρείες, η εφαρμογή της τηλεργασίας εξετάζεται πρώτη φορά ως πιθανότητα και η πρόκληση είναι μεγάλη, κυρίως για τους χρήστες που πρέπει να αποκτήσουν νέες δεξιότητες και να συνηθίσουν έναν νέο τρόπο εργασίας[252]. Αναμφίβολα, οι εταιρείες που έκαναν χρήση της τηλεργασίας, είναι αντιμέτωπες με λιγότερα ζητήματα, σε σχέση με όσες εταιρείες που δεν εφάρμοζαν την τηλεργασία. Οι τελευταίες πρέπει να αναδιοργανωθούν προσαρμοζόμενες στην τεχνολογία ώστε να η λειτουργία της εξ'αποστάσεως να είναι ασφαλής. Οφείλουν, για παράδειγμα, να διαθέτουν την κατάλληλη τεχνολογία για να προστατεύουν τα δεδομένα από μη εξουσιοδοτημένους χρήστες, αν και μέχρι να διευθετηθούν αυτά τα θέματα, οι εταιρείες πιθανόν να έρθουν αντιμέτωπες με παράπονα χρηστών και πελατών, ενώ και τα δεδομένα της εταιρείας μπορεί να βρίσκονται σε κίνδυνο[253].

Περαιτέρω, είναι αναγκαιότητα για τις εταιρείες να συμμορφωθούν με τα καινούρια δεδομένα, ώστε να διαχειριστούν τη νέα κατάσταση. Είναι σημαντικό να κατανοηθεί ότι, η τηλεργασία εγκυμονεί κινδύνους που συνδέονται με τα δεδομένα της εταιρείας, δηλαδή με πληροφορίες που παράγει η εταιρεία και είναι πολύτιμες γι' αυτήν[254].

Όσον αφορά τους κινδύνους που υποκρύπτει η τηλεργασία, αυτοί αφορούν την κλοπή δεδομένων της εταιρείας, την καταστροφή τους χωρίς να έχουν δημιουργηθεί αντίγραφα ασφαλείας, η οποία ενδέχεται να οδηγήσει και στην απόλυτη αδυναμία πρόσβασης σε αυτά και τέλος η παραποίησή τους. Όλα τα προαναφερθέντα μπορεί να οδηγήσουν σε μείωση της αποδοτικότητας της εταιρείας, να πλήξουν την εμπιστοσύνη των πελατών προς την εταιρεία, να

[252] Βλ. ' Κορωνοϊός: Η τηλεργασία απειλεί την κυβερνοασφάλεια -Πώς προστατεύονται επιχειρήσεις και χρήστες' (2021*), iefimerida* , 31 Μαρτίου. [Διαδίκτυο] Διαθέσιμο στο: https://www.iefimerida.gr/ellada/koronoios-tilergasia-apeilei-kybernoasfaleia Πρόσβαση στις 29-12-2021

[253] Βλ. ' Κορωνοϊός: Η τηλεργασία απειλεί την κυβερνοασφάλεια -Πώς προστατεύονται επιχειρήσεις και χρήστες'...

[254] Βλ. 'Κορωνοϊός: Η τηλεργασία απειλεί την κυβερνοασφάλεια -Πώς προστατεύονται επιχειρήσεις και χρήστες'...

βλάψουν οικονομικά την εταιρεία και, ακόμα, να οδηγήσουν την εταιρεία σε κατάρρευση[255].

ΣΥΜΠΕΡΑΣΜΑ

Όπως προκύπτει από τα όσα έχουν αναφερθεί ανωτέρω, το διαδίκτυο κυριαρχεί σε κάθε μορφή σχεδόν ανθρώπινης δραστηριότητας. Παρέχει πληθώρα εφαρμογών και υπηρεσιών, η πρόσβαση στις οποίες καθίσταται εφικτή μέσω των συστημάτων τεχνολογίας και είναι συνήθως ανοιχτή σε όλους, ιδιώτες και οργανισμούς.

