ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΟΙ ΕΙΔΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΠΡΟΣΤΑΣΙΑΣ ΚΑΙ ΒΟΗΘΕΙΑΣ ΤΩΝ ΘΥΜΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΚΑΙ ΓΕΡΜΑΝΙΚΗ ΕΝΝΟΜΗ ΤΑΞΗ

Διπλωματική Εργασία

τής

Ιωάννας Κυριακίδου

mli21032

Θεσσαλονίκη, Φεβρουάριος 2024

ΟΙ ΕΙΔΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΠΡΟΣΤΑΣΙΑΣ ΚΑΙ ΒΟΗΘΕΙΑΣ ΤΩΝ ΘΥΜΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΚΑΙ ΓΕΡΜΑΝΙΚΗ ΕΝΝΟΜΗ ΤΑΞΗ

Ιωάννα Κυριακίδου

Πτυχίο Νομικής, ΑΠΘ, 2019

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Συνεπιβλέποντες Καθηγητές:

Θεοχάρης Δαλακούρας

Νικόλαος Δαγκλής

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 29.02.2024.

Θεοχάρης Δαλακούρας Νικόλαος Δαγκλής Νικόλαος Σαββίδης

....

Ιωάννα Κυριακίδου

Περίληψη

Το θέμα τής παρούσας εργασίας είναι *"Οι ειδικές διατάξεις προστασίας και βοήθειας των θυμάτων ηλεκτρονικού εγκλήματος στην ελληνική και γερμανική έννομη τάξη"*. Επιχειρείται μία εις βάθος και ουσιαστική ανάλυση του νομικού πλαισίου προστασίας των θυμάτων του ηλεκτρονικού εγκλήματος στην Ελλάδα και στη Γερμανία. Ακολουθείται μία συγκριτική μελέτη μεταξύ των θεσμοθετημένων μέτρων προστασίας των δύο χωρών, στις οποίες, ωστόσο, οι ομοιότητες είναι περισσότερες από τις διαφορές. Αυτό πραγματοποιείται, όχι μόνο με την ανάλυση κειμένων νομικού περιεχομένου - ήτοι νομοθετημάτων, δικαστικών αποφάσεων, επιστημονικών νομικών άρθρων και συγγραμμάτων - αλλά και με την εξέταση της εφαρμογής τους στην πράξη και της αποτελεσματικότητάς τους στη μάχη για την αντιμετώπιση του ηλεκτρονικού εγκλήματος. Μία αποκλειστικά θεωρητική προσέγγιση, δε θα απέδιδε, άλλωστε, τα επιθυμητά πραγματικά αποτελέσματα, σε ένα ζήτημα πιο επίκαιρο από ποτέ. Η αντιμετώπιση του ηλεκτρονικού εγκλήματος αποτελεί μείζον ζήτημα στον ευρωπαϊκό χώρο, ενώ, παράλληλα, η ραγδαία εξέλιξη των εγκλημάτων στο διαδίκτυο, καθιστά αδήριτη ανάγκη την άμεση ανταπόκριση των αρμοδίων για την καταπολέμησή τους. Στην Ελλάδα παρατηρείται χρονικά μικρή καθυστέρηση εναρμόνισης και εφαρμογής μέτρων, τα οποία έχουν ήδη κριθεί ως αποτελεσματικά στις υπόλοιπες ευρωπαϊκές χώρες. Παρ' όλα αυτά, τα τελευταία χρόνια έχει σημειωθεί αλματώδης πρόοδος στην ελληνική έννομη τάξη, αν και το διαθέσιμο βιβλιογραφικό υλικό είναι σημαντικά περιορισμένο σε σχέση με το γερμανικό.

Λέξεις κλειδιά: μέτρα προστασίας θυμάτων, προστασία θυμάτων, κυβερνοέγκλημα, ηλεκτρονικό έγκλημα, καταπολέμηση κυβερνοεγκλήματος, εγκλήματα κατά γενετήσιας ελευθερίας, παιδική πορνογραφία, προστασία ανηλίκων, hacking, phishing.

Abstract

The subject of this thesis is *"Special provisions for the protection and assistance of victims of cybercrime in the Greek and German legal systems"*. It attempts an in-depth and substantial analysis of the legal framework for the protection of victims of cybercrime in Greece and Germany. This is followed by a comparative study of the established protective measures in the two countries, in which, however, the similarities outweigh the differences. This is achieved not only through the analysis of legal texts - including legislation, judicial decisions, scholarly legal articles, and textbooks - but also through an examination of their practical application and their effectiveness in the fight against cybercrime. An exclusively theoretical approach would not yield the desired real-world results in an issue more timely than ever. The fight against cybercrime is a major issue in the European space, and the rapid evolution of online crimes makes it an urgent necessity for the authorities responsible for combating them. In Greece, there has been a chronologically slow adaptation and implementation of measures that have already been deemed effective in the rest of the European countries. Nevertheless, in recent years, significant progress has been considerable in the Greek legal system, although the available literature is significantly limited compared to the German one.

Keywords: victim protection measures, victim protection, cybercrime, computer crime, combating cybercrime, gender-based violence, child pornography, protection of minors, hacking, phishing.

Στον μπαμπά μου

Ευχαριστίες

Θα ήθελα να ευχαριστήσω από καρδιάς την οικογένειά μου και τους φίλους μου για την βοήθειά και τις πολύτιμες συμβουλές τους κατά τη διάρκεια της έρευνας και συγγραφής τής παρούσας. Ιδιαίτερα, ευχαριστώ τον σύντροφό μου, Θανάση, για την υπομονή και την στήριξη που μου προσέφερε. Ακόμα, ένα πολύ μεγάλο ευχαριστώ στους καθηγητές και διδάσκοντες του μεταπτυχιακού μας προγράμματος. Ειδικότερα, θα ήθελα να ευχαριστήσω τους συνεπιβλέποντες καθηγητές μου, τον πάντοτε ευγενικό κύριο Θεοχάρη Δαλακούρα, ο οποίος αποτελεί έμπνευση για πολλούς από εμάς και ο οποίος ανταποκρίθηκε άμεσα και πρόθυμα σε κάθε προβληματισμό μου, και το κύριο Νικόλαο Δαγκλή, η συμβολή του οποίου ιδιαιτέρως κατά τη διάρκεια της φοίτησής μου ήταν καθοριστική για την εκπόνηση της παρούσας.

Περιεχόμενα

1. Εισαγωγή

Η μεταμόρφωση της κοινωνίας σε ψηφιακή αποτελεί τον κανόνα παγκοσμίως και συνεχίζει να εξελίσσεται με αυξανόμενη δυναμική. Η ανταλλαγή δεδομένων μέσω ηλεκτρονικών δικτύων και τεχνολογίας εξοπλισμένης με τεχνητή νοημοσύνη για την υλοποίηση λειτουργιών που προηγουμένως πραγματοποιούνταν από τον άνθρωπο συναντάται καθημερινά σε όλο και περισσότερους τομείς.

Η εφαρμογή τού νόμου σε αυτήν τη διαδικασία μετασχηματισμού παρουσιάζεται με διττή λειτουργία. Αφενός, πρέπει να προσαρμοστεί προκειμένου να διαμορφωθούν κανόνες που προσιδιάζουν στην νέα αυτή μορφή τής κοινωνίας. Αφετέρου λειτουργεί ως καίριος παράγοντας της μεταμόρφωσης, θέτοντας όρια στην τεχνολογική ανάπτυξη και παρέχοντας ένα πλαίσιο για την εφαρμογή της. Η προστασία των δεδομένων και η ασφάλεια των χρηστών των πληροφοριακών συστημάτων αποτελούν τεχνικούς και νομικούς ακρογωνιαίους λίθους τής ψηφιακής κοινωνίας. Κατ' επέκτασιν, η εποχή τής ψηφιακής τεχνολογίας έχει δημιουργήσει αναμφισβήτητα αρκετές δυνατότητες ανάπτυξης και εξάπλωσης εγκληματικών δραστηριοτήτων με τη χρήση τεχνολογικών μέσων και του διαδικτύου. Το φαινόμενο αυτό δεν αγνοεί σύνορα και η προστασία των θυμάτων τού ηλεκτρονικού εγκλήματος αποτελεί προτεραιότητα για πολλές χώρες παγκοσμίως.

Στο πλαίσιο αυτής της εργασίας, εξετάζονται τα μέτρα προστασίας που έχουν υιοθετηθεί στην Ελλάδα και τη Γερμανία για την προστασία των θυμάτων τού ηλεκτρονικού εγκλήματος, ιδίως σε σχέση με αντίστοιχες ευρωπαϊκές κατευθυντήριες γραμμές. Η επιλογή των δύο χωρών ερείδεται τόσο σε ιστορικούς όσο και σε πρακτικούς λόγους. Το γερμανικό δίκαιο αποτελεί τη βάση δημιουργίας και διατύπωσης των βασικότερων τομέων του ελληνικού δικαίου. Σήμερα, το ελληνικό δίκαιο έχει εξελιχθεί και προσαρμοστεί στις συγκεκριμένες ανάγκες και πραγματικότητα της χώρας, αλλά η επίδραση του γερμανικού δικαίου παραμένει ένα ιστορικό στοιχείο που σχημάτισε τα θεμέλια του ελληνικού νομικού συστήματος. Επιπλέον, και οι δύο χώρες αντιμετωπίζουν παρόμοιες προκλήσεις στον ψηφιακό κόσμο, ενώ η προσέγγιση και οι νομικοί κανόνες που εφαρμόζονται παρουσιάζουν πολλές ομοιότητες και ορισμένες διαφορές.

Μέσα από αυτήν την εργασία, εξετάζεται η νομοθεσία, οι πρακτικές και οι πρωτοβουλίες που έχουν ληφθεί στις δύο αυτές χώρες για την προστασία των θυμάτων τού ηλεκτρονικού εγκλήματος, καθώς και επικαιροποιημένη βιβλιογραφία και σύγχρονα

επιστημονικά άρθρα που πραγματεύονται το θέμα αυτό. Στόχος είναι η κατανόηση της αντιμετώπισης του ζητήματος αυτού σε δύο διαφορετικές πραγματικότητες και η αξιολόγηση της αποτελεσματικότητα των μέτρων που έχουν ληφθεί.

Προκειμένου να καταστεί αυτό δυνατό, κρίνεται σκόπιμο να διασαφηνιστούν, αρχικά, όροι και έννοιες καίριας σημασίας για την κατανόηση της παρούσας. Πιο συγκεκριμένα, στο Κεφάλαιο 2. αναλύεται η έννοια *"ηλεκτρονικό έγκλημα",* τα χαρακτηριστικά αυτού και σκιαγραφείται το προφίλ του δράστη. Στη συνέχεια, στο Κεφάλαιο 3. αναφέρονται τα σημαντικότερα ποινικά αδικήματα που τελούνται μέσω ηλεκτρονικών συστημάτων ή του διαδικτύου, σε σχέση με την αντίστοιχη νομοθεσία. Έπεται το Κεφάλαιο 4., το οποίο παρουσιάζει μεγάλο ενδιαφέρον, καθώς αναλύονται τα μέτρα προστασίας των θυμάτων τού ηλεκτρονικού εγκλήματος, όπως αυτά έχουν μέχρι στιγμής διαμορφωθεί στις δύο χώρες, που αποτελούν το αντικείμενο μελέτης. Ακολούθως, στο Κεφάλαιο 5. περιγράφονται τα ηλεκτρονικά εγκλήματα που συναντώνται συχνότερα στην πράξη με την παράλληλη αναφορά μέτρων προστασίας και αντιμετώπισής τους, σύμφωνα με το περιεχόμενο του Κεφαλαίου 4.. Η εν λόγω διπλωματική εργασία ολοκληρώνεται με το Κεφάλαιο 6., όπου παρατίθενται τα συμπεράσματα που προκύπτουν από την προηγηθείσα μελέτη.

2. Το ηλεκτρονικό έγκλημα

2.1 Όρος Ηλεκτρονικό έγκλημα - Διάκριση ηλεκτρονικού εγκλήματος και κυβερνοεγκλήματος

Γενικότερα, ο όρος *"ηλεκτρονικό έγκλημα"* αναφέρεται σε παράνομες πράξεις που διεξάγονται μέσω ηλεκτρονικών συστημάτων, υπολογιστών, δικτύων και του διαδικτύου και αφορά ποινικά αδικήματα στα οποία η τεχνολογία της πληροφορίας και της επικοινωνίας εντάσσεται στα συστατικά στοιχεία του ποινικού κανόνα. Αυτού του είδους τα εγκλήματα εκμεταλλεύονται τις τεχνολογικές εξελίξεις και την ψηφιακή επικοινωνία για να προκαλέσουν ζημίες, να κλέψουν πληροφορίες, να παραπλανήσουν ή να προκαλέσουν ενοχλήσεις[1]. Στην περίπτωση που το ηλεκτρονικό έγκλημα διαπράττεται με τη χρήση του διαδικτύου και των ψηφιακών συστημάτων, χρησιμοποιείται συχνότερα ο ειδικότερος όρος *"κυβερνοέγκλημα"*, ή *"διαδικτυακό έγκλημα"*, ή *"έγκλημα του κυβερνοχώρου"*. Στο σημείο αυτό, αξίζει να σημειωθεί ότι η διάκριση αυτή παρατηρείται μόνο στον ελληνικό χώρο, ενώ στον ευρωπαϊκό χρησιμοποιείται σε κάθε περίπτωση ο λατινικός όρος *"cybercrime"* ή *"internet crime"*, ήτοι *"κυβερνοέγκλημα"*.

Αρχικά, το ηλεκτρονικό έγκλημα περιελάμβανε ουσιαστικά μορφές εγκληματικότητας, όπως η χειραγώγηση τηλεφωνικών καρτών, η ακατάλληλη χρήση τηλεφωνικών συστημάτων και η δόλια χρήση υπηρεσιών προστιθέμενης αξίας. Ωστόσο, το εύρος στόχου των δραστών έχει διευρυνθεί σημαντικά. Δεν είναι, πλέον, μόνο τα δεδομένα πρόσβασης ενός θύματος που κατασκοπεύονται, αλλά ολόκληρη η ψηφιακή του ταυτότητα.

Επιπλέον, χάρη στη διευρυμένη πρόσβαση στο διαδίκτυο, παρατηρείται σήμερα ιδιαίτερα έντονη αύξηση του εγγεγραμμένου εγκλήματος στον κυβερνοχώρο, στα εγκλήματα που σχετίζονται άμεσα με την τεχνολογία και τον υπολογιστή, όπως η διάπραξη απάτης, η διακίνηση κακόβουλου λογισμικού (malware), η παραβίαση συστημάτων ασφαλείας, η κλοπή δεδομένων (όπως τα προσωπικά στοιχεία ή οι πιστωτικές κάρτες), η διακίνηση πορνογραφικού υλικού ανηλίκων στο διαδίκτυο και άλλες παρόμοιες παράνομες ενέργειες που εκμεταλλεύονται την τεχνολογία. Υπάρχουν διαδικτυακά καζίνο που συχνά χρηματοδοτούν παράνομες πράξεις, ενώ η ανάγκη για ανώνυμες πληρωμές έχει οδηγήσει στην ανάπτυξη των εικονικών συστημάτων πληρωμών και σε εικονικά νομίσματα, όπως το

[1] Δαλακούρας Θ. (2023), σελ. 4.

bitcoin και άλλα κρυπτονομίσματα[2]. Επιπροσθέτως, υποστηρίζεται ότι μέσω του διαδικτύου και των ψηφιακών συστημάτων προσφέρονται τέσσερα βασικά μεγέθη για την τέλεση εγκληματικής δραστηριότητας με κρυπτονομίσματα: φοροδιαφυγή, ξέπλυμα χρήματος, λαθρεμπορία και εκβίαση[3]. Πράγματι, σχεδόν κάθε ποινικό αδίκημα μπορεί να γίνει πιο αποτελεσματικό χρησιμοποιώντας το διαδίκτυο.

2.2 Σύμβαση της Βουδαπέστης

Με στόχο την εναρμόνιση των νομοθεσιών και την ενίσχυση της διεθνούς συνεργασίας για την καταπολέμηση του κυβερνοεγκλήματος και την ενίσχυση της κυβερνοασφάλειας, τα κράτη-μέλη τού Συμβουλίου της Ευρώπης υπέγραψαν στις 23.11.2001 τη *"Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο"*. Με τη Σύμβαση αυτή, η οποία τέθηκε σε ισχύ την 1η Ιουλίου 2004, δόθηκε ένας συγκεκριμένος ορισμός της έννοιας του κυβερνοεγκλήματος. Σύμφωνα με αυτή, το έγκλημα στον κυβερνοχώρο αναφέρεται σε παράνομες δραστηριότητες όπου οι ηλεκτρονικές δομές αποτελούν εργαλείο, στόχο ή τόπο εγκληματικής δραστηριότητας. Η Ελλάδα επικύρωσε αυτήν τη Σύμβαση στις 28 Ιανουαρίου 2005, οπότε έγινε ένα από τα κράτη μέλη που συμμετείχαν στη συμφωνία για τον αγώνα κατά του κυβερνοεγκλήματος στην Ευρώπη, ενώ η Γερμανία πολύ αργότερα στις 27 Νοεμβρίου 2015. Από τον όρο κυβερνοέγκλημα καλύπτονται οι ακόλουθες κατηγορίες εγκλημάτων[4] [5]:

1. Ποινικά αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας δεδομένων και συστημάτων υπολογιστών καλύπτονται από τον όρο κυβερνοέγκλημα και περιλαμβάνουν τα εξής ποινικά αδικήματα:

    a. Κατασκοπεία και υποκλοπή δεδομένων: Ανάκτηση ή παρακολούθηση πληροφοριών χωρίς την άδεια του κατόχου τους, συμπεριλαμβανομένου του ψηφιακού κατασκοπευτικού ρόλου (hacking) και της ανάκτησης πληροφοριών με απόκρυψη της ταυτότητας (phishing).

    b. Τροποποίηση δεδομένων: Αλλαγή ή παραπλάνηση των δεδομένων που αποθηκεύονται σε ηλεκτρονικά συστήματα.

[2] Gercke M. (2023).
[3] Bloomberg J. (2017).
[4] Convention on Cybercrime, Budapest, 23.11.2001 (CETS No. 185), https://rm.coe.int/1680081561.
[5] Δαλακούρας Θ. (2023), σελ. 7-21.

c. Δολιοφθορά υπολογιστών: Καταστροφή ή προκλητική ζημία σε ηλεκτρονικούς υπολογιστές ή δίκτυα.

d. Μόλυνση συστημάτων υπολογιστών με κακόβουλο λογισμικό: Εγκατάσταση κακόβουλου λογισμικού (malware) σε συστήματα υπολογιστών για εξαπάτηση ή παρακολούθηση.

e. Κατασκοπεία δεδομένων - *"hacking, phishing"*: Προσπάθεια εισβολής σε ηλεκτρονικά συστήματα ή απόκτηση πρόσβασης σε πληροφορίες χωρίς άδεια.

f. Διακοπή πρόσβασης σε συστήματα ηλεκτρονικών υπολογιστών: Παρεμπόδιση της λειτουργίας ή της πρόσβασης σε ηλεκτρονικά συστήματα.

g. Κατασκευή, απόκτηση και διάθεση κωδικών πρόσβασης, κωδικών ασφαλείας ή προγραμμάτων ηλεκτρονικών υπολογιστών που στοχεύουν στη διάπραξη εγκλημάτων - *"εργαλεία χάκερ, λογισμικό εγκληματικότητας"*: Διάθεση ή χρήση μέσων για τη διάπραξη εγκλημάτων στον κυβερνοχώρο.

2. Ποινικά αδικήματα που σχετίζονται με υπολογιστές και περιλαμβάνουν δόλιες επιθέσεις σε περιουσιακά στοιχεία, απάτη, απάτη μέσω υπολογιστή και άλλες παραβιάσεις, στις οποίες μπορεί να εμπλακεί η κατάχρηση της ψηφιακής ταυτότητας άλλου ατόμου. Ανάμεσα σε αυτά τα ποινικά αδικήματα περιλαμβάνονται:

   a. Δόλιες επιθέσεις σε περιουσιακά στοιχεία: Αυτό μπορεί να περιλαμβάνει τον παράνομο χειρισμό ή την καταστροφή δεδομένων, η διακίνηση κακόβουλου λογισμικού που προκαλεί οικονομική ζημία, ή άλλες ενέργειες που επηρεάζουν την περιουσία.

   b. Απάτη μέσω υπολογιστή: Αυτό περιλαμβάνει απάτες που διαπράττονται μέσω της χρήσης υπολογιστών ή του διαδικτύου, όπως απάτες μέσω email, ηλεκτρονικές αγορές, ή ψεύτικες ιστοσελίδες.

   c. Παραποίηση και χρήση δεδομένων: Εάν κάποιος παραποιήσει ηλεκτρονικά δεδομένα ή ψηφιακές ταυτότητες για απάτες, παράνομη πρόσβαση ή άλλες παραβιάσεις, αυτό μπορεί να αποτελέσει ποινικό αδίκημα.

   d. Cybermobbing και cyberbullying: Αυτά τα αδικήματα αναφέρονται σε επιθέσεις και παρενόχληση που διαπράττονται διαδικτυακά κατά άλλων

ατόμων, συμπεριλαμβανομένων του cyberbullying (παρενόχλησης παιδιών και εφήβων) και του cybermobbing (παρενόχλησης ενηλίκων).

3. Ποινικά αδικήματα που σχετίζονται με περιεχόμενο στο διαδίκτυο συνήθως περιλαμβάνουν τη μεταφορά, τη διανομή ή την ανάρτηση παράνομου περιεχομένου. Αυτά τα αδικήματα επιβάλλονται για τον έλεγχο και την αποτροπή της διάδοσης επιβλαβούς περιεχομένου στο διαδίκτυο. Ορισμένα παραδείγματα περιλαμβάνουν:

    a. Παιδική πορνογραφία: Η ανάρτηση, η διανομή ή η κατοχή παιδικής πορνογραφίας στο διαδίκτυο αποτελεί ένα από τα πιο σοβαρά αδικήματα που σχετίζονται με το περιεχόμενο στο διαδίκτυο.

    b. Απεικονίσεις βίας: Η δημοσίευση ή η διανομή παράνομων περιεχομένων που περιέχουν απεικονίσεις βίας, σεξουαλικής εκμετάλλευσης ή άλλων εγκληματικών ενεργειών είναι ποινικά αδίκημα.

    c. Προπαγάνδα εγκλημάτων: Η ανάρτηση παράνομων πληροφοριών που προωθούν την πρόκληση βίας, την τρομοκρατία, την παιδική πορνογραφία ή άλλες εγκληματικές ενέργειες είναι παράνομη και αντιμετωπίζεται ως ποινικό αδίκημα.

4. Αδικήματα που σχετίζονται με παραβίαση πνευματικών δικαιωμάτων και συγγενικών δικαιωμάτων και συγκεκριμένα με τη μη εξουσιοδοτημένη εκμετάλλευση έργων που προστατεύονται από πνευματικά δικαιώματα, καθώς και τη μη εξουσιοδοτημένη διανομή εικόνων και αρχείων. Ενδεικτικά αναφέρονται τα παρακάτω παραδείγματα περιλαμβάνουν:

    a. Πειρατεία λογισμικού: Η μη εξουσιοδοτημένη λήψη, αντιγραφή ή διανομή λογισμικού χωρίς την άδεια του δημιουργού αποτελεί παραβίαση πνευματικών δικαιωμάτων και είναι ποινικό αδίκημα.

    b. Πειρατεία μουσικής και ταινιών: Η μη εξουσιοδοτημένη λήψη, αντιγραφή και διανομή μουσικής, ταινιών και άλλου περιεχομένου που προστατεύεται από πνευματικά δικαιώματα αποτελεί παραβίαση των δικαιωμάτων των δημιουργών.

    c. Παραβίαση πνευματικών δικαιωμάτων μέσω δικτύων Peer-to-Peer: Η χρήση συστημάτων κοινής χρήσης αρχείων ή δικτύων peer-to-peer για την μη

εξουσιοδοτημένη διανομή προστατευόμενου περιεχομένου όπως μουσική, ταινίες, βιβλία κ.λπ. μπορεί να αντιμετωπιστεί ως παραβίαση πνευματικών δικαιωμάτων.

5. Σύμφωνα με το πρόσθετο πρωτόκολλο του 2006 που τροποποιεί τη Σύμβαση για το Έγκλημα στον Κυβερνοχώρο του Συμβουλίου της Ευρώπης, πράξεις ρατσιστικού και ξενοφοβικού χαρακτήρα που διαπράττονται μέσω συστημάτων υπολογιστών περιλαμβάνουν τη δημόσια δημοσίευση ή τη διάδοση μηνυμάτων, υλικού, εικόνων ή πληροφοριών που προκαλούν ή ενθαρρύνουν το μίσος, τη βία ή τη διάκριση εις βάρος ατόμων ή ομάδων ατόμων λόγω της φυλετικής καταγωγής, του θρησκευτικού πεπρωμένου, του χρώματος του δέρματος, της καταγωγής, της εθνικότητας, της εθνικής ή εθνοτικής καταγωγής κ.λπ..

Αυτός ο ορισμός λαμβάνει υπόψη τόσο τις εθνικές στρατηγικές ασφάλειας των κρατών-μελών, όσο και τις διεθνείς, καθώς είναι σύμφωνος με διεθνείς ορισμούς, όπως αυτή του Οργανισμού Ηνωμένων Εθνών και του FBI[6].

2.3 Χαρακτηριστικά κυβερνοεγκλήματος[7]

Τα εγκλήματα στον κυβερνοχώρο διακρίνονται από ορισμένα χαρακτηριστικά. Το πρώτο από αυτά, όπως προαναφέρθηκε, αποτελεί η αποτελεσματικότητά τους. Η αποτελεσματικότητα αυτή αναλύεται, πιο συγκεκριμένα στην ευκολία διάπραξης των αδικημάτων και στην έμμεση ή άμεση ανωνυμία από την πλευρά των δραστών για τη διάπραξη του εγκλήματος, ενώ συγχρόνως μειώνονται συνεχώς ψυχολογικές αναστολές των δραστών. Επιπλέον, οι δεξιότητες και τα μέσα για την διάπραξη των εγκλημάτων αυτών είναι πλέον εύκολα προσβάσιμα και ευρέως διαθέσιμα. Ακόμα και η επικοινωνία μεταξύ των δραστών γίνεται μέσω οργανωμένων ομάδων ηλεκτρονικά ή σε φόρουμ και συνομιλίες-chat, ώστε οι εμπλεκόμενοι να παραμένουν ανώνυμοι. Συγκεκριμένα, αποκρύπτουν την τοποθεσία τους με την χρήση διαδικτυακής τηλεφωνίας (VoIP) μέσω διεθνών παρόχων, τεχνικών κρυπτογράφησης και την απόκρυψη των διευθύνσεων IP[8].

Επιπλέον, οι δράστες δυσκολεύουν τις ερευνητικές αρχές να αποκτήσουν πρόσβαση σε αποδεικτικά στοιχεία, αποθηκεύοντας όλο και περισσότερες πληροφορίες και υλικό στο

[6] Wernert M. (2021), σελ. 35.
[7] Δαλακούρας Θ. (2023), σελ. 5.
[8] Ζέκος Γ. (2022), σελ. 390 επ.

διαδίκτυο και όχι στους δικούς τους υπολογιστές. Οι προσπάθειες διακρατικών συνεργασιών για τη δίωξη τους, η οποίες είναι απαραίτητες για την καταπολέμησή τους λόγω του διασυνοριακού τους χαρακτήρα, συχνά δεν ευδοκιμούν, εξαιτίας του γεγονότος ότι οι δράστες ανταποκρίνονται γρήγορα στα μέτρα ασφαλείας, αλλάζοντας αμέσως την προσέγγισή τους και προσαρμόζοντας το εκάστοτε κακόβουλο λογισμικό και τις πρακτικές τους στα νέα δεδομένα[9].

Τα παραπάνω σε συνδυασμό με την ταχύτητα που χαρακτηρίζει τα κυβερνοεγκλήματα, καθώς και το γεγονός ότι δεν δύνανται να περιοριστούν χωρικά, ευνοεί τις συνθήκες τέλεσης τους, ενώ παράλληλα δυσχεραίνει την καταπολέμησή τους. Ως αποτέλεσμα, τα μέτρα ασφαλείας των διωκτικών αρχών έχουν συνήθως βραχυπρόθεσμα αποτελέσματα.

Τέλος, πρέπει να τονιστεί ότι ο αριθμός των μη καταγγελθέντων περιστατικών στο χώρο τού κυβερνοεγκλήματος είναι πολύ υψηλός. Σε πολλές περιπτώσεις, το θύμα δεν αντιλαμβάνεται καν την παραβίαση. Ειδικά στις εμπορικές επιχειρήσεις, ο φόβος για την πιθανή δυσφήμισή τους, συχνά αποτελεί τον κύριο λόγο αδράνειάς τους απέναντι στο κυβερνοέγκλημα. Κατά συνέπεια η απροθυμία για καταγγελία δυσχεραίνει τη διαδικασία τής δίωξης και απόδειξης του διαπραχθέντος εγκλήματος[10].

2.4 Το προφίλ του δράστη

Τα είδη των δραστών στον κυβερνοχώρο ποικίλουν, τα κίνητρά τους και οι τεχνικές τους δεξιότητες είναι εξαιρετικά διαφορετικές. Εκπροσωπούνται όλοι, από αρχάριους έως επαγγελματίες, νεαροί χάκερ που θέλουν να δοκιμάσουν τις ικανότητές τους, εξτρεμιστές, εκβιαστές, τρομοκράτες, ήπιες εγκληματικές δομές και συμμορίες, διεθνώς οργανωμένοι εγκληματίες, υπηρεσίες πληροφοριών από άλλες χώρες. Το προφίλ του δράστη μπορεί να διαφέρει, ανάλογα με τις κατηγορίες των εγκλημάτων και τις συγκεκριμένες σε κάθε περίπτωση δραστηριότητες που διεξάγει. Ωστόσο, υπάρχουν κάποια κοινά χαρακτηριστικά που μπορεί να περιγράψουν τον τυπικό δράστη στον κυβερνοχώρο.

Αρχικά, παρατηρείται συχνά μια τεχνολογική επιδειξιομανία. Οι δράστες στον κυβερνοχώρο, που διαθέτουν προηγμένες τεχνικές γνώσεις, επιδεικνύουν εξαιρετική επιδειξιομανία στον τομέα τής τεχνολογίας. Χρησιμοποιούν αυτές τις γνώσεις για να

[9] Ιγγλεζάκης Ι. (2022), σελ. 215 επ.
[10] Ιγγλεζάκης Ι. (2021), σελ. 399 επ.

διαπράττουν εγκλήματα και για να αποφεύγουν την ανίχνευση με σκοπό κυρίως την κακόβουλη διασκέδαση και ηθική ικανοποίησή τους. Περαιτέρω, οι περισσότεροι έχουν συγκεκριμένα κίνητρα, συνήθως οικονομικών συμφερόντων ή πολιτικής-ακτιβιστικής δράσης, εκμεταλλευόμενοι ασφαλειακά κενά και ευκαιρίες για να εισβάλουν σε συστήματα ή να κλέψουν δεδομένα, ενώ μπορούν να επιτεθούν σε οποιαδήποτε τοποθεσία στον κόσμο, εκμεταλλευόμενοι την ανωνυμία και την απομακρυσμένη φύση της δραστηριότητάς τους.

Ανάλογα με τα κίνητρα και τις δραστηριότητές τους, ενδεικτικά αναφέρονται οι συνηθέστερες κατηγορίες δραστών των ηλεκτρονικών εγκλημάτων[11]:

- Χάκερς (Hackers): Οι χάκερς είναι τεχνικά επιδέξιοι αναλυτές των συστημάτων πληροφορικής και χρησιμοποιούν τις δεξιότητές τους για να εισβάλουν σε συστήματα, να ανακαλύψουν ευπάθειες και να προκαλέσουν προβλήματα ασφαλείας.

- Κυβερνο-εγκληματίες (Cybercriminals): Αυτοί οι δράστες επιδιώκουν τον οικονομικό κέρδος μέσω κυβερνοεγκληματικών δραστηριοτήτων, όπως η απάτη, η κλοπή ταυτότητας, η αποφυγή φορολογικών υποχρεώσεων, και η διακίνηση κακόβουλου λογισμικού.

- Κυβερνο-κακοποιοί (Cyberbullies): Αυτοί οι δράστες επικεντρώνονται στην προκλητική συμπεριφορά και την παρενόχληση στον κυβερνοχώρο, όπως το cyberbullying, το trolling και η αναρίθμητη προκλητική συμπεριφορά στα κοινωνικά δίκτυα και τα φόρουμ.

- Κυβερνο-ακτιβιστές (Hacktivists): Αυτοί οι δράστες εκμεταλλεύονται τις τεχνικές τους γνώσεις για να προωθήσουν πολιτικές ή κοινωνικές αιτίες, οι οποίοι συγκροτούνται συνήθως σε ομάδες και θεωρούν τους εαυτούς τους μαχητές κατά της αδικίας, κατανοούν ότι οι ενέργειές τους αποτελούν πολιτική ανυπακοή, ενώ το κέρδος είναι κυρίως ιδεαλιστικής φύσης.

- Κρατικοί Δράστες (State-sponsored Actors): Ορισμένες κυβερνήσεις χρησιμοποιούν κυβερνο-επιθέσεις για να κατασκοπεύσουν, να αντιμετωπίσουν ανταγωνιστές, ή να επιτύχουν πολιτικούς στόχους. Οι δραστηριότητές τους είναι συνήθως πολύ προηγμένες και δύσκολο να ανιχνευθούν.

[11] Bundeslagebild, BKA (2015),https://www.bka.de/DE/Home/home_node.html.

- Εσωτερικοί Δράστες (Insiders): Οι εσωτερικοί δράστες είναι άτομα που έχουν εσωτερική πρόσβαση σε συστήματα και δίκτυα και μπορούν να εκμεταλλευτούν αυτήν την πρόσβαση για παράνομες ενέργειες.

Επιπροσθέτως, μία ακόμα διάκριση που μπορεί να γίνει σχετικά με τους δράστες και το προφίλ τους, αφορά το επίπεδο γνώσεων και δυνατοτήτων τους. Στην περίπτωση αυτή παρατηρείται ότι ανάλογα με το επίπεδο του δράστη συνδέονται άμεσα τα εργαλεία και τα τεχνικά μέσα που χρησιμοποιεί[12]:

- Αρχάριοι - Script kiddies: άτομα, μικρής συνήθως ηλικίας, με βασικές γνώσεις πληροφορικής, που δεν διαθέτουν τις τεχνικές γνώσεις και τις δεξιότητες που απαιτούνται για να δημιουργήσουν κακόβουλο λογισμικό ή να διεξαγάγουν πολύπλοκες επιθέσεις από το μηδέν. Αντίθετα, βασίζονται σε έτοιμα εργαλεία, προ-προγραμματισμένες εργαλειοθήκες λογισμικού και σενάρια (scripts) που έχουν δημιουργηθεί από άλλους, προκειμένου να εκτελέσουν επιθέσεις. Ασχολούνται κυρίως με το phishing, στον τομέα της κοινωνικής μηχανικής και στο defacement, δηλαδή την αλλαγή ιστοσελίδων. Στόχος τους είναι η απόκτηση εμπειρίας και ο πειραματισμός στο ευρύ φάσμα των δυνατοτήτων που προσφέρει το διαδίκτυο.

- Χάκερ προηγμένων γνώσεων: Οι προηγμένοι χάκερ με υψηλή σχέση με την τεχνολογία είναι σημαντικά πιο επικίνδυνοι. Ξεκινούν δομημένες επιθέσεις, όπως DDoS[13], drive-by exploits[14] ή ενέσεις SQL[15]. Αυτή η κατηγορία έχει καλές δεξιότητες πληροφορικής που της επιτρέπουν να αποκτήσει προσωπικά δεδομένα, εσωτερικές

[12] Wernert M. (2021), σελ. 42-43.
[13] Το DDoS (Διανομής Διακοπής Υπηρεσιών - Distributed Denial of Service) είναι μια είδος κυβερνοεπίθεσης που στοχεύει στο να καταστήσει μια υπηρεσία, ιστότοπο ή δίκτυο ανεπιθύμητο ή μη λειτουργικό για τους χρήστες του. Κατά την επίθεση DDoS, οι δράστες προσπαθούν να υπερφορτώσουν το στόχο με την αποστολή μεγάλου όγκου κυκλοφορίας δεδομένων από διάφορες πηγές, κατακλύζοντας έτσι την υποδομή του και αναγκάζοντάς το να αποτύχει ή να λειτουργεί πολύ αργά (βλ. BSI, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/DoS-Denial-of-Service/dos-denial-of-service_node.html).
[14] Ο όρος Drive-by Exploits (Εκμετάλλευση κατά την διέλευση) αναφέρεται συχνά σε επιθέσεις κατά των ευπαθειών του περιηγητή (browser) του χρήστη. Σε αυτές τις επιθέσεις, οι κυβερνο-επιτιθέμενοι εκμεταλλεύονται αδυναμίες στον περιηγητή του χρήστη, καθιστώντας τον ευάλωτο σε επιθέσεις κατά την απλή επίσκεψη σε μια μολυσμένη ιστοσελίδα. Χωρίς καμία ενέργεια ή κλικ από τον χρήστη, ο κακόβουλος κώδικας εκτελείται αυτόματα στον περιηγητή του χρήστη και μπορεί να οδηγήσει σε κακόβουλο λογισμικό ή απώλεια ευαίσθητων πληροφοριών (βλ. IT-SERVICE.NETWORK, https://it-service.network/it-lexikon/drive-by-exploit).
[15] Οι ενέσεις SQL (SQL Injections) είναι μια είδος κυβερνοεπίθεσης που στοχεύει στην εκμετάλλευση αδυναμιών σε διαδικασίες επικοινωνίας με βάσεις δεδομένων μέσω SQL (Structured Query Language). Οι ενέσεις SQL συμβαίνουν όταν κακόβουλοι χρήστες εισάγουν κακόβουλο κώδικα SQL σε εισόδους που επεξεργάζονται οι εφαρμογές, όπως φόρμες σε ιστοσελίδες ή παραμέτρους σε URL (βλ. BSI, *Sicherheit von Webanwendungen - Maßnahmenkatalog*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/WebSec/WebSec.pdf?__blob=publicationFile&v=1).

πληροφορίες εταιρείας ή εμπιστευτικά κρατικά έγγραφα. Μπορούν να το κάνουν από χόμπι, για οικονομικούς ή ιδεολογικούς λόγους, ατομικά ή και σε οργανωμένες ομάδες.

- Επαγγελματίες χάκερ (professional hackers): Τόσο οι κρατικά κατευθυνόμενοι χάκερ, ήτοι οι *"νόμιμοι"* χάκερ, όσο και οι παράνομοι, μπορούν να ενταχθούν σε αυτήν την κατηγορία. Οι πρώτοι, γνωστοί ως λευκοί χάκερ (White Hat Hackers), που δρουν με σκοπό να βελτιώσουν την κυβερνοασφάλεια. Συνεργάζονται με επιχειρήσεις, οργανισμούς και κυβερνητικούς φορείς για να εντοπίσουν αδυναμίες στα συστήματά τους και να τις επιδιορθώσουν προτού τις εκμεταλλευτεί κάποιος κακόβουλος χάκερ. Οι λευκοί χάκερ εργάζονται συχνά ως ερευνητές ασφαλείας ή σε θέσεις ασφαλείας πληροφοριών (cybersecurity). Αντίθετα, οι μαύροι χάκερ (Black Hat Hackers) είναι κυβερνο-επιτιθέμενοι που δρουν με κακόβουλους σκοπούς. Επιδιώκουν να διαπραγματευτούν, να παραβιάσουν ή να κλέψουν δεδομένα, να προκαλέσουν καταστροφικές επιθέσεις ή να εξαπολύσουν κυβερνοεπιθέσεις για να επιτύχουν προσωπικό όφελος ή κακόβουλους σκοπούς. Στην υποκατηγορία εμπίπτουν οι χακτιβιστές.

3. Σχετικά ποινικά αδικήματα στο νόμο

3.1 Στην Ελλάδα

3.1.1 Ποινικά αδικήματα βάσει του ελληνικού Ποινικού Κώδικα (ΠΚ)

Στον ποινικό κώδικα της Ελλάδας (Ν. 4619/201, όπως αυτός τροποποιήθηκε με τον 4855/2021 και πιο πρόσφατα με τον Ν. 4947/2022), τα ηλεκτρονικά εγκλήματα αναφέρονται στις παραβάσεις που σχετίζονται με την παράνομη χρήση των ηλεκτρονικών συστημάτων και των πληροφοριών. Αυτά τα εγκλήματα αφορούν παράνομες δραστηριότητες που λαμβάνουν χώρα μέσω της διαδικτυακής πλατφόρμας και της ηλεκτρονικής επικοινωνίας.