Αυτή, ωστόσο, η ευρεία χρήση του συνιστά και τον μεγαλύτερο κίνδυνο για την ασφαλή λειτουργία του και ανεμπόδιστη χρήση του από τους χρήστες.

Σε αυτό ακριβώς το σημείο έγκειται ο ρόλος της Κυβερνοασφάλειας που στοχεύει στη διαμόρφωση ενός κυβερνοχώρου ασφαλούς, όπου τα δικαιώματα των χρηστών του δημόσιου και του ιδιωτικού χώρου θα προστατεύονται και θα υποστηρίζονται.

Βέβαια, προϋπόθεση για να επιφέρει η Κυβερνοασφάλεια τα μέγιστα δυνατά αποτελέσματα αποτελεί η συνεργασία και η συντονισμένη δράση όλων των εμπλεκόμενων, ενώ συγχρόνως απαιτείται η εφαρμογή αποτελεσματικότερων πρακτικών και στοχευμένων στρατηγικών Κυβερνοασφάλειας.

[255] Βλ. 'Κορωνοϊός: Η τηλεργασία απειλεί την κυβερνοασφάλεια -Πώς προστατεύονται επιχειρήσεις και χρήστες'...

Βιβλιογραφία

Αγγελής Ι., (2001) *Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο*, ΠοινΔικ

Αγγελοπούλου Σ., (2020) 'Covid-19 και κυβερνοασφάλεια: Ποια είναι τα μέτρα που μπορούν να λάβουν οι επιχειρήσεις', *GrantThornton*, 25 Σεπτεμβρίου, [Διαδίκτυο] Διαθέσιμο στο: https://www.grant-thornton.gr/insights/article/covid-19-and-cybersecurity-gr/ Πρόσβαση στις 30-12-2021

Βασιλάκη Ε., (1993) *Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών-Η αντιμετώπιση του προβλήματος μετά την εισαγωγή του ν. 1805/88*

Γερονικολού Μ.,(2021) 'Η εξέλιξη της κυβερνοασφάλειας στην ΕΕ',*ΟΔΕΘ*, Όμιλος Διεθνών & Ευρωπαϊκών Θεμάτων, 2021, [Διαδίκτυο] Διαθέσιμο στο: https://odeth.eu/%CE%B7-%CE%B5%CE%BE%CE%AD%CE%BB%CE%B9%CE%BE%CE%B7-%CF%84%CE%B7%CF%82-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82-%CF%83%CF%84%CE%B7%CE%BD-%CE%B5 / Πρόσβαση στις 20-11-2021

Θεοδωρίδη Κ.,(20070 *Πορνογραφία ανηλίκων στο Διαδίκτυο*, ΕΕΕυρΔ,

Ίδρυμα Μαραγκοπούλου (2007) *Η παιδική πορνογραφία στο διαδίκτυο*

Ιγγλεζάκης Ι., (2021) *Δίκαιο Πληροφορικής*, Δ' Έκδοση, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη

Ιγγλεζάκης Ι.,(2015) *Ο μισαλλόδοξος λόγος στο διαδίκτυο και η ποινική αντιμετώπισή του με τον Ν.4285/2014*, Συνήγορος 109/2015

Καϊάφα-Γκπάντι Μ., (2016) *Η ποινική καταστολή της ρατσιστικής ρητορίας, των εγκλημάτων ρατσισμού και της ρατσιστικής διάκρισης: προς μια ουσιαστική προστασία της αξίας του ανθρώπου*, ΠοινΔικ

Καρανικόλα Γ.,(2005) *Παιδική Πορνογραφία στο Διαδίκτυο: προβληματισμοί γύρω από τη νέα ρύθμιση του άρθρου348 Α ΠΚ*, ΠοινΔικ

Κουμάντου Γ., (2002) *Πνευματική ιδιοκτησία*

Μαρίνος Μ.Θ.,(2004) *Πνευματική ιδιοκτησία*

Μαρίνος Μ.Θ., (1992) *Λογισμικό. Νομική προστασία και συμβάσεις (Ι)*

Μαυρίδης Ι., (2015) *Ασφάλεια Πληροφοριών στο Διαδίκτυο*, Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών .

Μοροζίνη Ι., *Η μεταφορά χρημάτων με χρήση υπηρεσιών ηλεκτρονικής τραπεζικής ως ποινικώς κολάσιμη συμπεριφορά υπό το πρίσμα των εγκλημάτων κατά της ιδιοκτησίας και της περιουσίας, σε: Δαλακούρα*

Μυλωνόπουλος Χ.,(1991) *Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο. Συμβολή στην ερμηνεία των άρθρων 13γ, 370Β, 370Γ και 386 Α Π.Κ. (άρθρ. 2-5 ν. 1805/88),*

Νάϊντος Χ., *Ιδιαιτερότητες στην ποινική αντιμετώπιση του ρατσισμού που εκδηλώνεται μέσω του διαδικτύου, σε :Δαλακούρα (επιμ.), Ηλεκτρονικό έγκλημα*

Νούσκαλη Γ., (2020) *Κατοχή και διανομή/διάθεση πορνογραφικού υλικού ανηλίκων (άρθρο 348 Α ΠΚ): Η νομολογιακή προσέγγιση κρίσιμων ζητημάτων ουσιαστικού και δικονομικού δικαίου*, Επιθεώρηση Δικαίου Πληροφορικής [Διαδίκτυο] Διαθέσιμο στο: https://ejournals.lib.auth.gr/infolawj/article/view/7783 Πρόσβαση στις 12-11-2021

Γ. Νούσκαλη Γ., (2006) *Πορνογραφία ανηλίκων: τα κρίσιμα ζητήματα του άρθρου 348 Α ΠΚ*, Ποιν Δικ

Νούσκαλη Γ., (2003) *Απάτη με ηλεκτρονικό υπολογιστή (η/υ): Το παρελθόν και το μέλλον του άρθρου 386 Α ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση*, ΠοινΔικ

Παπαδαμάκης Α., (2020) *Τα περιουσιακά εγκλήματα*, 3η εκδ.

Πολυζωϊδου Β. ,(2016) *Το αξιόποινο της πορνογραφίας ανηλίκων*

Συμεωνίδου-Καστανίδου Ε., (2015) *Η ποινική αντιμετώπιση του ρατσισμού και της ξενοφοβίας στην Ελλάδα*, ΠοινΧρ,

Hoofnagle C. J., (2007) 'Identity Theft: Making the Known Unknowns Known', *Harvard Journal of Law and Technology*, Vol. 21 [Διαδίκτυο] Διαθέσιμο στο:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=969441 Πρόσβαση στις 30-11-2021

Martin N., Rice J.,(2011) 'Cybercrime: understanding and addressing the concerns of stakeholders', *Computers & Security*, [Διαδίκτυο] Διαθέσιμο στο: https://www.sciencedirect.com/science/article/pii/S016740481100085X Πρόσβαση στις 22-12-2021

Salu A. O. , (2004) 'Online crimes and advance fee fraud in Nigeria - are available legal remedies adequate?', *Journal of Money Laundering Control*, Vol. 8, No. 2, pp. 159-167 [Διαδίκτυο] Διαθέσιμο στο: https://doi.org/10.1108/13685200510621091 Πρόσβαση στις 10-12-2021

Stephenson D ,(2013) 'Spear Phishing: Who's Getting Caught?', Business 2 Community, [Διαδίκτυο] Διαθέσιμο στο: https://www.business2community.com/infographics/spear-phishing-attacks-whos-getting-caught-0505469 Πρόσβαση στις 20-12-2021

Tunggal A.T.,(2021) 'Why is Cybersecurity Important?; *UpGuard* [Διαδίκτυο] Διαθέσιμο στο: https://www.upguard.com/blog/cybersecurity-important Πρόσβαση στις 10-11-2021

Tunggal A. T., (2021) '*What is a Cyber Threat*?' *UpGuard* [Διαδίκτυο] Διαθέσιμο στο: https://www.upguard.com/blog/cyber-threat Πρόσβαση στις 10-12-2021