Ορισμένες πράξεις που αποτελούν ηλεκτρονικά εγκλήματα σύμφωνα με τον εν λόγω νόμο περιλαμβάνουν τα εξής:

- Απάτη με υπολογιστή (άρθρο 386Α): Η με σκοπό το προσωπικό όφελος του δράστη ή τρίτου μέσω του επηρεασμού των στοιχείων του υπολογιστή που οδηγεί άμεσα στη βλάβη ξένης περιουσίας.

- Παράνομη πρόσβαση σε πληροφοριακό σύστημα (άρθρο 370Γ): Η παράνομη πρόσβαση σε πληροφοριακό σύστημα και σε ψηφιακά δεδομένα χωρίς την εξουσιοδότηση του κατόχου των πληροφοριών.

- Παραβίαση του απορρήτου τηλεφωνικής επικοινωνίας και προφορικής συνομιλίας (άρθρο 370Α): Η παράνομη παρακολούθηση ή καταγραφή επικοινωνιών, όπως η παρακολούθηση των ηλεκτρονικών μηνυμάτων χωρίς τη συναίνεση των εμπλεκομένων.

- Απαγόρευση διακίνησης λογισμικών, συσκευών παρακολούθησης και άλλων δεδομένων (άρθρο 370ΣΤ): Η διάδοση λογισμικού ή συσκευών με δυνατότητα υποκλοπής, καταγραφής και κάθε είδους άντλησης περιεχομένου ή και δεδομένων επικοινωνίας (κίνησης και θέσης), με τα οποία μπορούν να τελεστούν οι πράξεις παραβίασης του απορρήτου τηλεφωνικής επικοινωνίας και προφορικής συνομιλίας.

- Διάδοση παιδικού πορνογραφικού υλικού (άρθρο 348): Η διάδοση, απόκτηση, αποθήκευση ή κατοχή παιδικού πορνογραφικού υλικού αποτελεί σοβαρό ποινικό αδίκημα.

Όπως προαναφέρθηκε, στην Ελλάδα, οι πτυχές που σχετίζονται με τα ηλεκτρονικά εγκλήματα τυποποιούνται κυρίως στον ποινικό κώδικα, ωστόσο υπάρχουν και άλλα νομοθετήματα και κανονισμοί σχετικά με αυτά, τα οποία στην ουσία αποτελούν ενσωμάτωση των αντίστοιχων ευρωπαϊκών κανονισμών στην εγχώρια νομοθεσία. Πιο συγκεκριμένα:

3.1.2 Νόμος 2121/1993 περί πνευματικής ιδιοκτησίας, συγγενικών δικαιωμάτων και πολιτιστικών θεμάτων

Με το νόμο 2121/1993 περί πνευματικής ιδιοκτησίας, συγγενικών δικαιωμάτων και πολιτιστικών θεμάτων τυποποιείται νομικά η προστασία των πνευματικών δικαιωμάτων, μεταξύ άλλων παραβάσεων, από την παράνομη εγγραφή, αντιγραφή, αναπαραγωγή, μετατροπή, παρουσίαση και διάδοση με οποιοδήποτε μέσο, πράξεις για την τέλεση των οποίων συχνά χρησιμοποιούνται ψηφιακά συστήματα και το διαδίκτυο, ενώ συχνά το ίδιο το έργο βρίσκεται σε ψηφιακή μορφή.

3.1.3 Νόμος 3471/2006 για τις Ηλεκτρονικές Επικοινωνίες

Ο Νόμος 3471/2006 για τις Ηλεκτρονικές Επικοινωνίες ρυθμίζει τις ηλεκτρονικές επικοινωνίες στην Ελλάδα και ορίζει κανόνες για την προστασία των δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.

3.2 Στη Γερμανία

3.2.1 Ποινικά αδικήματα βάσει του γερμανικού Ποινικού Κώδικα - Strafgesetzbuch (StGB)

Οι διατάξεις ενημερώθηκαν από τον 41ο νόμο τροποποίησης του ποινικού δικαίου για την καταπολέμηση του εγκλήματος ηλεκτρονικών υπολογιστών και ο οποίος τέθηκε σε ισχύ στις 11 Αυγούστου 2007. Οι αλλαγές βασίστηκαν στην απόφαση-πλαίσιο της ΕΕ για τις επιθέσεις κατά των συστημάτων πληροφοριών και στη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο. Ενδεικτικά, εγκλήματα που εμπίπτουν σε αυτήν την κατηγορία είναι τα ακόλουθα:

- Παράνομη πρόσβαση σε δεδομένα (§ 202c StGB): Αυτό περιλαμβάνει την παράνομη πρόσβαση ή χρήση δεδομένων, όπως προσπάθεια απόκτησης πρόσβασης σε προστατευμένα δεδομένα.

- Κακοβουλία σε συστήματα πληροφορικής (§ 303a StGB): Αυτό περιλαμβάνει την παράνομη παρέμβαση σε συστήματα πληροφορικής, όπως η διατάραξη, η καταστροφή ή η παρεμπόδιση της λειτουργίας τους.

- Διακίνηση κακόβουλου λογισμικού (§ 202b StGB): Αυτό αναφέρεται στη διάδοση κακόβουλου λογισμικού, όπως ιοί, τρόιανοι ίπποι, κλπ.

- Κλοπή προσωπικών δεδομένων (§ 202a StGB): Αυτό αναφέρεται στην παράνομη απόκτηση ή χρήση προσωπικών δεδομένων.

- Ηλεκτρονική απάτη (§ 263a StGB): Αυτό περιλαμβάνει παράνομες δραστηριότητες που οδηγούν σε οικονομική ζημία, όπως η ψευδής παρουσίαση, η απάτη και άλλες παρόμοιες πρακτικές μέσω ηλεκτρονικών μέσων.

- Παραβίαση απορρήτου επικοινωνίας (§ 202 StGB): Αυτό αναφέρεται στην παράνομη παρακολούθηση, καταγραφή ή αποκάλυψη επικοινωνιών χωρίς την άδεια των εμπλεκομένων.

- Διάδοση παιδικού πορνογραφικού υλικού (§ 184b StGB): Η διάδοση, απόκτηση, αποθήκευση ή κατοχή παιδικού πορνογραφικού υλικού αποτελεί σοβαρό ποινικό αδίκημα.

- Διαδικτυακή συκοφαντία (§ 187 StGB): Η ψευδής ανάρτηση πληροφοριών στο διαδίκτυο με σκοπό την προκλητική ζημία σε άλλα άτομα.

- Επίθεση κατά της ασφάλειας δεδομένων (§ 202d StGB): Αυτό αναφέρεται στην παράνομη πρόκληση ζημίας σε συστήματα πληροφορικής μέσω ανεπιθύμητων προγραμμάτων, όπως η διάδοση ιών. Με την εισαγωγή του άρθρου 202d StGB, η απόκτηση δεδομένων που δεν είναι γενικά προσβάσιμα και τα οποία κάποιος άλλος έχει λάβει παράνομα τιμωρείται επίσης ως κλοπή δεδομένων[16].

- Διαδικτυακή εκβίαση (§ 253b StGB): Αυτό αναφέρεται στην παράνομη εκβίαση άλλων ατόμων μέσω διαδικτύου, όπως η απειλή δημοσίευσης προσωπικών πληροφοριών.

[16] Bär W. (2013), CybercrimeBKAhttps://www.bka.de › Herbsttagungen › 2013 › he…

3.2.2 Νόμος περί πνευματικών και συγγενικών δικαιωμάτων - Gesetz über Urheberrecht und verwandte Schutzrechte (UrhG)

Σύμφωνα με τον Νόμο περί Πνευματικών και Συγγενικών δικαιωμάτων, η αντιγραφή, αναπαραγωγή, επεξεργασία, διακίνηση και παρουσίαση προστατευόμενων έργων απαγορεύεται γενικά, χωρίς τη συγκατάθεση του κατόχου του δικαιώματος, παρατηρώντας πολλές ομοιότητες με τον αντίστοιχο ελληνικό νόμο, τόσο ως προς το αντικείμενο, όσο και ως προς τα μέτρα προστασίας.

3.2.3 Νόμος περί τηλεπικοινωνιών - Telekommunikationsgesetz (TKG)

Ο νόμος περί Τηλεπικοινωνιών στοχεύει στην προώθηση του ανταγωνισμού στον τομέα των τηλεπικοινωνιών και της αποδοτικής τηλεπικοινωνιακής υποδομής μέσω μιας νομοθεσίας που είναι τεχνολογικά ουδέτερη. Επιπλέον, ο νόμος επιδιώκει να εξασφαλίσει επαρκείς και ποιοτικές υπηρεσίες τηλεπικοινωνιών για όλους τους τομείς. Μεταξύ άλλων στόχων, προστατεύει τα συμφέροντα των χρηστών, ιδίως των καταναλωτών στον τομέα των τηλεπικοινωνιών, διασφαλίζει το απόρρητο των τηλεπικοινωνιών και προστατεύει τα συμφέροντα της δημόσιας ασφάλειας. Το δεύτερο τμήμα του Μέρους 7 (Teil 7, Abschnitt 2) του νόμου περιέχει βασικούς κανονισμούς για την προστασία δεδομένων. Το τρίτο τμήμα του ίδιου μέρους περιέχει προδιαγραφές για τους παρόχους τηλεπικοινωνιακών υπηρεσιών και κανονισμούς για αιτήματα για πληροφορίες από αρχές ασφαλείας, ενώ στις διατάξεις 148 και 149 TKG προβλέπονται ποινικές κυρώσεις και πρόστιμα για τους παραβάτες.

3.3 Στην Ευρωπαϊκή Ένωση

3.3.1 Οδηγία 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την Ασφάλεια των Δικτύων και των Πληροφοριών

Η Οδηγία 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την Ασφάλεια των Δικτύων και των Πληροφοριών εισήγαγε το πλαίσιο για τον ορισμό και την καταπολέμηση των ηλεκτρονικών εγκλημάτων, περιλαμβάνοντας διάφορες παραβιάσεις, όπως η παράνομη πρόσβαση σε συστήματα, η παράνομη διάθεση προσωπικών δεδομένων, η παράνομη κατακράτηση ή χρήση κωδικών πρόσβασης, και θέτει τις βάσεις για την αύξηση της κυβερνοασφάλειας σε κρίσιμους τομείς όπως η ενέργεια, η μεταφορά, οι υδροδότηση, η υγεία, και η χρηματοοικονομική υποδομή. Επίσης, η Οδηγία προβλέπει υποχρεώσεις για τους

παρόχους υπηρεσιών ψηφιακών υπηρεσιών, ενδεχομένως θέτει απαιτήσεις για την αναφορά περιστατικών ασφάλειας, και περιλαμβάνει μέτρα για την αντιμετώπιση κυβερνοεγκλημάτων και την ενίσχυση της συνεργασίας μεταξύ των κρατών μελών σε θέματα κυβερνοασφάλειας. Στην Ελλάδα ενσωματώθηκε με τον Ν. 4577/2018 περί ηλεκτρονικού εγκλήματος και στην Γερμανία με τον *"Νόμο για την ασφάλεια των δικτύων και των πληροφοριών"* (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme - IT-Sicherheitsgesetz).

3.3.2 Γενικός Κανονισμός Προστασίας Δεδομένων [Κανονισμός (ΕΕ) 2016/679], γνωστός και ως General Data Protection Regulation - GDPR

Ο Γενικός Κανονισμός Προστασίας Δεδομένων αποτελεί μια ολοκληρωμένη νομική προσέγγιση για την προστασία των δεδομένων των ατόμων και την ρύθμιση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε όλα τα κράτη μέλη της ΕΕ και ισχύει για όλους τους φορείς επεξεργασίας δεδομένων που λειτουργούν στην επικράτεια της ΕΕ, ανεξάρτητα από το πού βρίσκονται φυσικά ή νομικά πρόσωπα. Στην Ελλάδα, η ενσωμάτωση του στο εθνικό δίκαιο πραγματοποιήθηκε με την έγκριση του *"Νόμου περί προστασίας φυσικών προσώπων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία αυτών των δεδομένων"* (Ν. 4624/2019), ενώ στην Γερμανία με την έγκριση του *"Bundesdatenschutzgesetz (BDSG) - Ομοσπονδιακός Νόμος για την Προστασία των Δεδομένων"* του 2017, που αντικατέστησε τον προηγούμενο νόμο περί προστασίας δεδομένων και ενσωμάτωσε τις απαιτήσεις του GDPR στη γερμανική νομοθεσία.

4. Μέτρα προστασίας θυμάτων ηλεκτρονικού εγκλήματος

Πέραν της κείμενης νομοθεσίας που ποινικοποιεί τα αδικήματα που σχετίζονται με το ηλεκτρονικό έγκλημα, τόσο το ελληνικό, όσο και το γερμανικό νομικό σύστημα, εναρμονισμένα με τα όσα ορίζει η αντίστοιχη ευρωπαϊκή νομοθεσία, προβλέπουν συγκεκριμένα μέτρα προστασίας για τα θύματα των ηλεκτρονικών εγκλημάτων.

4.1 Αναφορά - Καταγγελία

Κατ' αρχήν, το θύμα δύναται να αναφέρει το συμβάν στην αστυνομία, η οποία θα ερευνήσει και θα διώξει τους δράστες, εάν είναι δυνατόν. Η αναφορά αυτή μπορεί να γίνει προφορικά ή ορθότερα και για λόγους ασφάλειας και απόδειξης γραπτά, σε μορφή εντύπου καταγγελίας. Έτσι, τα στοιχεία καταγράφονται με σαφήνεια και μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία σε περίπτωση που απαιτείται δικαστική εξέταση ή έρευνα.

Αξίζει να σημειωθεί ότι στην Γερμανία, εδώ και αρκετά χρόνια, οποιαδήποτε καταγγελία μπορεί να γίνει και ηλεκτρονικά[17] [18], γεγονός το οποίο διευκολύνει την καταγραφή των στοιχείων του εγκλήματος, ιδίως του ηλεκτρονικού, και των διαθέσιμων στο θύμα πειστηρίων με ακρίβεια και λεπτομέρεια[19], με την καταγραφή ιστοτόπων, υπερσυνδέσμων, ή ακόμα και της διεύθυνσης IP, εφόσον πρόκειται για έναν πιο έμπειρο χρήστη ηλεκτρονικού υπολογιστή. Η αμεσότητα και η ταχύτητα, όσον αφορά τέτοιου είδους πειστήρια, είναι σημαντική, ώστε να αποτραπεί η αλλοίωσή τους.

Από τον Μάιο του 2022 αντίστοιχη πλατφόρμα ξεκίνησε να λειτουργεί και στην Ελλάδα[20]. Η πλατφόρμα αυτή αφορά, ωστόσο, μόνο τις περιπτώσεις καταγγελίας και δίωξης ηλεκτρονικών εγκλημάτων και συγκεκριμένα αδικήματα τελούμενα σε βάρος ανηλίκων μέσω διαδικτύου, οικονομικά κυβερνοεγκλήματα όπου εμπλέκονται ηλεκτρονικά/ψηφιακά νομίσματα, την παραβίαση του απορρήτου των ηλεκτρονικών και τηλεφωνικών επικοινωνιών, την παράνομη διακίνηση οπτικοακουστικών έργων μέσω διαδικτύου, την παράνομη πρόσβαση σε ηλεκτρονικό υπολογιστή και περιπτώσεις απάτης με υπολογιστή[21].

---

[17] Bundeskriminalamt, BKA, https://www.bka.de/SharedDocs/FAQs/DE/Anzeige/anzeigeFrage01.html.
[18] Polizei Nordrhein-Westfallen, https://internetwache.polizei.nrw/ich-moechte-eine-anzeige-erstatten.
[19] Polizei Nordrhein-Westfallen, https://formulare.polizei.nrw/ams/anzeige/wizardng/FFE7CD?v=1694083797072.
[20] Ελληνική Δημοκρατία η Κυρβέρνηση (2022), https://www.government.gov.gr/meso-gov-gr-katangelies-sti-dioxi-ilektronikou-egklimatos/.
[21] gov.gr, https://www.gov.gr/org/astynomia/kataggelies.

Τόσο στην Ελλάδα, όσο και στην Γερμανία, η πλειοψηφία των ηλεκτρονικών εγκλημάτων διώκεται κατ' έγκληση, δηλαδή ο ίδιος ο παθών θα πρέπει να αναφέρει το έγκλημα, ώστε να εκκινήσει η διαδικασία τής ποινικής δίωξης[22]. Σύμφωνα με το γερμανικό δίκαιο, βέβαια, τα εγκλήματα στον κυβερνοχώρο ανήκουν στην υποκατηγορία των σχετικώς κατ' έγκληση διωκόμενων, δηλαδή αυτών που μπορούν να διωχθούν ακόμη και αν δεν έχει υποβληθεί έγκληση, αλλά ο εισαγγελέας επιβεβαιώνει ότι υπάρχει ειδικό δημόσιο συμφέρον για την ποινική δίωξη, έναντι των αποκλειστικά κατ' έγκληση, στα οποία σε κάθε περίπτωση απαιτείται η προηγούμενη κατάθεση έγκλησης από τον παθόντα[23].

4.2 Αποζημίωση θυμάτων

Τα θύματα του ηλεκτρονικού εγκλήματος μπορούν, επίσης, να ζητήσουν αποζημίωση για τυχόν ζημίες που έχουν υποστεί ως αποτέλεσμα του εγκλήματος, κατ' αρχήν με τη δήλωση παράστασης προς υποστήριξη της κατηγορίας.

4.2.1 Στην Ελλάδα

Ειδικότερα, όμως, με το Νόμο 3811/2009, που αφορά την *"Αποζημίωση Θυμάτων Εγκληματικής Βίας",* προστατεύονται τα θύματα εγκληματικής βίας και παρέχονται ειδικότεροι μηχανισμοί για την αποζημίωσή τους. Ορισμένα από τα βασικά σημεία τού Ν. 3811/2009 περιλαμβάνουν τον καθορισμό των θυμάτων, την αποζημίωση τους και τον καθορισμό της διαδικασίας αποζημίωσης.

Λόγω της διασυνοριακής φύσης των συγκεκριμένων εγκλημάτων, της ανωνυμίας των δραστών και των γενικότερων χαρακτηριστικών τους, το θύμα αδυνατούσε να αποζημιωθεί τόσο για την ηθική, όσο και για την σωματική ζημία που υπέστη. Η αναγνώριση δυνατότητας αποκατάστασης των θυμάτων από το εθνικό δίκαιο, όπως και η ποινικοποίηση των εν λόγω εγκληματικών συμπεριφορών, καθυστέρησε στην Ελλάδα και πραγματοποιήθηκε, εν τέλει, με τον Ν. 3811/2009, κατ' εναρμόνιση της ελληνικής νομοθεσίας με την Οδηγία 2004/80/ΕΚ του Συμβουλίου της Ευρωπαϊκής Ένωσης της 29ης Απριλίου 2004.

Πιο συγκεκριμένα, στο πρώτο άρθρο τού νόμου αυτού ορίστηκε η σύσταση της Ελληνικής Αρχής Αποζημίωσης Θυμάτων Εγκληματικών Πράξεων, η οποία αποφαίνεται, κατά τις διατάξεις του άρθρου 3, επί των αιτήσεων αποζημίωσης των θυμάτων εγκλημάτων

[22] Παπαδαμάκης Α. (2021), σελ. 266-270.
[23] Jura Forum (2022), https://www.juraforum.de/lexikon/antragsdelikte.

βίας από πρόθεση. Για την εφαρμογή του Ν. 3811/2009 απαραίτητα στοιχεία αποτελούσαν η χρήση σωματικής βίας ή η απειλή αυτής, με συνέπεια να επέλθει ο θάνατος ή η βαριά σωματική ή διανοητική βλάβη, ενώ η περιπτωσιολογία της σωματεμπορίας καταδεικνύε την εκμετάλλευση της ευάλωτης θέσης του θύματος ως την συχνότερη μορφή τέλεσης. Επίσης, είχε εξαιρεθεί ρητά η υπαγωγή του εγκλήματος της εμπορίας ανθρώπων από το πεδίο εφαρμογής του εν λόγω νόμου, εφόσον δεν επέρχεται θάνατος ή βαριά σωματική βλάβη[24].

Επομένως, κατέστη άμεσα σαφές ότι ήταν απαραίτητες ορισμένες αλλαγές, προκειμένου να βελτιωθεί και να επιτευχθεί και να διευκολυνθεί η εν τοις πράγμασι προστασία της αποζημίωσης των θυμάτων. Με τον Ν. 4198/2013 και συγκεκριμένα με το άρθρο 5 παρ. 1 και παρ. 2 τροποποιήθηκαν τα άρθρα 1 παρ. 1 και 3 παρ. 1 του ως άνω νόμου και πλέον νομιμοποιούνται αυτοτελώς να αιτηθούν αποζημιώσεως τα θύματα των 323Α και 351 του Ποινικού Κώδικα.