Ελληνική Νομοθεσία

Απόφαση Α.Δ.Α.Ε. 205/2013 - ΦΕΚ 1742/Β/15-7-2013: *Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/apophase-adae-205-2013.html Πρόσβαση στις 28-12-2021

Νόμος 4619/2019-ΦΕΚ 95/Α/11-6-2019- *Κύρωση του Ποινικού Κώδικα,* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-kodikes-nomothesias/nomos-4619-2019-phek-95a-11-6-2019.html Πρόσβαση στις 27-12-2021

Νόμος 4577/2018 - ΦΕΚ 199/Α/3-12-2018: *Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις* [Διαδίκτυο] Διαθέσιμο

στο: https://www.e-nomothesia.gr/kat-nomothesia-genikou-endiapherontos/nomos-4577-2018-phek-199a-3-12-2018.html Πρόσβαση στις 28-12-2021

Νόμος 4360/2016 - ΦΕΚ 9/Α/29-1-2016: *Ενσωμάτωση στην εθνική νομοθεσία: της Οδηγίας 2011/99/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 2011, περί της ευρωπαϊκής εντολής προστασίας, της απόφασης πλαίσιο 2009/315/ΔΕΥ του Συμβουλίου της 26ης Φεβρουαρίου 2009,* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-dikasteria-dikaiosune/nomos-4360-2016.html

Πρόσβαση στις 28-12-2021

Νόμος 4411/2016-ΦΕΚ 142/Α/3-8-2016: *Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών,* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-nomothesia-genikou-endiapherontos/nomos-4411-2016.html Πρόσβαση στις 27-12-2021 .

Νόμος 4285/2014 - ΦΕΚ 191/Α/10-9-2014: Τροποποίηση του ν. 927/1979 (Α' 139) και προσαρμογή του στην απόφαση πλαίσιο *2008/913/ΔΕΥ της 28ης Νοεμβρίου 2008, για την καταπολέμηση ορισμένων μορφών και εκδηλώσεων ρατσισμού και ξενοφοβίας μέσω του ποινικού δικαίου (L 328) και άλλες διατάξεις*[Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-anthropina-dikaiomata/n-4285-2014.html Πρόσβαση στις 20-12-2021

Νόμος 4267/2014 - ΦΕΚ 137/Α/12-6-2014: *Καταπολέμηση της σεξουαλικής κακοποίησης και εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και άλλες διατάξεις* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-anilikoi/n-4267-2014.html Πρόσβαση στις 22-11-2021

Νόμος 4070/2012 - ΦΕΚ 82 Α/10-4-2012: *Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/n-4070-2012.html Πρόσβαση στις 28-12-2021

Νόμος 3625/2007 - ΦΕΚ 290/Α/24-12-2007: *Κύρωση, εφαρμογή του Προαιρετικού Πρωτοκόλλου στη Σύμβαση για τα Δικαιώματα του Παιδιού σχετικά με την εμπορία παιδιών, την παιδική πορνεία και παιδική πορνογραφία και άλλες διατάξεις.*[Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-anilikoi/n-3625-2007.html Πρόσβαση στις 22-12-2021

Νόμος 3115/2003-ΦΕΚ 47/Α/2722003: *Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/n-3115-2003.html Πρόσβαση στις 28-12-2021

Νόμος 3064/2002 - ΦΕΚ 248/Α/15-10-2002: Νόμος 3064/2002 :*Καταπολέμηση της εμπορίας ανθρώπων, των εγκλημάτων κατά της γενετήσιας ελευθερίας, της πορνογραφίας ανηλίκων και γενικότερα της οικονομικής εκμετάλλευσης της γενετήσιας ζωής και αρωγή στα θύματα των πράξεων αυτών* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-egklema-organomeno/n-3064-2002.html Πρόσβαση στις 20-12-2021

Νόμος 2121/1993 - ΦΕΚ 25/Α/4-3-1993: *Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-pneumatike-idioktesia/n-2121-1993.html Πρόσβαση στις 20-12-2021

Νόμος 1805/1988 - ΦΕΚ 199/Α/31-8-1988: *Εκσυγχρονισμός τον θεσμού τον ποινικού μητρώου, τροποποίηση ποινικών διατάξεων και ρύθμιση άλλων σχετικών θεμάτων.* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-dikasteria-dikaiosune/n-1805-1988.html Πρόσβαση 11-12-2021

Νόμος 927/1979 - ΦΕΚ 139/Α/28-6-1979: *Περί κολασμού πράξεων ή ενεργειών αποσκοπουσών εις φυλετικάς διακρίσεις* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-anthropina-dikaiomata/n-927-1979.html
Πρόσβαση στις 12-12-2021

Νόμος 5060 ΦΕΚ Α' 172/30.6.1931: *Περί τύπου,προσβολών της τιμής εν γένει και άλλων σχετικών διατάξεων* [Διαδίκτυο] Διαθέσιμο στο:

https://www.kodiko.gr/nomothesia/document/579264/nomos-5060-1931 Πρόσβαση στις 22-11-2021

Προεδρικό Διάταγμα 82/2017 - ΦΕΚ 117/Α/10-8-2017: *Οργανισμός του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/enemerose-tupos-radiophono-teleorase/proedriko-diatagma-82-2017-fek-117a-10-8-2017.html Πρόσβαση στις 28-12-2021

Προεδρικό Διάταγμα υπ' αριθμ. 39, τεύχος πρώτο, αρ. φύλλου 104, 6 Μαΐου 2011: *Προσαρμογή της ελληνικής νομοθεσίας προς τις διατάξεις της Οδηγίας 2008/114/ΕΚ του Συμβουλίου της 8ης Δεκεμβρίου 2008 «σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους»(L 345/23–12–2008)* [Διαδίκτυο] Διαθέσιμο στο: http://www.kemea.gr/images/documents/pd39-2011.pdf Πρόσβαση στις 28-12-2021

Υπουργική Απόφαση 1027/2019 - ΦΕΚ 3739/Β/8-10-2019:*Θέματα εφαρμογής και διαδικασιών του ν. 4577/2018 (Α 199)* [Διαδίκτυο] Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/upourgike-apophase-1027-2019-phek-3739b-8-10-2019.html Πρόσβαση στις 28-12-2021

Υπουργική Απόφαση 3218/2018: *Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας* [Διαδίκτυο] Διαθέσιμο στο: https://mindigital.gr/wp-content/uploads/2020/01/NCSSGR.pdf Πρόσβαση στις 15-12-2021

Ευρωπαϊκή Νομοθεσία

Απόφαση-Πλαίσιο 2008/913/ΔΕΥ του Συμβουλίου της 28ης Νοεμβρίου 2008 *για την καταπολέμηση ορισμένων μορφών και εκδηλώσεων ρατσισμού και ξενοφοβίας μέσω του ποινικού δικαίου* [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX:32008F0913 Πρόσβαση στις 22-12-2021

Απόφαση-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου, της 22ας Δεκεμβρίου 2003, *για την καταπολέμηση της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας*, L 013 της 20/01/2004 [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32004F0068 Πρόσβασης στις 20-12-2021

2001/413/ΔΕΥ: Απόφαση-πλαίσιο του Συμβουλίου, της 28ης Μαΐου 2001, *για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών* [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32001F0413 Πρόσβαση στις 3-1-2022

Ενοποιημένη απόδοση της Συνθήκης για την Ευρωπαϊκή Ένωση και της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης - Ενοποιημένη απόδοση της Συνθήκης για την Ευρωπαϊκή Ένωση [Διαδίκτυο]Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:12012E/TXT Πρόσβαση στις 30-12-2021

Κανονισμός (ΕΕ) 1019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019 *σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια)* [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/eli/reg/2019/881/oj?locale=el Πρόσβαση στις 29-11-2021

Κανονισμός (ΕΕ) αριθ.910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 *σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ*, [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32014R0910 Πρόσβαση στις 28-12-2021