Επιπροσθέτως, με το άρθρο 17 παρ 1α και 1β του Ν. 4267/2014, το οποίο ενσωμάτωσε το άρθρο 20 της Οδηγία 2011/93/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαίσιο 2004/ 68/ ΔΕΥ του Συμβουλίου, διευρύνεται το πεδίο δικαιούχων θυμάτων αποζημίωσης, κατά τον Ν. 3811/2009, συμπεριλαμβάνοντας αυτά των άρθρων 323, 323Β, 339 παράγραφοι 1 και 4, 342 παράγραφοι 1 και 2, 348Α, 348Β, 348Γ, 349, 351Α και του 366 ΠΚ όταν αφορά ανήλικο.

Πιο συγκεκριμένα, σχετικά με την αξίωση προς αποζημίωση, αυτή υπάρχει στην περίπτωση που ο δράστης δεν διαθέτει τους απαιτούμενους οικονομικούς πόρους, ώστε να αποζημιώσει το θύμα κατά την έκδοση αμετάκλητης καταδικαστικής απόφασης, στην περίπτωση που δεν μπορεί να εξακριβωθεί η ταυτότητα του, καθώς και όταν ο δράστης δεν μπορεί να διωχθεί ποινικά ή να του επιβληθεί ποινή, όταν τίθεται η δικογραφία στο αρχείο με πράξη του αρμόδιου εισαγγελέα ή με την έκδοση αμετάκλητου απαλλακτικού βουλεύματος ή από την έκδοση αμετάκλητης αθωωτικής απόφασης ή με την οριστική περάτωση της υπόθεσης (άρθρο 3 παρ. 2). Απαραίτητη προϋπόθεση για υποβολή αίτησης αποζημίωσης στην πρώτη και τρίτη περίπτωση από την πλευρά του παθόντος συνιστά η αδυναμία του να

[24] Σύμφωνα με την Αιτιολογική Έκθεση του άρθρου 3, παρ. 3 του νόμου για τον αποκλεισμό της εμπορίας ανθρώπων από το πεδίο εφαρμογής του δεν ήταν βάσιμη, εφόσον η έστω, περιορισμένη, νομολογία των ελληνικών δικαστηρίων έχει να επιδείξει περιπτώσεις καταδίκης για βαριά σωματική βλάβη στα θύματα εμπορίας ανθρώπων.

ικανοποιήσει την αξίωση αποζημίωσης εναντίον του δράστη, εφόσον αυτή προσδιορίστηκε με τελεσίδικη απόφαση (άρθρο 3 παρ. 3).

Στις ως άνω προστατευτικές ρυθμίσεις, ανήκουν επιπλέον η υποχρέωση των ανακριτικών, προανακριτικών και εισαγγελικών αρχών για ενημέρωση του θύματος σχετικά με το δικαίωμά προς αποζημίωση (άρθρο 4 παρ. 3), η δυνατότητα της Αρχής να ερευνήσει την περιουσιακή κατάσταση του δράστη των εγκλημάτων (άρθρο 4 παρ. 4), η δυνατότητα κλήσης και εξέτασης του δράστη ή και τρίτων προσώπων από την Αρχή (άρθρο 6 παρ. 1) και η πρόβλεψη καταβολής αποζημίωσης για ιατρικά έξοδα, νοσήλια, απώλεια εισοδήματος και έξοδα κηδείας (άρθρο 8 παρ.2). Επιπροσθέτως, στο άρθρο 12 προβλέπεται η δυνατότητα άσκησης προσφυγής στον αιτούντα και στο Ελληνικό Δημόσιο ενώπιον του Διοικητικού Πρωτοδικείου. Συνεπώς, καθίσταται πρόδηλο, ότι η προσφυγή στην Αρχή για αποζημίωση συνιστά ένα επικουρικό ένδικο βοήθημα, εφόσον η αντίστοιχη απόφαση της Αρχής υπόκειται σε προσφυγή ενώπιον του Διοικητικου Πρωτοδικείου[25].

Σχετικά, ωστόσο, με τα παραπάνω, έχουν δημιουργηθεί στην πράξη πλείστα ζητήματα και προβληματισμοί, για τα οποία μέχρι και σήμερα δεν έχει δοθεί λύση. Αρχικά, δικαιούχοι της ως άνω αποζημίωσης είναι όσοι έχουν την κατοικία ή τη συνήθη διαμονή του σε κάποιο κράτος-μέλος της Ευρωπαϊκής Ένωσης, γεγονός που έρχεται σε πλήρη αντίθεση με το άρθρο 14 της ΕΣΔΑ περί απαγόρευσης των διακρίσεων[26] [27]. Επιπλέον, τα κριτήρια αδυναμίας τού δράστη για καταβολή αποζημίωσης στο θύμα, καθώς και για το ύψος αυτής, στην περίπτωση καταβολής της από το κράτος, παραμένουν ρευστά και κρίνονται ad hoc κατά περίπτωση, ενώ η αρχή τής αναλογικότητας συμβάλει ερμηνευτικά για τον προσδιορισμό τού ποσού τής αποζημίωσης[28].

4.2.2 Στη Γερμανία

Στην Γερμανία η παραπάνω Οδηγία εφαρμόζεται σε συνδυασμό με τον νόμο περί αποζημίωσης θυμάτων (Opferentschädigungsgesetz - OEG), ο οποίος προβλέπει την παροχή αποζημίωσης σε θύματα εγκλημάτων, συμπεριλαμβανομένου του εγκλήματος στον

[25] Μίχα Ε. (2016).
[26] Απόφαση ΔΕΕ της 5ης Ιουνίου 2008, στην υπόθεση C-164/0, *James Wood v Fonds de garantie des victimes des actes de terrorisme et d'autres infractions,* https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62007CJ0164, 25.07.2023.
[27] Brodowski D. (2021), σελ. 382.
[28] Μιαούρας Κ. (2018), σελ. 74.

κυβερνοχώρο, που έχουν υποστεί σωματική ή ψυχολογική βλάβη[29]. Ο νόμος για την αποζημίωση θυμάτων είναι απόρροια της αρχής του κράτους πρόνοιας του άρθρου 20 παρ. 1 του Συντάγματος (GG). Βασίζεται στην ιδέα ότι το κράτος είναι υπεύθυνο για την προστασία των πολιτών του από πράξεις βίας και εγκληματικές πράξεις, επειδή είναι υπεύθυνο για την καταπολέμηση και την πρόληψη του εγκλήματος και έχει το μονοπώλιο στη χρήση βίας.

Ως εκ τούτου, τα άτομα που είναι θύματα βίαιης πράξης στο έδαφος της Ομοσπονδιακής Δημοκρατίας της Γερμανίας και που υφίστανται βλάβη στην υγεία τους ως αποτέλεσμα δικαιούνται αποζημίωση για τα θύματα (ενότητα 1 άρθρο 1 OEG). Οι επιζώντες συγγενείς του θύματος δικαιούνται επίσης την αξίωση εάν ο παθών πέθανε ως αποτέλεσμα της βίαιης πράξης (ενότητα 1 άρθρο 5 OEG).

Κατόπιν τροποποίησης του νόμου το 2009, από την 1η Ιουλίου 2008, και με στόχο την αντιστάθμιση των υγειονομικών και οικονομικών συνεπειών τέτοιων πράξεων, παρέχονται επίσης παροχές στο πλαίσιο του OEG εάν ο ζημιωθείς έπεσε θύμα βίαιης πράξης στο εξωτερικό, ακόμα και αναδρομικά, εφόσον ο παθών να διαμένει στη Γερμανία και βρισκόταν μόνο προσωρινά (έως έξι μήνες) εκτός Γερμανίας τη στιγμή του εγκλήματος (ενότητα 3a OEG). Σε κάθε περίπτωση, προϋποτίθεται, ότι το θύμα δεν φέρει υπαιτιότητα στην πρόκληση της ζημίας.

Στην περίπτωση που το θύμα κατοικεί σε κράτος-μέλος της ΕΕ, εφαρμόζεται η Οδηγία 2004/80/ΕΚ για την αποζημίωση των θυμάτων εγκληματικών πράξεων σε διασυνοριακές υποθέσεις. Στη Γερμανία, το ρόλο της Γερμανικής Αρχής Υποστήριξης έχει αναλάβει το Ομοσπονδιακό Υπουργείο Εργασίας και Κοινωνικών Υποθέσεων, το οποίο εφόσον παραστεί ανάγκει, επικοινωνεί με την αντιστοιχεί αρμόδια αρχή άλλου κράτους-μέλους, παρέχει μεταφραστικές υπηρεσίες και συνοδεύει τη διαδικασία. Σε κάθε περίπτωση, η αίτηση αποζημίωσης κατά την Οδηγία αυτή δεν αναιρεί την δυνατότητα υποβολής αίτησης αποζημίωσης κατά των OEG, ή το αντίστροφο. Φυσικά ο παθών δεν λαμβάνει διπλές παροχές ή αποζημίωση, αλλά κατόπιν συνεργασίας των αρμοδίων αρχών, παρέχονται η αντίστοιχη βοήθεια και υπηρεσίες. Εάν άλλο κράτος-μέλος, για παράδειγμα,

[29] BMAS (2021), https://www.bmas.de/DE/Soziales/Soziale-Entschaedigung/Opferentschaedigungsrecht/opferentschaedigungsrecht-art.html.

καταβάλει αποζημίωση στο θύμα, αυτή θα συμψηφιστεί με τα οφέλη που ενδέχεται να χορηγηθούν βάσει του OEG[30].

Ο κεντρικός κανόνας τού νόμου περί αποζημίωσης θυμάτων είναι η ενότητα 1 παρ. 1 OEG, η οποία ρυθμίζει το δικαίωμα αποζημίωσης. Σύμφωνα με αυτό, όποιος έχει υποστεί βλάβη στην υγεία του ως αποτέλεσμα εκ προθέσεως, παράνομης σωματικής επίθεσης, δικαιούται περίθαλψης. Ως σωματική επίθεση νοείται κάθε άμεση εχθρική επίθεση στο σώμα κάποιου άλλου, χωρίς να είναι απαραίτητο να συνέβη πράγματι σωματική επαφή. Σύμφωνα με τη νομολογία του Ομοσπονδιακού Κοινωνικού Δικαστηρίου (BSG), για την επίθεση πρέπει επίσης να ελεγχθεί εάν η υγεία του θύματος βλάπτεται μόνο ως αποτέλεσμα της απόδρασης, για παράδειγμα πέφτοντας από το παράθυρο[31].

Η επίθεση δεν πρέπει απαραίτητα να στρέφεται εναντίον του ίδιου του ζημιωθέντος μέρους, αλλά μπορεί επίσης να στρέφεται εναντίον άλλου ατόμου (π.χ. του συντρόφου ή τρίτου προσώπου). Αυτό περιλαμβάνει επίσης τη λεγόμενη ζημιά από σοκ από άτομα που δεν τραυματίστηκαν άμεσα από το έγκλημα, π.χ. αυτόπτες μάρτυρες. Η αξίωση υφίσταται επίσης εάν η βλάβη στην υγεία προκλήθηκε μέσω της νόμιμης υπεράσπισης της επίθεσης (π.χ. μέσω αυτοάμυνας). Ωστόσο, η επίθεση πρέπει να είναι σκόπιμη, τόσο ως προς την επίθεση όσο και για τη βλάβη στην υγεία (από την άποψη αυτή αρκεί η υπό όρους πρόθεση), αλλά όχι όσον αφορά τις συγκεκριμένες συνέπειες της ζημίας.

Στη συνέχεια, στην ενότητα 2 OEG προβλέπονται ως εξαίρεση λόγοι άρνησης που μπορούν να αποκλείσουν την αξίωση για αποζημίωση, με κυριότερη την περίπτωση όπου ο ζημιωθείς προκάλεσε ο ίδιος τη ζημία (ενότητα 2 παρ. 1 προτ. 1 OEG). Άλλοι λόγοι άρνησης είναι να ανήκει ο ζημιωθείς στο οργανωμένο έγκλημα, (ενότητα 2 παρ. 1 προτ. 2 αρ. 3 OEG), αν εμπλέκεται ή συμμετέχει ενεργά σε πολιτικές διαμάχες στο κράτος καταγωγής του (ενότητα 2 παρ. 1 προτ. 2 αρ. 1 OEG) ή σε στρατιωτική σύγκρουση στο κράτος καταγωγής του και υπέστη βλάβη στο πλαίσιο αυτό (ενότητα 2 παρ. 1 προτ. 1 αρ. 2 OEG).

Αναφορικά με τον προσδιορισμό της αποζημίωσης του OEG, αυτή προσδιορίζεται σύμφωνα με πίνακες του Federal Pension Act (BVG) και περιλαμβάνει σε περίπτωση ενδοοικογενειακής βίας, όχι μόνο την αποκατάσταση σωματικής βλάβης αλλά και την ηθική

[30] BMAS (2021), https://www.bmas.de/DE/Soziales/Soziale-Entschaedigung/Opferentschaedigungsrecht/anspruch-auf-entschaedigung-bei-gewalttaten.html.

[31] BSG, Judgment of November 30, 2006 – Ref.: B 9a VG 4/05 R, https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BSG&Datum=30.11.2006&Aktenzeichen=B%209a%20VG%204/05%20R.

ικανοποίηση του θύματος. Πιο συγκεκριμένα, η αποζημίωση αυτή δύναται να καλύψει ιατρική, νοσηλευτικές υπηρεσίες, βοηθήματα και παροχές υγείας (π.χ. οδοντοστοιχίες, αναπηρικό καροτσάκι), παροχές κηδείας και θανάτου και πρόσθετα επιδόματα πρόνοιας σε περίπτωση οικονομικής ανάγκης. Κατ' αρχήν, ο ζημιωθείς δεν θα αποζημιωθεί για περιουσιακές και οικονομικές ζημίες. Εξαιρέσεις ισχύουν για βοηθήματα που φέρει στο σώμα του, όπως γυαλιά, φακοί επαφής ή οδοντοστοιχίες.

Η αποζημίωση για πόνο και ταλαιπωρία (ενότητα 253 του Γερμανικού Αστικού Κώδικα – BGB) δεν καταβάλλεται από το κράτος. Οι περιουσιακές και οικονομικές ζημιές γενικά δεν αποζημιώνονται από το κράτος. Η μόνη εξαίρεση είναι τα βοηθήματα που φοριούνται στο σώμα, όπως γυαλιά, φακοί επαφής ή οδοντοστοιχίες (ενότητα 1 παρ. 7 OEG).

Οι παροχές αποζημίωσης για τους τραυματίες και τους επιζώντες καταβάλλονται ως μηνιαίες συνταξιοδοτικές παροχές για την αντιστάθμιση των υγειονομικών και οικονομικών συνεπειών του τραυματισμού. Το ποσό εξαρτάται από την έκταση της ζημιάς και τα πραγματικά οικονομικά μειονεκτήματα. Εάν, ωστόσο, η πράξη βίας διαπράχθηκε στο εξωτερικό, εκτός από την αξίωση για επιστροφή των εξόδων ως μέρος της ιατρικής περίθαλψης και αποκατάστασης, υπάρχει μόνο αξίωση για εφάπαξ πληρωμή (ενότητα 3α παρ. 2 OEG).

Σχετικά με τη διαδικασία, ο δικαιούχος μπορεί να υποβάλει αίτηση στην κρατική συνταξιοδοτική αρχή, η οποία είναι αρμόδια για αυτή, ανάλογα με τον τόπο κατοικίας του θύματος. Προκειμένου να δικαιούται αποζημίωση, το θιγόμενο πρόσωπο πρέπει να συνεργαστεί με κάθε μέσο που διαθέτει, ώστε να βοηθήσει στην διαλεύκανση του εγκλήματος. Συνίσταται, επομένως, η υποβολή καταγγελίας στις αστυνομικές αρχές ή στον εισαγγελέα το συντομότερο δυνατό. Δεν υπάρχει προθεσμία υποβολής αιτήσεων, αλλά τα οφέλη γενικά παρέχονται μόνο από τη στιγμή που υποβάλλεται η αίτηση. Αξίζει, επίσης, να σημειωθεί ότι αν ο ζημιωθείς κριθεί ότι δεν έκανε ό,τι ήταν δυνατό για να βοηθήσει στη διαλεύκανση του εγκλήματος και στη δίωξη του δράστη, ιδιαίτερα δεν το ανέφερε αμέσως στην αστυνομία, σύμφωνα με την ενότητα 2 παρ. 2 OEG, μπορεί να αποκλειστεί από το δικαίωμά του προς αποζημίωση.

4.3 Παροχή Νομικής Βοήθειας

Η νομική βοήθεια είναι ένα σύστημα που παρέχει νομική υποστήριξη και συμβουλές σε άτομα που δεν έχουν τη δυνατότητα να πληρώσουν για νομικές υπηρεσίες, λόγω

οικονομικών περιορισμών. Ο σκοπός της νομικής βοήθειας είναι να διασφαλίσει ότι οι άνθρωποι έχουν πρόσβαση στη δικαιοσύνη και μπορούν να υπερασπιστούν τα νόμιμα δικαιώματά τους, ανεξαρτήτως της οικονομικής τους κατάστασης.

4.3.1 Στην Ελλάδα

Στην Ελλάδα για πρώτη φορά επιχειρήθηκε η παροχή νομικής βοήθειας στα θύματα εκμετάλλευσης ως μέσο προστασίας και αρωγής με το άρθρο 12 παρ. 1 εδ. β' του Ν. 3064/2002, δυνάμει του π.δ. 233/2003. Σημαντικές είναι οι τροποποιήσεις που εισήγαγε ο Νόμος 3226/2004, ο οποίος αναδιαμόρφωσε τον θεσμό της νομικής βοήθειας στο πλαίσιο της ποινικής δίκης και καθόρισε συγκεκριμένες διατάξεις σχετικά με αυτήν. Σύμφωνα με αυτόν, το σύνολο των θυμάτων εγκλημάτων κατά της προσωπικής και γενετήσιας ελευθερίας περιλαμβάνονται στην κατηγορία των ατόμων που δικαιούνται δωρεάν νομική βοήθεια, υπό τον όρο ότι πληρούν τις προβλεπόμενες προϋποθέσεις. Αυτές οι προϋποθέσεις βασίζονται κυρίως στον υπολογισμό της οικονομικής κατάστασης του αιτούντος[32]. Πέραν του χαμηλού εισοδηματος, το οποίο δεν θα πρέπει να υπερβαίνει τα δύο τρίτα των κατώτατων ετήσιων ατομικών αποδοχών που προβλέπει η Εθνική Γενική Συλλογική Σύμβαση Εργασίας, βασική προϋπόθεση για την αξίωση της παροχής νομικής βοήθειας αποτελεί η ιδιότητα του πολίτη ή η κατοικία ή συνήθης διαμονή κράτους-μέλους της Ευρωπαϊκής Ένωσης.

Αργότερα, με την τροποποίηση της ως άνω διάταξης με το άρθρο 6 παρ. 1 Ν. 3625/2007, σχετικά με τα ανήλικα θύματα, στη συνέχεια με το άρθρο 7 του Ν. 3875/2010, το οποίο αφορά τους ενήλικες και μετέπειτα με το άρθρο 17 παρ. 2 του Ν. 4267/2014, με το οποίο ενσωματώθηκε το άρθρο 20 Οδηγία 2011/93/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαίσιο 2004/ 68/ ΔΕΥ του Συμβουλίου, δικαιούχοι νομικής βοήθειας είναι τα θύματα των πράξεων που προβλέπονται των άρθρων 323, 323Α, 323Β εδ. α', 324, 336, 338, 339, 342, 343, 345, 346, 347, 348, 348Α, 348Β, 348Γ, 349, 351, 351Α του Ποινικού Κώδικα ως προς τις τυχόν ποινικές και αστικές αξιώσεις τους. Με την προσθήκη παρ. 5 του άρθρου 3 του Ν. 3625/2007, ο εισαγγελέας, ο ανακριτής με διάταξη, το συμβούλιο ή το δικαστήριο με απόφασή του μπορούν, κατά περίπτωση, να διορίσουν συνήγορο αυτεπαγγέλτως από τον ειδικό πίνακα του άρθρου 3 παρ. 1 του Ν. 3226/2004.

[32] Χατζηνικολάου Ν. (2009), σελ 226.