Κανονισμός (ΕΚ) αριθ. 460/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαρτίου 2004, *για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών* [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32004R0460 Πρόσβαση στις 29-11-2021

Οδηγία (ΕΕ) 2019/713 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019 *για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών και την αντικατάσταση της απόφασης-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου*, ΕΕ L 123/18, 10.5.2019 [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX:32019L0713 Πρόσβαση στις 17-12-2021

Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 5ης Ιουλίου *2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου κα πληροφοριών σε ολόκληρη την Ένωση*, ΕΕ L 194/1 19.7. 2016 [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016L1148 Πρόσβαση στις 7-11-2021

Οδηγία 2011/93/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 2011 *σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου*, L335/1, 17.12.2011, [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32011L0093 Πρόσβαση στις 28-12-2021

Οδηγία 2010/0273 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου *για τις επιθέσεις κατά των συστημάτων πληροφοριών και την κατάργηση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου {SEC(2010)1122 final}{SEC(2010)1123 final}*, αιτιολογική έκθεση [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52010PC0517&from=EN Πρόσβαση στις 14-11-2021

Άρθρα

Βρουμάς Α., (2020) 'Το Νομικό Πλαίσιο για την Ασφάλεια των Δικτύων / Υπηρεσιών Ηλεκτρονικών Επικοινωνιών' *Law&Tech* [Διαδίκτυο] Διαθέσιμο στο: https://lawandtech.eu/2020/04/27/%CF%80%CE%BF%CE%B9%CE%BF-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-%CE%BD%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C-%CF%80%CE%BB%CE%B1%CE%AF%CF%83%CE%B9%CE%BF-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B7%CE%BD-%CE%B1%CF%83/ Πρόσβαση στις 28-12-2021

Μ. Γερονικολού Μ., (2021) 'Η εξέλιξη της κυβερνοασφάλειας στην ΕΕ',*ΟΔΕΘ Όμιλος Διεθνών & Ευρωπαϊκών Θεμάτων* [Διαδίκτυο] Διαθέσιμο στο: https://odeth.eu/%CE%B7-%CE%B5%CE%BE%CE%AD%CE%BB%CE%B9%CE%BE%CE%B7-%CF%84%CE%B7%CF%82-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82-%CF%83%CF%84%CE%B7%CE%BD-%CE%B5/ Πρόσβαση στις 20-11-2021

Ηλιόπουλος Ν., (2008) 'Περί κινδύνων ο λόγος... Διαχείριση και αντιμετώπισή του'ς, *it PROFESSIONAL security*, [Διαδίκτυο]Διαθέσιμο στο: https://www.itsecuritypro.gr/peri-kindynon-o-logos-diachirisi-ke-antimetopisi-tous-2/ Πρόσβαση στις 22-12-2021

Ηλιόπουλος Ν.,(2008) 'Διαχείριση Ασφάλειας Πληροφοριών: Η Σύγχρονη Επιχειρησιακή Αναγκαιότητα', *it PROFESSIONAL security*, [Διαδίκτυο]Διαθέσιμο στο: https://www.itsecuritypro.gr/diachirisi-asfalias-pliroforion-sygchroni-epichirisiaki-anagkeotita-2 / Πρόσβαση στις 22-12-2021

Μεϊμάρογλου Ε., (2020) 'Η κυβερνοασφάλεια στην Ελλάδα: Αποσαφήνιση όρων και νέες,προκλήσεις', *ΟΔΕΘ* [Διαδίκτυο] Διαθέσιμο στο: https://odeth.eu/%CE%B7-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1-%CF%83%CF%84%CE%B7%CE%BD-

%CE%B5%CE%BB%CE%BB%CE%AC%CE%B4%CE%B1-%CE%B1%CF%80%CE%BF%CF%83%CE%B1%CF%86/ Πρόσβαση στις 22-12-2021

Ιστοσελίδες-Ιστότοποι

Αιτιολογική έκθεση ν. 4411/2016, σελ. 6, [Διαδίκτυο] Διαθέσιμο στο: https://www.hellenicparliament.gr/UserFiles/2f026f42-950c-4efc-b950-340c4fb76a24/k-raxef-eis.pdf Πρόσβαση στις 27-12-2021