Επιπρόσθετο κριτήριο για την παροχή νομικής βοήθειας αποτελεί η διάκριση της αξιόποινης πράξης η οποία απδίδεται στον αιτούντα σε σχέση με την απειλούμενη γι' αυτήν ποινή κατά το στάδιο της ανάκρισης ή της συζήτησης στο ακροατήριο στην περίπτωση κακουργήματος[33]. Στην περίπτωση μακρόχρονης ποινικής διαδικασίας προβλέπεται επιπλέον αμοιβή συνηγόρου, ενθαρρύνοντας την αποτελεσματική υποστήριξη του δικαιώματος του κατηγορούμενου. Όσον αφορά τα πλημμελήματα, προϋποτίθεται ότι θα πρέπει να αποτελούν αρμοδιότητα τριμελούς πλημμελειοδικείου, απειλούμενα με ποινή τουλάχιστον έξι μηνών. Στο δεύτερο βαθμό δικαιοδοσίας πρέπει να αφορά σε έφεση στο τριμελές εφετείο κακουργημάτων, στο μικτό ορκωτό ή στο τριμελές πλημμελειοδικείο, με την επιπρόσθετη προϋπόθεση ότι η επιβληθείσα ποινή από την πρωτοβάθμια καταδικαστική απόφαση ήταν τουλάχιστον έξι μήνες. Τέλος, παρέχεται νομική βοήθεια σε ποινικές υποθέσεις για αναίρεση, υπό τον όρο ότι έχει επιβληθεί ποινή τουλάχιστον ενός έτους.

Όσον αφορά τη διαδικασία χορήγησης νομικής βοήθειας, αυτή παρέχεται μετά από αίτηση του δικαιούχου, η οποία περιλαμβάνει σύντομη περιγραφή του αντικειμένου της δίκης ή της πράξης και τα στοιχεία που επαληθεύουν την πλήρωση των προϋποθέσεων για τη χορήγηση της βοήθειας, ήτοι τα απαραίτητα δικαιολογητικά που επιβεβαιώνουν την οικονομική κατάσταση του αιτούντος καθώς και την κατοικία ή διαμονή, εάν πρόκειται για πολίτη τρίτου κράτους, του αιτούντος. Για την υποβολή των δικαιολογητικών τίθεται προθεσμία δεκαπέντε ημερών πριν από τη δίκη ή την πράξη για την οποία απαιτείται η νομική βοήθεια, εκτός αν υπάρχει μετέπειτα κλήτευση. Η διαδικασία αυτή διεξάγεται χωρίς την υποχρεωτική παρουσία δικηγόρου. Για την έγκριση του αιτήματος αρκεί μια πιθανολογούμενη αίτηση, ενώ η αποδοχή ή η απόρριψη της πρέπει να είναι πάντα τεκμηριωμένη. Επιπλέον, επιτρέπεται η υποβολή πρόσθετου αιτήματος σε κάθε περίπτωση, ενώ νέα αίτηση μπορεί να υποβληθεί σε περίπτωση μεταβολής των πραγματικά περιστατικά, σύμφωνα με το άρθρο 2.

Επιπροσθέτως, σύμφωνα με το άρθρο 4 περί παύσης, ανάκλησης και περιορισμού της νομικής βοήθειας ορίζεται ότι η νομική βοήθεια παύει με το θάνατο του δικαιούχου, ωστόσο πράξεις που δεν επιδέχονται αναβολή μπορούν να ενεργηθούν και αργότερα με βάση τη βοήθεια που δόθηκε. Η νομική βοήθεια μπορεί, επίσης, να ανακληθεί ή να περιορισθεί με απόφαση του αρμόδιου δικαστή, αυτεπαγγέλτως ή ύστερα από πρόταση του εισαγγελέα, εφόσον αποδεικνύεται ότι οι προϋποθέσεις της παροχής είτε δεν υπήρχαν εξ αρχής, είτε

[33] Συμεωνίδης Δ. (2004), σελ. 1485 επ..

μεταβλήθηκαν ουσιωδώς. Επιπλέον, υπάρχει η δυνατότητα επιβολής χρηματικής ποινής στον αιτούντα που κατάφερε να λάβει νομική βοήθεια με ψευδή αίτηση.

Κατά το άρθρο 6 παρ.1, αρμόδιος να αποφανθεί επί του αιτήματος παροχής νομικής βοήθειας σε ποινικές υποθέσεις είναι ο πρόεδρος του δικαστηρίου στο οποίο εκκρεμεί η προς εκδίκαση του διακαιούχου ή ενώπιον της οποίας πρέπει να ασκηθεί το σχετικό ένδικο μέσο ή βοήθημα. Σύμφωνα με την παρ. 2 του άρθρου αυτού, στις περιπτώσεις των άρθρων 100 παρ. 3, 200 παρ. 1 εδ. β', 340, 376, 423 παρ. 1 Κ.Π.Δ. εισάγεται εξαίρεση και προβλέπεται ότι ο διορισμός του συνηγόρου γίνεται όπως ορίζεται με τις διατάξεις των άρθρων αυτών.

Παρά τις αναμφίβολα καινοτόμες νομοθετικές εξελίξεις σε σχέση με την παροχή νομικής βοήθειας στους οικονομικά αδύναμους, έχουν προκήψει πλείστα ζητήματα συνταγματικότητας και ορθότητας στην εν τοις πράγμασι εφαρμογής της. Αρχικά, ιδιαίτερα αρνητικές παρατηρήσεις σχετικά με τον συγκεκριμένο θεσμό, όσον αφορά τη συμμόρφωσή του προς το ενωσιακό πρότυπο, περιλαμβάνουν την πλήρη έλλειψη κατοχύρωσης των δικαιωμάτων του υπόπτου σύμφωνα με τα άρθρα της Οδηγίας 2016/1919/ΕΕ για την παροχή νομικής βοήθειας., ο προσδιορισμός αρκετά χαμηλού ανώτατου οικογενειακού εισοδήματος του δικαιούμενου προσώπου, το οποίο δεν ανταποκρίνεται πάντοτε στην πραγματικότητα, και η εξ αρχής γενική απαγόρευση δυνατότητας παροχής νομικής αρωγής για κακουργήματα κατά το στάδιο της προανάκρισης ή προκαταρκτικής εξέτασης.

Επιπροσθέτως, το πεδίο εφαρμογής στις ποινικές υποθέσεις κρίνεται περιορισμένο, αφού δεν προβλέπεται νομική βοήθεια στο στάδιο της προκαταρκτικής εξέτασης και της προδικασίας στα πλημμελήματα ή σε περίπτωση άσκησης ενδίκου μέσου από τον Εισαγγελέα κατά αθωωτικής απόφασης. Στο ζήτημα αυτό, εν μέρει λύση έδωσε ο Άρειος Πάγος με την απόφαση ΑΠ 944/2005, όπου απεφάνθει πως δεν αποκλείεται η επέκταση του θεσμού της νομικής βοήθειας και σε περιπτώσεις μη προβλεπόμενης ρητώς στον νόμο[34].

Τέλος, η πρόβλεψη περί παροχής νομικής βοήθειας μόνο σε πολίτες και κατοίκους κράτους-μέλους της Ε.Ε ορθά έχει κριθέι ότι ποτελεί αδικαιολόγητο περιορισμό[35] του δικαιώματος υπό το φως της αρχής της δίκαιης δίκης και της διεθνούς και ευρωενωσιακής της κατοχύρωσης, σύμφωνα με το άρθρο 6 ΕΣΔΑ. Άλλωστε η Ελλάδα έχει ήδη δύο

[34] Τριανταφύλλου Α. (2017).
[35] Συμεωνίδης Δ. (2004), σελ. 1490.

καταδικαστικές αποφάσεις από το ΕΔΔΑ εξαιτίας της άρνησης παροχής νομικής βοήθειας σε αλλοδαπούς κατηγορουμένους[36].

4.3.2 Στη Γερμανία

Στη Γερμανία, κατ' αρχήν, δεν παρέχεται νομική βοήθεια στην ποινική δίκη. Αναφορικά με τον παθών, ο ίδιος έχει δικαίωμα για παροχή νομικής βοήθειας σύμφωνα με το στο άρθρο 397a StPO (Κώδικας Ποινικής Δικονομίας - Strafprozessordnung), το οποίο τυγχάνει επίσης εφαρμογής σε θέματα αστικού, διοικητικού, συνταγματικού και κοινωνικού δικαίου. Οι νομική βοήθεια περιλαμβάνει, εκτός από συμβουλές, εκπροσώπηση, υποβολή υπομνημάτων και πλήρη δικαστική ή εξωδικαστική επίλυση διαφορών[37].

Οι προϋποθέσεις χορήγησής της σχετίζονται, αρχικά, με την οικονομική δύναμη του θύματος, η οποία κρίνεται σύμφωνα με το εισόδημά του, και κυρίως με το είδος του ποινικού αδικήματος και των συνεπειών που έχει υποστεί. Πιθανολόγηση τέλεσης εγκλήματος που προβλέπεται στην εν λόγω διάταξη αρκεί για την συνδρομή νομικής βοήθειας. Πιο συγκεκριμένα, δικαίωμα υποβολής αίτησης, σύμφωνα με το άρθρο 397a StPO έχει ο παθών των εγκλημάτων των άρθρων 177, 232, 232a, 232b και 233a, *"εφόσον τραυματίστηκε από ποινικό αδίκημα σύμφωνα με το άρθρο 184i StGB και η διάπραξη αυτού του αδικήματος βασίζεται σε έγκλημα σύμφωνα με το άρθρο 177 StGB,"* ή *".....από απόπειρα παράνομης ενέργειας σύμφωνα με τα άρθρα 211 και 212 StGB ή είναι συγγενής κάποιου που σκοτώθηκε από παράνομη πράξη κατά την έννοια του άρθρου 395 παράγραφος 2 αριθμός 1,"* ή *".....έχει τραυματιστεί από έγκλημα σύμφωνα με τα άρθρα 226, 226a, 234 έως 235, 238 έως 239b, 249, 250, 252, 255 και 316a StGB, το οποίο οδήγησε ή είναι πιθανό να προκαλέσει σοβαρή σωματική ή ψυχική κακό του,"* ή *"....έχει τραυματιστεί από παράνομη πράξη σύμφωνα με τα άρθρα 174 έως 182, 184i έως 184k και 225 του StGB και κατά τη στιγμή της πράξης δεν είχε συμπληρώσει ακόμη την ηλικία των 18 ετών ή δεν ήταν σε θέση να προστατεύσει επαρκώς τους δικούς του συμφέροντα ή", "....με παράνομη πράξη σύμφωνα με τα άρθρα 221, 226, 226α, 232 έως 235, 237, 238 παράγραφοι 2 και 3, άρθρα 239a, 239b, 240 παράγραφος 4, άρθρα 249, 250, 252, 255 και 316a παραβίασε και δεν έχει συμπληρώσει ακόμη το 18ο έτος της ηλικίας του κατά την υποβολή της αίτησης ή αδυνατεί να προστατεύσει επαρκώς τα δικά του συμφέροντα"*.

[36] Χειδάρης Β. (2016), https://lawtakpap.blogspot.com/2016/04/h.html.
[37] Hase D. (2012), https://www.akademie.de/de/wissen/beratungshilfeschein-kostenlose-rechtshilfe.

Συνεπεία των ανωτέρω, ανακύπτει η προβληματική σχετικά με την νομική εκπροσώπηση του κατηγορουμένου, στην περίπτωση που ο ίδιος δεν έχει τη δυνατότητα να αναλάβει τα δικαστικά έξοδα, όπως το δικαίωμα σε δίκαιη δίκη του άρθρου 6 ΕΣΔΑ ορίζει. Τη λύση σε αυτό το ζήτημα δίνει, εν μέρει, η διαδικασία του άρθρου 114 ZPO, η οποία στην περίπτωση αυτή τυγχάνει εφαρμογής και στην περίπτωση του κατηγορουμένου, μόνο όμως σε σχέση με τις αστικές αξιώσεις και διαδικασίες της υπόθεσης και εφόσον προβλέπονται εύλογες πιθανότητες επιτυχίας, ήτοι αθώωσής του.

Επίσης, εάν η φύση και η σοβαρότητα του αδικήματος το επιτρέπει, δύναται να ορισθεί από το Δικαστήριο δημόσιος συνήγορος σύμφωνα με το άρθρο 140 StPO, ανεξάρτητα, γεγονός που δεν σχετίζεται, ωστόσο, με την οικονομική κατάσταση του κατηγορουμένου, αλλά με τη φύση και σοβαρότητα του εγκλήματος. Η συμβουλευτική βοήθεια καλύπτει νομικές συμβουλές που λαμβάνουν χώρα εκτός της ποινικής διαδικασίας.

Ο κατηγορούμενος μπορεί, ακόμα, να υποβάλει αίτηση για το λεγόμενο πιστοποιητικό συμβουλευτικής βοήθειας (άρθρο 1 Beratungshilfegesetz - BerHG), όπως και ο παθών άλλωστε, στο τοπικό δικαστήριο του τόπου κατοικίας του ή δύναται να επικοινωνήσει απευθείας με δικηγόρο της επιλογής του με αίτημα τη συμβουλευτική βοήθεια. Στη συνέχεια, ο δικηγόρος χρησιμοποιεί το πιστοποιητικό για να χρεώσει τις αμοιβές για νομικές συμβουλές και άλλες δραστηριότητες απευθείας στο δικαστήριο. Πρέπει να καταβληθεί αμοιβή δέκα ευρώ, από την οποία ο δικηγόρος μπορεί να παραιτηθεί.

Προϋπόθεση χορήγησης του πιστοποιητικού συμβουλευτικής βοήθειας αποτελεί το εισόδημα του ενδιαφερομένου, το οποίο δεν θα πρέπει να υπερβαίνει ορισμένα ατομικά εισοδηματικά όρια, στα οποία προσμετράται το σύνολο των περιουσιακών του στοιχείων, και αφού αφαιρεθούν έξοδα ενοικίου, διατροφής και εισφορές υγείας. Όποιος δικαιούται ταμείο ανεργίας, παροχές κοινωνικής πρόνοιας ή άλλες κρατικές παροχές, λόγω χαμηλού εισοδήματος, τεκμαίρεται, κατ' αρχήν, ότι πληροί τις προϋποθέσεις για τη λήψη συμβουλευτικής βοήθειας. Εάν η αίτηση πιστοποιητικού συμβουλευτικής απορριφθεί, θα πρέπει ο ενδιαφερόμενος να ασκήσει ένσταση κατά της απορριπτικής απόφασης χορήγησης συμβουλευτικής βοήθειας στο αρμόδιο τοπικό δικαστήριο. Στη συνέχεια, η απόφαση υπόκειται σε νομικό έλεγχο από το δικαστήριο.

Ωστόσο, το πιστοποιητικό αυτό καλύπτει μόνο τις γενικές πληροφορίες που παρέχονται από τον δικηγόρο, καθώς ο ίδιος δεν έχει δικαίωμα πρόσβασης και γνώσης της

δικογραφίας που έχει δημιουργηθεί. Άλλα μέσα άμυνας, όπως επιθεώρηση φακέλων, υπομνήματα, αιτήσεις διακοπής δεν καλύπτονται από αυτή[38].

Θα πρέπει να τονιστεί ότι το πιστοποιητικό συμβουλευτικής βοήθειας δεν είναι το ίδιο με νομική βοήθεια των άρθρων 114 επ. ZPO (Κώδικας Πολιτικής Δικονομίας - Zivilprozessordnung) και δεν θα πρέπει να συγχέεται με αυτή, η οποία αφορά την πολιτική και διοικητική δίκη και μπορεί να χρησιμοποιηθεί για την κάλυψη του συνόλου ή μέρους των εξόδων για το δικαστήριο και τον δικηγόρο του δικαιούχου. Ωστόσο, οι προϋποθέσεις χορήγησης του πιστοποιητικού σχετικά με τα περιουσιακά στοιχεία και το εισόδημα είναι οι ίδιες με αυτές της νομικής βοήθειας και οι διατάξεις του άρθρου 114 επ. του ZPO ισχύουν εξίσου για τη συμβουλευτική βοήθεια.

Εν κατακλείδι, ο κατηγορούμενος δεν προστατεύεται επαρκώς σε σχέση με την οικονομική του ενίσχυση και κατ' επέκταση περιορίζεται υπέρμετρα το δικαίωμά του για συμμετοχή στις δικονομικές διαδικασίες, σαν να προδικάζεται και να τιμωρείται μερικώς εκ των προτέρων για την πράξη για την οποία κατηγορείται, πριν καν ακόμα εκκινήσει η αποδεικτική διαδικασία και αποφανθεί το ιδιο το Δικαστήριο επ' αυτού.

4.4 Εξέταση μαρτύρων - θυμάτων

4.4.1 Στην Ελλάδα

Οι μάρτυρες αποτελούν ένα από τα πλέον σημαντικά μέσα απόδειξης, καθώς η ανεξιχνίαστη κατάθεσή τους, χωρίς προκαταλήψεις, προσωπικές απόψεις και πεποιθήσεις, αποτελεί το ουσιαστικότερο στοιχείο για τη διαμόρφωση της δικανικής κρίσης. Η νομοθετική επιλογή να αξιοποιηθούν οι πληροφορίες που προσφέρουν οι μάρτυρες, με σκοπό την άμεση υποστήριξη της απόδειξης για τη θεμελίωση της δικανικής κρίσης, επισημαίνει τον κρίσιμο ρόλο της μαρτυρικής κατάθεσης στο δικαιοδοτικό σύστημα[39]. Η θεώρηση της μαρτυρίας ως ενός εκ των θεμελίων τής αποδεικτικής διαδικασίας ενισχύεται από τη θέση που της αποδίδει ο ίδιος ο ποινικός νομοθέτης. Λαμβάνοντας υπόψη τη σημασία που αποδίδεται στον ρόλο του μάρτυρα και τον χαρακτήρα του ως ενεργού υποκειμένου στη δίκη, η αναζήτηση της ουσιαστικής αλήθειας στην ποινική διαδικασία απαιτεί την εξασφάλιση της ανεξαρτησίας της μαρτυρικής κατάθεσης από εξωτερικές επιρροές, με κύριο εκείνον του κατηγορούμενου.

[38] ο.π.: Hase D. (2012).
[39] Δαλακούρας Θ. (2003), σελ. 68.

4.4.1.1 Δικονομικές αρχές τής απόδειξης

Το δικαίωμα απόδειξης αντλεί την έννοιά του από τις συνταγματικές αρχές τού δικαιώματος ακρόασης στο δικαστήριο και της αξίας τού ανθρώπου. Εξασφαλίζοντας όχι μόνο τη διακανονιστική εξακρίβωση της υπόθεσης, αλλά και την προάσπιση του ανθρώπου σε μια δύσκολη στιγμή της δίκης, το δικαίωμα απόδειξης υποστηρίζεται από αρχές συνταγματικής εγγύησης. Στο πλαίσιο αυτό, οι αρχές της προφορικότητας και της αμεσότητας διαδραματίζουν καίριο ρόλο στην ποινική δίκη, αποτελώντας τους στυλοβάτες για την εύρεση της ουσιαστικής αλήθειας[40]. Η αμεσότητα απαιτεί την άμεση αντίληψη του δικαστή για τα αποδεικτικά στοιχεία, ενώ η προφορικότητα, η οποία πηγάζει από την αρχή τής δημοσιότητας, εξασφαλίζει τη ζωντανή επικοινωνία και την άμεση αντίληψη των παραγόντων της δίκης. Οι τρεις αυτές αρχές εγγυώνται την αξιοπιστία τής δικαστικής διαδικασίας.

Στο πλαίσιο της μαρτυρικής απόδειξης, όπου οι μάρτυρες συνθέτουν το ζωντανό αποδεικτικό υλικό, αυτές οι αρχές αποκτούν ιδιαίτερη σημασία. Η επίδραση της προδικασίας παραμένει περιορισμένη, καθώς η άμεση αντίληψη των δικαστών σε όλα τα στάδια της δίκης εξασφαλίζει την επίκαιρη και αξιόπιστη αξιολόγηση του αποδεικτικού υλικού. Παρόλο, όμως, που η μαρτυρική απόδειξη μπορεί να οδηγήσει στην άμεση ανακάλυψη της αλήθειας, εισάγει, παράλληλα, τον κίνδυνο αναληθών μαρτυριών που μπορούν να προκαλέσουν δικαστική πλάνη. Εύλογα, οι συνθήκες κατά τις οποίες συλλέγεται το υλικό κατά την προδικασία μπορούν να δημιουργήσουν αμφιβολίες σχετικά με την ακρίβεια και την αξιοπιστία του, ειδικά όταν εμπλέκονται παράγοντες όπως η βιασύνη, η προκατάληψη και, συχνά, ο δόλος του εν λόγω συλλέγοντος κατά τη διεξαγωγή προανάκρισης. Από αυτήν την άποψη, είναι απαραίτητο να εμπιστεύεται ο δικαστής μόνο στην άμεση προσωπική του αντίληψη.

Γι’ αυτόν τον λόγο, ο νομοθέτης επισημαίνει μια συστηματική και λογικά δεσμευμένη διαδικασία εξέτασης των μαρτύρων στην Ποινική Δικονομία. Αυτή η διαδικασία είναι σχεδιασμένη με σκοπό να ενισχύσει και να διασφαλίσει τη συμμόρφωση προς τις αρχές της αμεσότητας και της προφορικότητας. Μέσα από αυτήν τη συνεκτική προσέγγιση, ο νομοθέτης προσπαθεί να αντιμετωπίσει τον κίνδυνο αναληθών μαρτυριών, ενισχύοντας παράλληλα τη διαδικασία ανακάλυψης της αλήθειας στο πλαίσιο της δικαιοσύνης.

[40] Κωνσταντινίδης Α. (2012), σελ.37.

Η συνδυασμένη εφαρμογή των αρχών της αμεσότητας και της προφορικότητας αποτελεί θεμέλιο για την διεξαγωγή αποτελεσματικής ποινικής δίκης, δίνοντας έμφαση στη ζωντανή επικοινωνία των παραγόντων της δίκης με τα αποδεικτικά στοιχεία. Η αρχή της προφορικότητας επιτρέπει την άμεση αντίληψη του δικαστή για τα γεγονότα, καθώς ο ίδιος έρχεται σε επαφή με τους μάρτυρες, τους κατηγορούμενους και τα αποδεικτικά στοιχεία. Η αμεσότητα εξασφαλίζεται με τον άμεσο διάλογο του δικαστή με τα ενεχόμενα μέρη, ενώ η προφορικότητα ενισχύεται με τη ζωντανή παρουσία και επικοινωνία τους. Ο δικαστής οφείλει να θεμελιώσει την κρίση του μόνο σε εκείνα τα αποδεικτικά στοιχεία που έχει καταλάβει απευθείας μέσω της αντίληψής του. Η αρχή αυτή εξασφαλίζει ότι ο δικαστής είναι άμεσα ενημερωμένος για τα γεγονότα και τις καταθέσεις των μαρτύρων, ενισχύοντας την επικοινωνία των παραγόντων της δίκης με την αλήθεια. Άλλωστε, η απόλυτη ισχύς του δικαιώματος απόδειξης στην ποινική δίκη, που απορρέει από το απόλυτο δικαίωμα ακρόασης, έχει ως αποτέλεσμα την εφαρμογή της αρχής της αμεσότητας, ακόμη και χωρίς ρητή πρόβλεψη στον Κώδικα Ποινικής Δικονομίας για την καθοδήγηση της ποινικής δίκης από την αρχή έως το τέλος της. Έτσι, το δικαστήριο εξετάζει ο ίδιος όλα τα αποδεικτικά μέσα προκειμένου να διαλευκάνει την κατηγορούμενη πράξη, προσδίδοντας ζωντάνια στην ποινική δίκη ως πεδίο διαλεκτικής αντιπαράθεσης.

Κατά πάγια, μάλιστα, νομολογία τού Αρείου Πάγου[41], η παραβίαση των αρχών της αμεσότητας, της προφορικότητας και της διεξαγωγής της δίκης με αντιδικία δικαιολογεί την εφαρμογή του άρθρου 510 παρ. 1 στοιχείο Γ’ του Κώδικα Ποινικής Δικονομίας, σε συνδυασμό με το άρθρο 329 του ιδίου νόμου. Κατά την ερμηνεία αυτή, η έννοια της δημοσιότητας καλύπτει τη δημόσια διεξαγωγή της δίκης μέσω προφορικού λόγου (αρχή της προφορικότητας), καθώς και τη διαδικασία εξέτασης μαρτύρων, ανάγνωσης εγγράφων και γενικότερα τη διεξαγωγή οποιουδήποτε γεγονότος που συντελεί στο σχηματισμό της δικαστικής απόφασης (αρχή της αμεσότητας).

Η προδικαστική φάση μπορεί να επηρεάσει ελαφρώς την ακροαματική διαδικασία, αλλά η άμεση επικοινωνία κατά τη διάρκεια της δίκης εξασφαλίζει ότι οι πληροφορίες παρέχονται στο δικαστή κατ' ευθείαν. Η αμεσότητα και η προφορικότητα επιτρέπουν στο δικαστήριο να διαμορφώσει μια πεποίθηση για την αλήθεια των γεγονότων, εξασφαλίζοντας την ουσιαστική και δίκαιη απόφαση. Συνολικά, ο συνδυασμός αυτών των αρχών αποτελεί το θεμέλιο για μια αποτελεσματική ποινική διαδικασία[42]. Η στενή σχέση ανάμεσα στις αρχές

[41] ΑΠ 43/2023, 681/2023, α’ δημοσ. ΤΝΠ NOMOS.
[42] Κωνσταντινίδης Α. (2012), σελ.47.

αυτές, λόγω της κοινής προέλευσής τους, δεν υποδηλώνει πλήρη ταύτιση, καθώς είναι δυνατή η διεξαγωγή μιας διαδικασίας πλήρως προφορικής χωρίς απαραίτητα να εφαρμόζεται η αρχή της αμεσότητας. Επιπλέον, η αρχή της προφορικότητας καλύπτει την ακροαματική διαδικασία από την έναρξη έως το τέλος, ενώ η αρχή της αμεσότητας αφορά αποκλειστικά την αποδεικτική διαδικασία.

4.4.1.2 Από τον Ν. 1916/1990 μέχρι σήμερα

Σχετικά με την προστασία των μαρτύρων, αυτή εισήχθη στο εγχώριο δίκαιο ως θεσμός με το άρθρο 9 του Ν. 1916/1990. Με το άρθρο αύτο ορίστηκε ως "ειδική και αναγκαία" η προστασία μόνο των δικαστικών λειτουργών, από το Υπουργείο Δημόσιας Τάξης, και των μαρτύρων, κατόπιν αιτήσεως τους, υποθέσεων οργανωμένου εγκλήματος και τρομοκρατίας[43]. Αργότερα, με τον Ν. 2172/1993, η προστασία των εμπλεκόμενων με τέτοιες υποθέσεις δικαστικών λειτουργών επεκτάθηκε και στα μέλη τής οικογένειάς τους. Με τον Ν. 2173/1999 διευρύνθηκε το πλαίσιο παροχής προστασίας μαρτύρων σε περισσότερες κατηγορίες υποθέσεων, μέσω, ωστόσο, αστυνομικών και όχι δικονομικών μέσων προστασίας[44]. Αρχικά, η παροχή προστασίας στους μάρτυρες επικεντρωνόταν στο να προφυλάσσει τον κάθε μάρτυρα από τυχόν επηρεασμό από τον κατηγορούμενο ή από άλλα άτομα του περιγύρου του, να του παρέχει προστασία από προσβολή της τιμής και της προσωπικότητάς τους, καθώς και να αντιμετωπίζει το ψυχολογικό βάρος που μπορεί να αντιμετωπίζουν ιδίως οι ανήλικοι ή ενήλικοι μάρτυρες που έχουν υποστεί κακοποίηση, εξαιτίας τής παρουσίας του κατηγορούμενου κατά τη διαδικασία ακρόασης[45].

Στο πλαίσιο της προστασίας μαρτύρων, ο νόμος εξειδικεύει κατηγορίες μαρτύρων που επωφελούνται αυτής, συμπεριλαμβάνοντας τους ουσιώδεις μάρτυρες με άμεση ή έμμεση γνώση των πραγματικών περιστατικών, καθώς και τα πρώην μέλη εγκληματικών οργανώσεων που είτε παραιτήθηκαν είτε συνεργάζονται εθελοντικά. Επίσης, προστατεύονται οι καλυμμένοι δρώντες αστυνομικοί, καθώς και τα ίδια τα θύματα της εγκληματικής οργάνωσης. Επιπλέον, εισαγγελείς, ανακριτές και δικαστές που αναλαμβάνουν υποθέσεις σχετιζόμενες με το οργανωμένο έγκλημα προστατεύονται με την απόκρυψη της ταυτότητάς τους σε περίπτωση μειοψηφίας κατά την προφορική απαγγελία της απόφασης στο ακροατήριο, καθώς και κατά την εκπόνηση της απόφασης. Η προστασία διαφοροποιείται ανάλογα με την αιτιολογική βάση, καλύπτοντας προληπτικά μέτρα για τους ουσιώδεις

[43] Τριανταφύλλου Α. (2014), σελ. 275.
[44] Δαλακούρας Θ. / Κωνσταντινίδης Α. (2014), σελ. 318.
[45] ο. π. Δαλακούρας Θ. / Κωνσταντινίδης Α. (2014), σελ. 319.

μάρτυρες, και επικεντρώνεται στην πρόληψη πράξεων εκφοβισμού και εκδίκησης. Η αντιμετώπιση των μαρτύρων διαμορφώνεται βάσει της παρουσίας συγκεκριμένων ενδείξεων εκφοβισμού, απαιτώντας συγκεκριμένες πράξεις για την ενεργοποίηση των μέτρων προστασίας. Η νομοθεσία σχετικά με την προστασία των μαρτύρων στην Ελλάδα εφαρμόζεται εναλλακτικά ή σωρευτικά, λαμβάνοντας υπόψη τον εκτιμώμενο κίνδυνο εκφοβισμού ή αντεκδίκησης. Το κύριο αίτημα είναι η αποτελεσματική συγκέντρωση αποδεικτικού υλικού κατά τη διάρκεια της προδικασίας, με τη λήψη μέτρων προστασίας που καθορίζονται από τον αρμόδιο εισαγγελέα[46].

Ο νόμος περί προστασίας μαρτύρων υποστέγασε αλλαγές με το άρθρο 42 του Ν. 3251/2004. Η τροποποίηση αυτή επέτρεψε τη χορήγηση προστασίας και σε περιπτώσεις τρομοκρατικών οργανώσεων και συμμοριών, συμμορφούμενη με την πολιτική δέσμευση της Ελλάδας προς την Ευρωπαϊκή Ένωση προς αποτροπή των επιπτώσεων της τρομοκρατικής απειλής στην οικονομική και κοινωνική ζωή και προς διατήρηση και ανάπτυξη των αρχών της ελευθερίας, της ασφάλειας και της δικαιοσύνης. Επιπλέον, με τον Ν. 3691/2008 θεσμοθετήθηκε η προστασία υπαλλήλων που καταγγέλλουν νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες και χρηματοδότηση της τρομοκρατίας. Η εφαρμογή των μέτρων προστασίας, συμπεριλαμβανομένης της αποστολής μαρτύρων σε άλλες χώρες, ρυθμίζεται από τον Ν. 4411/2016, εξαλείφοντας τα προϋπάρχοντα νομοθετικά κενά.

Το άρθρο 9 του Ν. 2928/2001, που αφορά την προστασία μαρτύρων, εισήχθη στον Κώδικα Ποινικής Δικονομίας στο δεύτερο βιβλίο αυτό των "αποδείξεων" με τη διάταξη του άρθρου 218. Η αλλαγή αυτή αντιπροσωπεύει μια συνειδητή και ολοκληρωμένη μεταφορά των διατάξεων του άρθρου 9 στο νέο άρθρο 218 ΚΠΔ, επεκτείνοντας παράλληλα την προστασία των μαρτύρων σε ευρύτερο φάσμα ποινικών αδικημάτων[47]. Το νέο άρθρο 218 επιτρέπει την προστασία μαρτύρων όχι μόνο για εγκληματικές οργανώσεις αλλά και για θύματα, οικείους, και ουσιώδεις μάρτυρες εγκλημάτων εμπορίας ανθρώπων και παράνομης διακίνησης μεταναστών. Επιπλέον, προσθέτει στον κατάλογο ποινικών αδικημάτων τη διαφθορά, ενισχύοντας το ποινικό οπλοστάσιο για αποτελεσματική αντιμετώπιση του φαινομένου, με στόχο τη διατήρηση της λειτουργίας των δημόσιων θεσμών.

Η παρεχόμενη από το άρθρο 218 ΚΠΔ προστασία επεκτείνεται και σε ιδιώτες που συμμετέχουν στην Ειδική Ανακριτική Πράξη (ΕΑΠ) της συγκαλυμμένης έρευνας του άρθρου

[46] Τριανταφύλλου Α. (2014), σελ. 279-280.
[47] Δαλακούρας Θ. / Κωνσταντινίδης Α. (2014), σελ. 317.

255 παρ. 1 στοιχ. α' ΚΠΔ. Σύμφωνα με τις διατάξεις, η έρευνα αυτή διενεργείται υπό την εποπτεία του ανακριτικού, ενώ συμμετέχουν τόσο ανακριτικοί υπάλληλοι όσο και ιδιώτες υπό τις οδηγίες του ανακριτικού υπαλλήλου. Το άρθρο 218 ΚΠΔ προβλέπει επίσης ότι η πρωτοβουλία τέλεσης εγκλημάτων σε αυτό το πλαίσιο πρέπει να συντρέχει στο πρόσωπο του δράστη, ενώ προϋπόθεση είναι και η σύνταξη αναλυτικής έκθεσης σύμφωνα με τα οριζόμενα στο άρθρο 148 ΚΠΔ.

Ειδικές Ανακριτικές Πράξεις (ΕΑΠ), που προβλέπονται από ειδικούς ποινικούς νόμους, ενσωματώθηκαν στον ΚΠΔ μέσω του Ν. 2928/2001. Αυτές εφαρμόζονται σε περιορισμένα εγκλήματα, με αυξημένες εγγυήσεις και σεβασμό προς τις διεθνείς υποχρεώσεις, οι οποίες απορρέουν από το άρθρο 20 της Σύμβασης του ΟΗΕ κατά του Διεθνικού Οργανωμένου Εγκλήματος, η οποία ενσωματώθηκε στον ελληνικό δίκαιο με την κύρωση του Ν. 3875/2010. Η διαδικασία τους λαμβάνει χώρα με συγκαλυμμένο τρόπο για διασφάλιση της μυστικότητας, με απόκλιση από τις συνηθισμένες αρχές της ποινικής διαδικασίας. Επιπλέον, η λειτουργία τους έχει εγκληματοπροληπτικό χαρακτήρα, επιτρέποντας τη διεύρυνση του κύκλου των εμπλεκόμενων και προκαλώντας κάμψη στο τεκμήριο αθωότητας μέσω της ανάγκης εφαρμογής των αρχών του προσήκοντος βαθμού υπονοιών και της αναγκαιότητας[48]. Επίσης, υπόκεινται σε αυστηρές εγγυήσεις που ορίζονται από τις αρχές της νομιμότητας, της αναγκαιότητας και της αναλογικότητας, οι οποίες εξασφαλίζουν τη συνάφεια μεταξύ του σκοπού που εξυπηρετούν και του περιορισμού των ατομικών δικαιωμάτων, αποφεύγοντας την προσβολή της ουσίας των δικαιωμάτων αυτών. Ακόμα, η εκτέλεση των ΕΑΠ προϋποθέτει την έκδοση ειδικά αιτιολογημένου βουλεύματος, με σαφή και λεπτομερή αιτιολογία της διενέργειας ΕΑΠ, αποτελώντας ένα επιπλέον μέσο ελέγχου και διασφαλίζοντας ότι η συγκαλυμμένη έρευνα πραγματοποιείται με την απαιτούμενη νομιμότητα και δικαιοσύνη. Η προστασία των συγκαλυμμένα δρώντων ιδιωτών ως μαρτύρων αιτιολογείται από τον κίνδυνο αποκάλυψης της ταυτότητάς τους κατά την κατάθεση, αποφεύγοντας την αχρήστευσή τους στον αγώνα κατά του εγκλήματος

4.4.1.3 Προστασία ανηλίκων μαρτύρων

Εξαιτίας των ιδιαίτερων κοινωνικών και ψυχολογικών λόγων κατά την εμπλοκή ανηλίκων ως θύματα σε εγκλήματα που αφορούν κατά της προσωπικής και γενετήσιας ελευθερίας του, έχει θεσπιστεί στο άρθρο 227 ΚΠΔ (π226Α)[49] ειδική διάταξη σχετικά με τη

[48] Νάϊντος Χ. (2017), σελ 491.
[49] Μαργαρίτης Λ. (2020), σελ. 1225.

διαδικασία εξέτασής τους ως μάρτυρες, με σκοπό την αντικειμενική και ανεπηρέαστη συναισθηματικά, κατάθεσης κατά το στάδιο της προδικασίας. Σκοπός της διάταξης αυτής είναι η εξασφάλιση του συμφέροντος των ανηλίκων, η αποφυγή νέας θυματοποίησής τους, η ευάλωτη θέση τους και ταυτόχρονα ο ειδικός τρόπος, με τον οποίον πρέπει να αντιμετωπίζονται, προκειμένου να διασφαλισθεί η χωρίς την πρόκληση νέων ψυχικών τραυμάτων λήψη αξιόπιστων καταθέσεων[50]. Η διάταξη αυτή αφορά τα ανήλικα θύματα των αξιόποινων πράξεων των άρθρων 323Α παρ. 4, 324, 336, 338, 339, 342, 343, 345, 346, 347, 348, 348Α, 349, 351, και 351Α ΠΚ, και κατόπιν τροποποίησης των 323Β εδ.α', 337 παρ. 3 και 4 ΠΚ, καθώς και τα άρθρα 87 παρ. 5 και 6 και 88 του Ν.3386/2005. Ορίζεται λοιπόν ότι κατά την εξέταση του ανηλίκου θύματος διορίζεται και παρίσταται ως πραγματογνώμων, παιδοψυχολόγος ή παιδοψυχίατρος και ότι είναι δυνατή η παρουσία του νομίμου εκπροσώπου του, εκτός εάν αυτό απαγορευθεί για σπουδαίο λόγο.

Ο ρόλος του παιδοψυχολόγου ή του παιδοψυχίατρου αφορά την προετοιμασία του ανηλίκου για την κατάθεση του με τη δημιουργία σχέσης εμπιστοσύνης και ενός αισθήματος ασφάλειας έναντι της άγνωστης σε αυτό δικαστικής διαδικασίας, την ενημέρωση του παιδιού για τη σημασία της αλήθειας, τη συνεργασία με τους ανακριτικούς υπαλλήλους και το δικαστήριο και τη σύνταξη γραπτής έκθεσης περί της αντιληπτικής ικανότητας και της ψυχικής καταστάσης του ανηλίκου.

Ειδικά, για την εμφάνισή του στο ακροατήριο ορίζεται ότι αυτή δεν είναι δυνατή, εκτός εάν κατά το στάδιο αυτό έχει συμπληρώσει το δέκατο όγδοο έτος της ηλικίας του, οπότε υφίσταται η δυνατότητα αυτοπρόσωπης εμφάνισής του. Επίσης, ρητά ορίζεται ότι η γραπτή κατάθεση του ανηλίκου που είχε ληφθεί κατά το στάδιο της προδικασίας αναγιγνώσκεται πάντα στο ακροατήριο.

Κατ' αρχήν θεσπίζεται, επομένως, ο κανόνας της μη εμφάνισης του ανήλικου θύματος στο ακροατήριο, με εξαίρεση τη δυνατότητα του εισαγγελέα ή των διαδίκων να αιτηθούν, μετά την εισαγωγή της υπόθεσης στο ακροατήριο, την εξέτασή του, εάν δεν έχει εξετασθεί στην ανάκριση ή κρίνεται ότι πρέπει να εξετασθεί συμπληρωματικά. Σε περίπτωση αποδοχής του σχετικού αιτήματος, η εξέταση πραγματοποιείται από ανακριτικό υπάλληλο που διορίζεται από τον δικαστή που την διέταξε, ο οποίος οφείλει να του υποβάλλει συγκεκριμένες και εκ των προτέρων προσδιορισμένες ερωτήσεις, ενώ παράλληλα διορίζεται

[50] ΑΠ 931/2012, α' δημοσ. areiospagos.gr, https://www.areiospagos.gr/nomologia/apofaseis_DISPLAY.asp?cd=FKS3IS4EWVCQE9LSSJU8CLVTQ7X73S&apof=931_2012&info=%D0%CF%C9%CD%C9%CA%C5%D3%20-%20%20%D3%D4.

με την απόφαση ως πραγματογνώμων κάποιος παιδοψυχίατρος ή παιδοψυχολόγος. Ακολουθείται, δηλαδή, ο τρόπος εξέτασης που προσδιορίζεται για το στάδιο της προδικασίας, στον χώρο του ανηλίκου και χωρίς την παρουσία διαδίκων.