Ελληνική Δημοκρατία Υπουργείο Ψηφιακής Διακυβέρνησης Εθνική Αρχή Κυβερνοασφάλειας (2020). *Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025* [Διαδίκτυο]Διαθέσιμο στο: https://mindigital.gr/wp-content/uploads/2020/12/%CE%95%CE%B8%CE%BD%CE%B9%CE%BA%CE%B7%CC%81-%CE%A3%CF%84%CF%81%CE%B1%CF%84%CE%B7%CE%B3%CE%B9%CE%BA%CE%B7%CC%81-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%B1%CC%81%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf Πρόσβαση στις 10-11-2021

Ελληνική Δημοκρατία Υπουργείο Παιδείας και Θρησκευμάτων. [χ.χ.] *Cyberbullying – Διαδικτυακός Εκφοβισμός*. [Διαδίκτυο] Διαθέσιμο στο: https://saferinternet4kids.gr/hot-topics-ef/cyberbullying-ef/ Πρόσβαση στις 30-11-2021

Εφημερίδα της Κυβερνήσεως (2001) *Convention on Cybercrime* [Διαδίκτυο] Διαθέσιμο στο: https://www.lawspot.gr/sites/default/files/annex_files/other/sumvasi_voudapestis_eng_fr.pdf Πρόσβαση στις 14-11-2021

Ένωση Ελλήνων Νομικών e-Θέμις (2021) *Κυβερνοασφάλεια της ΕΕ: Η Επιτροπή προτείνει τη δημιουργία μιας Κοινής Κυβερνομονάδας*, [Διαδίκτυο] Διαθέσιμο στο: https://www.ethemis.gr/2021/06/24/%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%

CE%B1-%CF%84%CE%B7%CF%82-%CE%B5%CE%B5-%CE%B7-%CE%B5%CF%80%CE%B9%CF%84%CF%81%CE%BF%CF%80%CE%AE-%CF%80%CF%81%CE%BF%CF%84%CE%B5%CE%AF%CE%BD%CE%B5%CE%B9-%CF%84%CE%B7-%CE%B4%CE%B7%CE%BC%CE%B9%CE%BF%CF%85%CF%81%CE%B3%CE%AF%CE%B1-%CE%BC%CE%B9%CE%B1%CF%82-%CE%BA%CE%BF%CE%B9%CE%BD%CE%AE%CF%82-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%BC%CE%BF%CE%BD%CE%AC%CE%B4%CE%B1%CF%82.html Πρόσβαση στις 25=11-2021

Ευρωπαϊκό Ελεγκτικό Συνέδριο (2019) *Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια* Λουξεμβούργο: Ευρωπαϊκό Ελεγκτικό Συνέδριο [Διαδίκτυο] Διαθέσιμο στο: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EL.pdf Πρόσβαση στις 7-11-2021

Ευρωπαϊκό Συμβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης [χ.χ.] , *Κυβερνοασφάλεια: Πώς αντιμετωπίζει η ΕΕ τις κυβερνοαπειλές* Ευρωπαϊκό Συμβούλιο, Συμβούλιο της Ευρωπαϊκής Ένωσης [Διαδίκτυο] Διαθέσιμο στο: https://www.consilium.europa.eu/el/policies/cybersecurity/ Πρόσβαση στις 29-12-2021

‘ Κορωνοϊός: Η τηλεργασία απειλεί την κυβερνοασφάλεια -Πώς προστατεύονται επιχειρήσεις και χρήστες’(2020) , *iefimerida* 31 Μαρτίου. [Διαδίκτυο] Διαθέσιμο στο: https://www.iefimerida.gr/ellada/koronoios-tilergasia-apeilei-kybernoasfaleia Πρόσβαση στις 29-12-2021

Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια(ENISA)[n.d.] *enisa* https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/enisa_el [Διαδίκτυο] Πρόσβαση στις 29-11-2021.

Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ (2020) Κυβερνοασφάλεια [Διαδίκτυο] Διαθέσιμο στο:

https://www2.deloitte.com/content/dam/Deloitte/gr/Documents/risk/gr_SEV_Deloitte_Cybersecurity_noexp.pdf Πρόσβαση στις 20-12-2021

Ποινικός Κώδικας [Διαδίκτυο] Διαθέσιμο στο: https://www.legal-tools.org/doc/60f2e6/pdf/ Πρόσβαση στις 10-12-2021

Σύνταγμα [Διαδίκτυο] Διαθέσιμο στο: https://www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/ Πρόσβαση στις 20-12-2021

Council of the Europoean Union (2010) *Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime* Luxembourg: Council of the Europoean Union [Διαδίκτυο] Διαθέσιμο στο: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/114028.pdf Πρόσβαση στις 30-12-2021

Council of Europe Portal Treaty Office (2003*) Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189*). Strasbourg: Council of Europe Portal Treaty Office [Διαδίκτυο] Διαθέσιμο στο: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189 Πρόσβαση 10-12-2021

Council of Europe (2001*) Explanatory Report to the Convention on Cybercrime*, υπό ΙΙΙ Luxembourg: Council of Europe [Διαδίκτυο] Διαθέσιμο στο: https://rm.coe.int/16800cce5b Πρόσβαση στις 10-12-2021

European Commission (2017) *Communication from the Commission to the European Parliament, the European Council and the Council, Eleventh progress report towards an effective and genuine Security Union* Brussels: European Commission [Διαδίκτυο] Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0608 Πρόσβαση στις 29-12-2021

European Parliament Directorate-General for Internal Policies, Policy Department Citizens' Rights and Constitutional Affairs (2015). *The law enforcement challenge of cybercrime: area we really playing catch-up?* European Parliament Directorate-General for Internal Policies, Policy Department Citizens' Rights and Constitutional Affairs

[Διαδίκτυο] Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536471/IPOL_STU(2015)536471_EN.pdf Πρόσβαση στις 28-12-2021

European Court of Human Rights Council of Europe *Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου.* Strasbourg: European Court of Human Rights Council of Europe [Διαδίκτυο] Διαθέσιμο στο: https://www.echr.coe.int/documents/convention_ell.pdf Πρόσβαση στις 28-11-2021

European Commission Migration and Home Affairs [n.d.] *Cybercrime.* European Commission Migration and Home Affairs [Διαδίκτυο] Διαθέσιμο στο: https://ec.europa.eu/home-affairs/what-we-do/cybercrime_en Πρόσβαση στις 28-11-2021

SafeInternet4Kids.gr, [χ.χ.] *Hate Speech, Ρητορική Μίσους στο Διαδίκτυο.* [Διαδίκτυο] Διαθέσιμο στο: https://saferinternet4kids.gr/wp-content/uploads/2018/05/hate-speech-per-page.pd f Πρόσβαση στις 22-11-2021

Trend Micro. [n.d.] *Spear phishing* [Διαδίκτυο] Διαθέσιμο στο: https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing

The Cybersmile foundation [n.d.] *What is cyberbulling*? [Διαδίκτυο] Διαθέσιμο στο: https://www.cybersmile.org/advice-help/category/what-is-cyberbullying Πρόσβαση στις 30-11-2021

Νομολογία

Ολ ΑΠ 3/2010 ΝΟΜΟΣ ΤΝΠ

ΑΠ 858/2020 ΝΟΜΟΣ ΤΝΠ

ΑΠ 1726/2019 ΝΟΜΟΣ ΤΝΠ

ΑΠ 813/2015 ΝΟΜΟΣ ΤΝΠ

ΑΠ 770/2015 ΝΟΜΟΣ ΤΝΠ

ΑΠ 810/2007 ΝΟΜΟΣ ΤΝΠ

ΑΠ 628/2006 ΤΝΠ ΝΟΜΟΣ

ΑΠ 2087/2003 (Ε΄ ΠοινΤμ)