Στη θεωρία υποστηρίχθηκε ότι δεν προβλέπεται η κύρωση της σχετικής ακυρότητας για την περίπτωση της παραβίασης της υποχρέωσης ανάγνωσης της προδικαστικής μαρτυρικής κατάθεσης του ανήλικου μάρτυρα στο ακροατήριο (άρθρο 172 παρ. 1 ΚΠΔ σε συνδυασμό με το άρθρο 227 παρ. 5α ΚΠΔ). Για το λόγο αυτό, η παράλειψη ανάγνωσης στο ακροατήριο της έκθεσης εξέτασης του ανήλικου θύματος δεν επιφέρει ακυρότητα της διαδικασίας, υπό την προϋπόθεση ότι δεν θα ληφθεί υπόψη από το δικαστήριο στο σχηματισμό της δικανικής του πεποίθησης, χωρίς να αναγνωσθεί[51]. Αντιθέτως ο Άρειος Πάγος έκρινε ότι υφίσταται έλλειψη ειδικής και εμπεριστατωμένης αιτιολογίας, λόγω του υποχρεωτικού για το δικαστήριο χαρακτήρα της συνεκτίμησης της έγγραφης κατάθεσης (άρθρο 510 παρ. 1 στοιχ. Δ' ΚΠΔ)[52].

Σχετικά με αυτήν την ρύθμιση, η νομική πρακτική πολλές φορές έχει εκφράσει αντίθετη γνώμη, ισχυριζόμενη ότι αυτή οδηγεί σε έναν σημαντικό περιορισμό των δικαιωμάτων του κατηγορουμένου. Αρχικά, γίνεται η ανάγνωση της κατάθεσης, η οποία παρέχεται στην προδικασία χωρίς την παρουσία της υπεράσπισης και τη δυνατότητα υποβολής ερωτήσεων από αυτήν, και αυτό θεωρείται ο κανόνας. Επιπλέον, ακόμη και μετά την εισαγωγή της υπόθεσης στο ακροατήριο, επιτρέπεται - υπό συγκεκριμένες προϋποθέσεις και χωρίς την παρουσία των αναφερόμενων - η εξέταση των ανηλίκων θυμάτων μόνον κατά το προπαρασκευαστικό στάδιο της κύριας διαδικασίας. Αναμφισβήτητα, λοιπόν, παρατηρεί κανείς ότι αυτή η διάταξη είναι αντίθετη με την αρχή της προφορικότητας της διαδικασίας, την αρχή της αμεσότητας και την αρχή της διεξαγωγής της δίκης κατ' αντιδικία.

Γι' τον λόγο αυτό, με την τελευταία τροποποίηση του άρθρου αυτού με τον Ν. 4620/2019 επιχειρήθηκε εν μέρει η διασφάλιση των δικαιωμάτων του κατηγορουμένου. Πιο συγκεκριμένα, σύμφωνα με το άρθρο 227 παρ.2 εδ. α', προβλέπεται το δικαίωμα του κατηγορουμένου να διορίσει τεχνικό σύμβουλο, χωρίς να έρχεται όμως σε προσωπική επαφή με τον ανήλικο. Επιπλέον, σύμφωνα με το άρθρο 3 παράγραφος 3 του ίδιου άρθρου, ο εκάστοτε συνήγορος μπορεί επίσης να ζητήσει από τον ανακριτή να θέσει στον ανήλικο ερωτήσεις που έχουν προετοιμαστεί εκ των προτέρων εγγράφως. Οι ερωτήσεις αυτές τίθενται

[51] ΑΠ 279/2020, 1572/2017, 169/2015, α' δημοσ. ΤΝΠ NOMOS.
[52] ΑΠ 1332/2019, 985/2015, α' δημοσ. ΤΝΠ NOMOS.

κατά την κρίση του παιδοψυχολόγου ή του ψυχιάτρου και μπορούν να απαγορευτούν από αυτούς ακόμη και στο δικαστήριο χωρίς την παρουσία των διαδίκων, συμφωνα με την παράγραφο 6, αν ο παιδοψυχολόγος ή ο ψυχίατρος κρίνει ότι μπορεί να επηρεάσουν την ψυχική κατάσταση του ανηλίκου. Τέλος, οι καταθέσεις τού ανηλίκου καταγράφονται εγγράφως καθώς και σε ηλεκτρονικά οπτικοακουστικά μέσα.

Ωστόσο, παρά την προαναφερθείσα τροποποίηση, η εν λόγω ρύθμιση δεν φαίνεται να πληροί τα κριτήρια που έχουν διαμορφώσει η νομολογία των οργάνων της Ευρωπαϊκής Ένωσης και του Δικαστηρίου της Ευρωπαϊκής Ένωσης. Αυτό συμβαίνει διότι αποκλείει, κατά τη διάρκεια της εξέτασης από τον ανακριτικό υπάλληλο ή τον ανακριτή, την παρουσία του συνηγόρου υπεράσπισης. Όμως, λαμβάνοντας υπόψη την σταθερή νομολογία του Ευρωπαϊκού Δικαστηρίου για τα Δικαιώματα του Ανθρώπου, η διακυβερνητική αυτή ρύθμιση πρέπει να ερμηνεύεται με τρόπο που να αποκλείει την παρουσία του κατηγορουμένου στη διαδικασία εξέτασης του ανηλίκου θύματος. Αυτό δεν αποκλείει, ωστόσο, την παρουσία του συνηγόρου του κατηγορούμενου. Ο συνήγορος του κατηγορουμένου πρέπει να είναι παρών σε κάθε περίπτωση, ακόμη και αν δεν του επιτρέπεται να θέτει ερωτήσεις απευθείας στον μάρτυρα, αλλά μόνο να τις υποβάλλει γραπτώς στον ανακρίνοντα.

Από την άλλη πλευρά, υπάρχει και η άποψη ότι με την υποχρεωτική παρουσία ειδικών επιστημόνων και την προγραμματισμένη ηχογράφηση της μαρτυρικής κατάθεσης του ανηλίκου, έχει επιδιωχθεί να αντισταθμιστεί η απώλεια του δικαιώματος υπεράσπισης του κατηγορούμενου. Συγκεκριμένα, σύμφωνα με ορισμένες αποφάσεις[53], αναφέρεται ότι η παρουσία ενός παιδοψυχιάτρου διασφαλίζει το δικαίωμα υπεράσπισης του κατηγορούμενου και, ειδικότερα, τη δυνατότητα εξέτασης της αξιοπιστίας του ανηλίκου και την ανακάλυψη της πραγματικής αλήθειας, ακόμη και προς όφελος του, σύμφωνα με το άρθρο 239 παράγραφος 2 του Κώδικα Ποινικής Δικονομίας. Παρά ταύτα, αυτά τα δικονομικά μέτρα δεν είναι ισοδύναμα και σαφώς δεν αρκούν για να εξασφαλίσουν την επικύρωση της ποινικής δίκης στο σύνολό της ως δίκαιη, και την κατάθεση του ανήλικου μάρτυρα ως αξιόπιστη.

Σχετικά με την υφιστάμενη διαδικασία, υπάρχουν ανησυχίες σχετικά με τον σωστό τρόπο εφαρμογής της διάταξης όσον αφορά τα ανήλικα θύματα. Καταρχάς, το έλλειμμα ενός ειδικού πρωτοκόλλου εξέτασης ανηλίκων θυμάτων προκαλεί προβλήματα, ειδικά σε δικονομικό και ιατρικό επίπεδο. Ένα τέτοιο πρωτόκολλο θα ήταν απαραίτητο για την

[53] Απόφαση 113/2015 του Συμβουλίου της Επικρατείας Κρήτης.

διενέργεια της διαδικασίας και θα λειτουργούσε ως προστατευτικό μέτρο, τόσο για τα δικαιώματα του ανηλίκου μάρτυρα όσο και για του κατηγορούμενου, κατά τη διάρκεια ολόκληρης της διαδικασίας, πράγμα που σε πολλές χώρες έχει ήδη συνταχθεί ήδη εδώ και περισσότερες από 4 δεκαετίες, ενώ έχουν εκπαιδευτεί χιλιάδες επαγγελματίες στη χρήση ειδικών εργαλείων και έχουν υιοθετηθεί πρακτικές μείωσης των δεινών που συνεπάγεται η συμμετοχή του ανήλικου στις σχετικές διαδικασίες.

Στη συνέχεια, όπως ήδη αναφέρθηκε, είναι ευρέως γνωστό ότι δεν υπάρχει εξειδικευμένο επιστημονικό προσωπικό για τη συγκεκριμένη διαδικασία. Ωστόσο, αυτή η έλλειψη είναι ακόμη πιο αισθητή εξαιτίας της ιδιαίτερα απαιτητικής φύσης του έργου που αναλαμβάνουν οι επαγγελματίες που έρχονται σε επαφή με τα ανήλικα θύματα - μάρτυρες. Πολλοί ερευνητές επισημαίνουν τις αρνητικές επιπτώσεις που μπορεί να έχει η χρήση ανεπαρκών μεθόδων και ιδίως η συνεχής επανάληψη συνεντεύξεων σε διάφορες χρονικές στιγμές από διάφορα άτομα χωρίς ειδική εκπαίδευση[54]. Η ακατάλληλη χρήση τεχνικών μπορεί να οδηγήσει στην απομόνωση ψευδών διακηρύξεων, στην αλλοίωση της μνήμης, στη δημιουργία υπερβολικής αγωνίας στα παιδιά, στη μείωση της αξιοπιστίας των καταθέσεών τους, στην ανεξέλεγκτη επανάληψη επιζήμιων ψυχολογικών διαδικασιών και άλλα. Σε αυτό το πλαίσιο, η ανηλικία υφίσταται ακόμη μεγαλύτερη πίεση και υποβάλλεται σε περαιτέρω ψυχολογικό τραύμα.

Επιπλέον, διαμορφώνεται μια διαδικασία που, κυρίως λόγω της κατά γράμμα ερμηνείας του νόμου, ο ρόλος του παιδοψυχολόγου περιορίζεται σε μια απλή ιατρική αξιολόγηση σχετικά με τη σωστή λειτουργία της αντίληψης και των ψυχικών λειτουργιών του ανήλικου μάρτυρα. Αυτό φυσικά δεν αρκεί για να δώσει στη μαρτυρική κατάθεση του παιδιού την απαιτούμενη αποδεικτική αξία. Έπειτα, είναι απαραίτητο να υπάρχει πραγματική εφαρμογή του άρθρου 227 ΚΠΔ του Κώδικα Ποινικής Δικονομίας, συνεπώς ο παιδοψυχολόγος δεν πρέπει να περιορίζεται σε μια απλή ιατρική γνωμάτευση, αλλά πρέπει να προβαίνει σε αξιολόγηση της μαρτυρικής κατάθεσης βάσει της προσωπικότητας του μάρτυρα. Αυτή η αξιολόγηση πρέπει να λαμβάνει υπόψη πτυχές όπως ο βαθμός ψυχραιμίας, αυτοκυριαρχίας, υποβολιμότητας και άλλες, ιδίως εν όψει του γεγονότος ότι ο ανήλικος μάρτυρας απουσιάζει κατά τη διάρκεια της διαδικασίας στο ακροατήριο.

[54] Θεμελή Ό. (2014).

4.4.1.4 Μέτρα προστασίας μαρτύρων σύμφωνα με τον Ν. 4139/2013

Σύμφωνα με το άρθρο 27 του νόμου 4139/2013, προβλέπεται η δυνατότητα υπαγωγής των δραστών που εμπλέκονται σε υποθέσεις ναρκωτικών στο καθεστώς προστασίας των άρθρων 9 και 10 του νόμου 2928/2001. Επιπλέον, προβλέπεται η λήψη ευνοϊκών μέτρων για εκείνους που συνδράμουν σημαντικά στην παροχή πληροφοριών που συμβάλλουν στην αντιμετώπιση εγκληματικής δράσης, υψηλότερου επιπέδου από εκείνο των μαρτύρων-δραστών, με στόχο την αντιμετώπιση εγκληματικής δράσης[55]. Σύμφωνα με το άρθρο 27 του νόμου 4139/2013, προβλέπεται η δυνατότητα υπαγωγής των δραστών που εμπλέκονται σε υποθέσεις ναρκωτικών στο καθεστώς προστασίας των άρθρων 9 και 10 του νόμου 2928/2001.

Επιπλέον, προβλέπεται η λήψη ευνοϊκών μέτρων για εκείνους που συνδράμουν σημαντικά στην παροχή πληροφοριών που συμβάλλουν στην αντιμετώπιση εγκληματικής δράσης, υψηλότερου επιπέδου από εκείνο των μαρτύρων-δραστών. Στις περιπτώσεις αυτές, η παροχή πληροφοριών από τον δράστη πριν την αμετάκλητη καταδίκη του, η οποία συνεισφέρει σημαντικά στην εξάρθρωση εγκληματικής οργάνωσης ή στη σύλληψη εμπόρων ναρκωτικών, επιφέρει την υποχρεωτική αναγνώριση ελαφρυντικού από το δικαστήριο, με την προϋπόθεση ότι η πράξη του προστατευόμενου είναι μικρότερης βαρύτητας από αυτήν των εμπλεκόμενων δραστών, και το δικαστήριο έχει την ευχέρεια να αναστείλει την εκτέλεση της ποινής. Παράλληλα, το δικαστήριο έχει την ευχέρεια να αναστείλει την εκτέλεση της επιβληθείσας στο δράστη ποινής, ανεξάρτητα από την συνδρομή των όρων της διάταξης του άρθρου 99 ΠΚ.

Επιπλέον, προβλέπεται η έκδοση βουλευμάτων αναστολής της ποινικής δίωξης και υφ' όρων απόλυσης του δράστη, ανεξάρτητα από τις προϋποθέσεις του άρθρου 105 ΠΚ. Συνεπώς, τα άτομα που εντάσσονται σε αυτά τα μέτρα ενδέχεται να έχουν τρεις ιδιότητες: αυτή του πληροφοριοδότη των διωκτικών αρχών, του κατηγορουμένου των αδικημάτων του νόμου 4139/2013, και του μάρτυρα για τις παρεχόμενες πληροφορίες[56]. Η εν λόγω έκθεση ένορκης εξέτασης μάρτυρα παραμένει εμπιστευτική, με τη γνώση της να διατίθεται μόνο στον εποπτεύοντα εισαγγελέα, διασφαλίζοντας τη μυστικότητα των πληροφοριών, ενώ φυλάσσονται σε ειδικό αρχείο της εισαγγελίας εφετών. Αυτές οι πληροφορίες δεν κοινοποιούνται στα πρόσωπα που αφορούν, προστατεύοντας έτσι τα υπερασπιστικά τους

[55] Παύλου Σ. / Σάμιος Θ. (2014), σελ 7.
[56] Τριανταφύλλου Α. (2014), σελ. 282-285.

δικαιώματα, τα οποία σύμφωνα με την υφιστάμενη θεωρία, παραμένουν αδιατάρακτα, καθώς η αναφερόμενη έκθεση δεν συμπεριλαμβάνεται στον φάκελο της δικογραφίας που συντάσσεται εναντίον τους. Ως αποτέλεσμα, οι δικαστές που θα εξετάσουν την υπόθεσή τους δεν θα έχουν γνώση αυτής της έκθεσης, διασφαλίζοντας την προστασία των δικαιωμάτων τους.

4.4.2 Στη Γερμανία

Στις 30 Απριλίου 1998 ψηφίστηκε στη Γερμανία ο νόμος για την προστασία των μαρτύρων (Zeugenschutzgesetz - ZSchG) και τέθηκε σε ισχύ την 1η Δεκεμβρίου 1998. Σύμφωνα με τον νόμο αυτό προβλέπεται αλλαγή στον γερμανικό Κώδικα Ποινικής Δικονομίας με την οποία να θεσπίζεται η δυνατότητα χρήσης οπτικοακουστικών μέσων κατά τη διεξαγωγή της ανάκρισης, ειδικά όσον αφορά τα παιδιά-θύματα, με στόχο τη μείωση του ψυχολογικού άγχους που συνήθως συνοδεύει την ανάκριση και τον κίνδυνο δευτερογενούς θυματοποίησης. Επιπλέον, ο νόμος καθιέρωσε τη δυνατότητα αυτεπάγγελτου διορισμού δικηγόρου για την υποστήριξη των μαρτύρων.

Τα πρωτόδικα δικαστήρια είχαν προηγουμένως επιτρέψει, σε ορισμένες περιπτώσεις, να γίνεται η ανάκριση παιδιών-μαρτύρων από τον προεδρεύοντα δικαστή εκτός της αίθουσας του δικαστηρίου και στη συνέχεια να μεταφέρεται αυτή η ανάκριση στην αίθουσα του δικαστηρίου, ένα μοντέλο που ονομάζεται μοντέλο Mainz[57]. Αυτή η πρακτική προκάλεσε αμφιλεγόμενες αντιδράσεις στη νομολογία, ιδίως όσον αφορά το άρθρο 226 StPO, το οποίο απαιτεί τη συνεχή παρουσία του δικαστή κατά τη διάρκεια της κύριας ακρόασης και το δικαίωμα του κατηγορουμένου για αντιπαράθεση σύμφωνα με το άρθρο 240 παρ. 2 StPO. Έχοντας υπόψη τα διάφορα μοντέλα, ο νομοθέτης αποφάσισε στη συνέχεια, μετά από πρόταση της Επιτροπής Διαμεσολάβησης[58], να επιλέξει το μοντέλο που εφαρμόζεται ήδη στο Ηνωμένο Βασίλειο, όπου ο πρόεδρος και οι άλλοι συμμετέχοντες στη διαδικασία δεν αποχωρούν από την ακρόαση, και ο μάρτυρας βρίσκεται σε άλλη τοποθεσία, ακούγεται μέσω απευθείας μετάδοσης εικόνας-ήχου[59].

Αρκετοί νόμοι περιλαμβάνονταν στο μεταρρυθμιστικό πρόγραμμα, ιδίως το 2004, 2009 και 2015[60], που επέφεραν περαιτέρω βελτιώσεις στο νομικό καθεστώς των μαρτύρων

[57] LG Mainz, Beschluss vom 26. Juni 1995 – 302 Js 21307/94 jug. 3 A Kls, NJW 1996.
[58] Deutscher Bundestag (1998), https://dserver.bundestag.de/btd/13/100/1310001.pdf.
[59] Siegismund C. (2009).
[60] Burhoff D. (2016)., https://www.burhoff.de/veroeff/aufsatz/zap_F22_861ff.htm#I.

που εμπλέκονται σε εγκλήματα. Ειδικότερα, αυτοί οι νόμοι διασφαλίζουν ότι οι μάρτυρες δεν θεωρούνται πλέον απλώς μέσα για την εξεύρεση της αλήθειας, αλλά πρέπει να θεωρούνται και να αντιμετωπίζονται ως ανεξάρτητα νομικά υποκείμενα[61].

4.4.2.1 Νόμος για την εναρμόνιση της προστασίας των ευάλωτων μαρτύρων

Στη γερμανική ποινική διαδικασία, ο μάρτυρας είναι ένα από τα πιο σημαντικά στοιχεία. Σύμφωνα με το άρθρο 48 παρ. 1 προτ. 2 StPO, ένας μάρτυρας είναι κατά κανόνα υποχρεωμένος να καταθέσει. Σύμφωνα με τα άρθρα 52 επ. StPO, δικαίωμα επιλογής υπάρχει μόνο για στενούς συγγενείς, για όσους έχουν επαγγελματικό απόρρητο, όπως οι δικηγόροι υπεράσπισης ποινικών πράξεων, και για μάρτυρες που θα έπρεπε να αυτοενοχοποιηθούν μέσω μαρτυρία. Η συμμετοχή ενός μάρτυρα στην ποινική διαδικασία, η οποία γενικά δεν είναι προαιρετική, μπορεί μερικές φορές να θέσει σε κίνδυνο τον εαυτό του ή για τα κοντινά του πρόσωπα[62]. Για την προστασία τόσο των ίδιων των μαρτύρων όσο και για την έμμεση εξασφάλιση της ορθής διεξαγωγής της ποινικής διαδικασίας σε αυτήν την ένταση μεταξύ του προσδιορισμού της αλήθειας και των ανησυχιών προστασίας, υπάρχουν κρατικά μέτρα προστασίας μαρτύρων. και προστασία μαρτύρων μετά το πέρας ή εκτός ποινικής διαδικασίας.

4.4.2.2 Προστασία μαρτύρων εκτός ποινικής διαδικασίας

Η προστασία των μαρτύρων στη Γερμανία δεν περιορίζεται σε συγκεκριμένους τομείς εγκληματικότητας. Αντίθετα, τα μέτρα προστασίας μαρτύρων αξιολογούνται κατά περίπτωση και είναι ανάλογα και κατάλληλα. Η προστασία μαρτύρων εκτός ποινικής διαδικασίας ρυθμίζεται πρωτίστως από τον Νόμο για την εναρμόνιση της προστασίας των μαρτύρων σε κίνδυνο (Zeugenschutz-Harmonisierungsgesetz - ZSHG).

Σύμφωνα με το άρθρο 1 παρ. 1 ZSHG, προϋπόθεση για την ένταξη ενός ατόμου σε πρόγραμμα προστασίας μαρτύρων είναι η ύπαρξη συγκεκριμένου κινδύνου για ένα πρόσωπο, χωρίς τη συμβολή του οποίου σε ποινική διαδικασία η διερεύνηση των γεγονότων της υπόθεσης ή ο προσδιορισμός της θέσης των κατηγορουμένων θα ήταν αδύνατος ή σημαντικά δυσκολότερος. Με τη συγκατάθεσή τους, αυτά τα άτομα μπορούν να προστατευθούν με ειδικό τρόπο, εάν υπάρχουν πραγματικά στοιχεία που καθιστούν πιθανό ότι θα προκληθεί

[61] Bock S. (2013), https://www.zis-online.com/dat/artikel/2013_4_747.pdf.

[62] Μια έρευνα σχετικά με τον αριθμό των υποθέσεων προστασίας μαρτύρων από το 2004 έως το 2009 έδειξε ότι περίπου το 72% των μέτρων προστασίας μαρτύρων αποδίδονταν στο οργανωμένο έγκλημα [βλ. Mischkewitz A. (2014), σελ. 38].

ζημιά στη ζωή, τα μέλη, την ελευθερία ή την ιδιοκτησία ως αποτέλεσμα της δήλωσης. Σύμφωνα με την ενότητα 1 παρ. 2 ZSHG, συγγενείς του μάρτυρα ή άτομα που βρίσκονται κοντά του μπορούν επίσης να λάβουν μέρος σε αυτή την προστασία.

Σύμφωνα με τη διατύπωση των διατάξεων του ZSHG, ο μάρτυρας δεν έχει νόμιμο δικαίωμα να συμπεριληφθεί σε πρόγραμμα προστασίας. Κατ' αρχήν, ο μάρτυρας δεν δικαιούται επίσης ατομικά προστατευτικά μέτρα από την υπηρεσία προστασίας μαρτύρων. Η απόφαση σχετικά με την έναρξη, το είδος, το πεδίο εφαρμογής και την περάτωση τέτοιων μέτρων απαιτεί έλεγχο αναλογικότητας σε κάθε μεμονωμένη περίπτωση, ιδίως τη σοβαρότητα του εγκλήματος, τον λόγο του κινδύνου, τα δικαιώματα του κατηγορουμένου του προσώπου κατά του οποίου πρόκειται να κατατεθεί πρέπει να ληφθούν υπόψη τα αποτελέσματα της προστασίας των μαρτύρων.

Ακολούθως στην ενότητα 1 παρ. 4 ZSHG καθορίζεται ο χρόνος και οι προϋποθέσεις τερματισμού των μέτρων προστασίας. Αυτό ισχύει ιδιαίτερα όταν η απειλή δεν υφίσταται πλέον. Από την άλλη πλευρά, η περάτωση της ποινικής διαδικασίας δεν οδηγεί αυτομάτως στην απώλεια της προστασίας των μαρτύρων. Αυτό σημαίνει ότι ακόμη και αν ο μάρτυρας δεν θεωρείται πλέον ως αποδεικτικό στοιχείο στην ποινική διαδικασία, η προστασία του μάρτυρα θα διατηρηθεί έως ότου δεν υφίσταται πλέον ο συγκεκριμένος κίνδυνος για τον πρώην μάρτυρα.

Σύμφωνα με την ενότητα 5 ZSHG, οι υπηρεσίες προστασίας μαρτύρων υποχρεούνται να παρέχουν στα προς προστασία πρόσωπα έγγραφα και αποδεικτικά στοιχεία που μπορούν να χρησιμοποιηθούν για τη διαμόρφωση μιας εικονικής ταυτότητας (ταυτότητα καμουφλάζ), ενώ σύμφωνα με την ενότητα 4 ZSHG, οι υπηρεσίες προστασίας μαρτύρων μπορούν να αρνηθούν να παράσχουν σε δημόσιους και μη δημόσιους φορείς (αλλά όχι στον εισαγγελέα) οποιαδήποτε πληροφορία σχετικά με προσωπικά δεδομένα του προς προστασία προσώπου, στο βαθμό που αυτό είναι απαραίτητο για την προστασία τους .

Δεδομένου ότι όλα τα μέτρα που λαμβάνονται ως μέρος της προστασίας μαρτύρων, όπως η έκδοση συνοδευτικών εγγράφων, τα οικονομικά οφέλη ή ο τερματισμός της προστασίας μαρτύρων, μπορούν να επανεξεταστούν από διοικητικό δικαστήριο ανά πάσα στιγμή, οι υπηρεσίες προστασίας μαρτύρων υποχρεούνται να παρέχουν πλήρη αιτιολόγηση σχετικά με την εφαρμογή αυτών. Ένας Κανονισμός σχετικά με αυτό μπορεί να βρεθεί στην ενότητα 2 παρ. 3 ZSHG.

4.4.2.3 Προστασία μαρτύρων κατά την ποινική διαδικασία

Εκτός από τα μέτρα που βασίζονται στο ZSHG για την προστασία των ατόμων που διατρέχουν κίνδυνο, ο Κώδικας Ποινικής Δικονομίας (Strafprozessordnung - StPO) και ο Νόμος για το Συνταγματικό Δικαστήριο (Gerichtsverfassungsgesetz - GVG) περιέχουν επιπρόσθετες επιλογές για τη διασφάλιση της προστασίας των μαρτύρων στις εν εξελίξει ποινικές διαδικασίες.

Ειδικότερα, σύμφωνα με το άρθρο 247 StPO, ο κατηγορούμενος μπορεί να απομακρυνθεί προσωρινά από την κύρια δίκη, ενώ εάν υπάρχει τεκμηριωμένη υποψία ότι η δήλωση του τόπου κατοικίας θα θέσει σε κίνδυνο τον μάρτυρα ή άλλο πρόσωπο, ο μάρτυρας μπορεί, σύμφωνα με το άρθρο 68 παρ. 2 και 3 StPO, να δηλώσει τον τόπο εργασίας του αντί του τόπου κατοικίας τους. Περαιτέρω, ο πρόεδρος μπορεί να επιτρέψει στον μάρτυρα της κύριας ακρόασης να μην δηλώσει τον τόπο διαμονής του.

Οι δικαστικές, εισαγγελικές και αστυνομικές ανακρίσεις (άρθρο 161a παρ. 1 προτ. 2 StPO) κατά την προκαταρκτική έρευνα μπορούν να καταγράφονται σύμφωνα με το άρθρο 58a StPO με οπτικοακουστικό μέσο, σύμφωνα με το οποίο *"Η ανάκριση μάρτυρα μπορεί να καταγραφεί σε βίντεο και ήχο. Θα πρέπει να καταγράφεται αφού αξιολογηθούν οι σχετικές περιστάσεις και θα πρέπει να διεξαχθεί ως δικαστική ακρόαση εάν: 1. έτσι ώστε να προστατεύονται καλύτερα τα συμφέροντα που αξίζουν προστασίας ατόμων κάτω των 18 ετών και ατόμων που, ως παιδιά ή νέοι, έχουν τραυματιστεί από ένα από τα εγκλήματα που αναφέρονται στο άρθρο 255α παράγραφος 2 ή 2. Η ανησυχία είναι ότι ο μάρτυρας δεν μπορεί να ακουστεί στην κύρια ακρόαση και η ηχογράφηση είναι απαραίτητη για να διαπιστωθεί η αλήθεια…."*. Το άρθρο αυτό παραπέμπει στις διατάξεις περί ανάγνωσης εγγράφων, θέτοντας προϋποθέσεις σχετικά με την ορθή ενημέρωση του κατηγορούμενου.

Η καταγραφή της μαρτυρίας στην κύρια ανάκριση ορίζεται στο άρθρο 247a προτ. 4 StPO, αφού το δικαστήριο διατάξει να παραμείνει ο μάρτυρας σε άλλο σημείο κατά την εξέταση. Στην περίπτωση αυτή η κατάθεσή του μεταδίδεται με τη βοήθεια τεχνολογικών μέσων στην δικαστική αίθουσα με εικόνα και ήχο. Η παρουσίαση των αρχείων που δημιουργήθηκαν με αυτόν τον τρόπο ως μέρος της διεξαγωγής αποδεικτικών στοιχείων ορίζεται στο άρθρο 255a StPO. Σύμφωνα με τις διατάξεις 223, 251 StPO, το δικαστήριο μπορεί να εξετάσει εάν ένας μάρτυρας αναμένεται να εμφανιστεί στην κύρια ακρόαση ή να καταθέσει καθόλου, λαμβάνοντας υπόψη τα προσωπικά του συμφέροντα. Το κοινό μπορεί να αποκλειστεί σύμφωνα με τις ενότητες 170 επ. GVG.

4.4.2.4 Νόμος περί Ψυχοκοινωνικής Υποστήριξης σε ποινικές διαδικασίες - Psychosoziale Prozessbegleitung im Strafverfahren (PsychPbG)

Επιπλέον, με στόχο την συμμόρφωση με την ευρωπαϊκή Οδηγία για την προστασία των θυμάτων, τέθηκε σε ισχύ από την 1η Ιανουαρίου 2017 ο νόμος περί ψυχοκοινωνικής υποστήριξης σε ποινικές διαδικασίες. Ειδικότερα, τα παιδιά και οι νέοι που έχουν πέσει θύματα σοβαρών σεξουαλικών ή βίαιων εγκλημάτων δικαιούνται νομικά δωρεάν ψυχοκοινωνική υποστήριξη κατά τη διάρκεια της διαδικασίας (άρθρο 406g StPO). Όσον αφορά άλλα θύματα σοβαρών βίαιων και σεξουαλικών εγκλημάτων, το δικαστήριο θα πρέπει να αποφασίζει, ανάλογα με την εκάστοτε περίπτωση, εάν πρέπει να παρέχεται ψυχοκοινωνική υποστήριξη.

Η ψυχοκοινωνική υποστήριξη είναι μια εξαιρετικά πυκνή μορφή υποστήριξης πριν, κατά τη διάρκεια και μετά την ποινική διαδικασία. Περιλαμβάνει ειδική υποστήριξη, παροχή πληροφοριών και συνδρομή καθ' όλη τη διάρκεια της δίκης. Κύριος στόχος είναι η μείωση του ψυχολογικού βάρους που αντιμετωπίζουν τα θύματα. Σημαντικό να σημειώσουμε ότι η δικαστική υποστήριξη δεν αντικαθιστά τη ρόλο του δικηγόρου. Οι νομικές συμβουλές εξακολουθούν να είναι αποκλειστική ευθύνη των δικηγόρων. Η ψυχοκοινωνική υποστήριξη αποτελεί μη νομική υποστήριξη και αποτελεί μια επιπλέον προσφορά για τα θύματα που έχουν ειδικές ανάγκες προστασίας. Σημαντικό είναι ότι οι ψυχοκοινωνικοί κηδεμόνες έχουν το δικαίωμα να παρακολουθούν την ανάκριση του θύματος[63].

Ειδικότερα, η ψυχοκοινωνική υποστήριξη κατά τη διάρκεια της ποινικής διαδικασίας δικαιούνται κατ' αρχήν οι ανήλικοι που έχουν πέσει θύματα βίαιων και σεξουαλικών εγκλημάτων. Ωστόσο, πρέπει να υποβάλουν αίτηση στο δικαστήριο, το οποίο, εάν πληρούνται οι προϋποθέσεις, θα προσφέρει και νομική υποστήριξη. Ενήλικα θύματα βίαιων ή σεξουαλικών εγκλημάτων μπορεί επίσης να δικαιούνται ψυχοκοινωνικής υποστήριξης στη διαδικασία, καθώς και τα παιδιά, οι γονείς, τα αδέρφια, οι σύζυγοι ή οι σύντροφοι που έχουν υποστεί απώλεια ενός συγγενούς λόγω εγκλήματος. Η απόφαση για την χορήγηση αυτής της υποστήριξης στα ενήλικα θύματα βίαιων ή σεξουαλικών εγκλημάτων, καθώς και στους στενούς συγγενείς των ατόμων που έχουν πέσει θύματα κρίνεται από το δικαστήριο.

[63] BMJ, https://www.bmj.de/DE/themen/praevention_opferhilfe/opferschutz_strafverfahren/psychosoziale_prozessbegleitung/psychosoziale_prozessbegleitung.html.

Τέλος, πρέπει να σημειωθεί ότι στη Γερμανία τίθενται υψηλές απαιτήσεις όσον αφορά τις δεξιότητες των ψυχολόγων-ψυχοθεραπευτών. Οι ελάχιστες απαιτήσεις προσόντων ρυθμίζονται από το νόμο για την ψυχοκοινωνική υποστήριξη σε ποινικές διαδικασίες (PsychPbG). Ο συντονιστής της διαδικασίας πρέπει να διαθέτει επαγγελματικά, προσωπικά και διεπιστημονικά προσόντα, ώστε η στήριξη που θα παρέχει στο θύμα να είναι ουσιαστική και τα συμπεράσματα που θα εξάγει ρεαλιστικά και εύστοχα, χωρίς να αρκείται σε μία τυπική ιατρική γνωμάτευση.

4.5 Αστυνομική οργάνωση, Εξειδικευμένες Υπηρεσίες και Κέντρα Αριστείας

Η ευρεία χρήση νέων τεχνολογιών επηρεάζει τη συμπεριφορά των ανθρώπων καθώς και τις εργασιακές και επιχειρηματικές διαδικασίες, συμπεριλαμβανομένων των αρχών ασφαλείας. Η σύγχρονη τεχνολογία πληροφοριών και επικοινωνιών, και ιδιαίτερα το διαδίκτυο, δεν αποτελούν μόνο νέους, αόριστους χώρους εγκλήματος για τις αρχές ασφαλείας, οι τεχνολογικές εξελίξεις παρέχουν παράλληλα νέους τρόπους πρόληψης κινδύνου και καταπολέμησης του εγκλήματος, όπως για παράδειγμα η Πανευρωπαϊκή Δικτύωση Αστυνομικών Πληροφοριών (SIRENE)[64] ή η παρακολούθηση ψηφιακών ιχνών που αφήνουν πίσω τους τα ποινικά αδικήματα στο διαδίκτυο.

Για τις αστυνομικές αρχές, είναι σημαντικό να διατηρούν συνεχή επαφή και ενημέρωση σχετικά με τις νέες τεχνολογίες, προκειμένου να αντιμετωπίζουν αποτελεσματικά τις νέες μορφές εγκληματικότητας. Επιπλέον, πρέπει να εφαρμόζονται στρατηγικές δράσης κατάλληλες να αντιμετωπίσουν τις προκλήσεις που προκύπτουν από την ψηφιοποίηση. Το διαδίκτυο δεν πρέπει να λειτουργεί χωρίς να υπόκειται σε επιβολή του νόμου. Αυτό σημαίνει ότι πρέπει να αναπτύσσονται νέες τεχνολογικές γνώσεις και συγκεκριμένα μέτρα, ενώ πρέπει να αναγνωρίζονται οι εγκληματικές πράξεις και να διατηρούνται αποδεικτικά στοιχεία κατά

[64] Τα γραφεία SIRENE παρέχουν πρόσθετες πληροφορίες για προειδοποιήσεις και συντονίζουν τις ενέργειες που σχετίζονται με προειδοποιήσεις στο Σύστημα Πληροφοριών Σένγκεν (SIS). Φροντίζουν να ληφθούν τα απαραίτητα μέτρα όταν ένας καταζητούμενος συλλαμβάνεται ή ένας αγνοούμενος, όταν ένα άτομο που απορρίπτεται στα σύνορα προσπαθεί να εισέλθει ξανά στον χώρο Σένγκεν, όταν ένα κλεμμένο όχημα ή έγγραφο ταυτότητας κατασχέθηκε, κ.λπ. Η περιοχή αναφέρεται ως χώρος Σένγκεν των οποίων τα εσωτερικά σύνορα δεν υπόκεινται σε ελέγχους. Τα γραφεία SIRENE ανταλλάσσουν επίσης σημαντικά δεδομένα για αστυνομική και δικαστική συνεργασία, πραγματοποιούν έρευνα βάσεων δεδομένων, συντονίζουν διασυνοριακές επιχειρήσεις κ.λπ. (βλ. Europäische Kommission, https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/sirene-cooperation_de).

τη διαχείριση των μέσων ενημέρωσης και επικοινωνίας, προκειμένου να προστατεύονται οι πολίτες από τυχόν εγκληματικές επιθέσεις.

Ακόμα, για να αντιμετωπιστεί αποτελεσματικά το ηλεκτρονικό έγκλημα, είναι απαραίτητο να υπάρχει ενεργή παρουσία της αστυνομίας στο διαδίκτυο. Οι εικονικές περιπολίες στο διαδίκτυο είναι εξίσου σημαντικές με τις πεζές περιπολίες στο κέντρο της πόλης. Η αστυνομία πρέπει να εκτελεί έρευνα στο διαδίκτυο συστηματικά, προκειμένου να αυξήσει τον κίνδυνο δίωξης για τους εγκληματίες και το ύποπτο περιεχόμενο να εντοπίζεται άμεσα.

Στο πλαίσιο αυτό, στην Ελλάδα συστάθηκε με το Π.Δ. 178/2014 η Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα την Αθήνα και η Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα τη Θεσσαλονίκη. Στόχος είναι η πρόληψη, η έρευνα και η καταπολέμηση των ηλεκτρονικών εγκλημάτων και των κυβερνοεγκλημάτων, αποσκοπώντας στον ενισχυμένο ρόλο της αστυνομίας στην αντιμετώπιση των κυβερνοεγκλημάτων και την προστασία της ασφάλειας του κυβερνοχώρου και των πολιτών.

Εσωτερικά διαρθρώνεται σε πέντε τμήματα που καλύπτουν το σύνολο του φάσματος προστασίας των πολιτών και διασφαλίζουν την προστασία στον κυβερνοχώρο. Πιο αναλυτικά, η Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος αποτελείται από το Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών, το Τμήμα Καινοτόμων Δράσεων και Στρατηγικής, το Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων, το Τμήμα διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης και το Τμήμα Ειδικών Υποθέσεων και Δίωξης διαδικτυακών Οικονομικών Εγκλημάτων[65].

Αντίστοιχα, η Ομοσπονδιακή Αστυνομία Εγκλημάτων της Γερμανίας (BKA) συνέστησε για τον παραπάνω σκοπό το Κεντρικό Γραφείο Ανεξάρτητης Έρευνας σε Δίκτυα Δεδομένων (Zentralstelle für anlassunabhängige Recherchen in Datennetzen - ZaRD). Το ZaRD αποτελεί μέρος του Κέντρου Τεχνικής Ανάπτυξης και Εξυπηρέτησης για Καινοτόμες Τεχνολογίες που έχει ιδρυθεί από την BKA, με βασικά καθήκοντα την ανάπτυξη και τη δοκιμή μεθόδων και εργαλείων για την ασφάλεια, τη διερεύνηση, την οπτικοποίηση, την επεξεργασία και την παροχή ψηφιακών δεδομένων με στόχο την αξιολόγηση από τα εντεταλμένα ερευνητικά τμήματα.

[65] Ελληνική Αστυνομία (2022), https://www.astynomia.gr/elliniki-astynomia/eidikes-ypiresies/diefthynsi-dioxis-ilektronikou-egklimatos/

Στο πλαίσιο της γενικής οργανωτικής δομής, στο αρχηγείο της αστυνομίας συγκροτούνται σε εθνικό και περιφερειακό επίπεδο εξειδικευμένες ανακριτικές μονάδες για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Συνεπώς, αυτές οι μονάδες χειρίζονται περίπλοκες υποθέσεις εγκλήματος στον κυβερνοχώρο, όπως π.χ. η εισβολή σε συστήματα πληροφορικής (hacking), οι επιθέσεις άρνησης υπηρεσίας και η διανομή κακόβουλου λογισμικού, ειδικά εάν εντοπιστούν μέθοδοι επιθεώρησης συμμοριών ή εμπορικών. Η τακτική διεκπεραίωση υποθέσεων απαιτεί ειδική τεχνογνωσία στον τομέα της πληροφορικής και ειδικές μεθόδους τεχνικής απόδειξης. Εκτός από την εξασφάλιση ψηφιακών ιχνών και την ιατροδικαστική εξέταση συστημάτων πληροφορικής, το πεδίο δραστηριότητας περιλαμβάνει επίσης την επεξεργασία και, εάν χρειαστεί, την αποκρυπτογράφηση ασφαλισμένων δεδομένων[66].

Η έρευνα στο διαδίκτυο πραγματοποιείται με διακρατική προσέγγιση και σε συνεργασία μεταξύ των εμπλεκόμενων τμημάτων. Τόσο η ομοσπονδιακή όσο και η πολιτειακή κυβέρνηση έχουν δημιουργήσει μια κοινή συντονιστική ομάδα για την ανεξάρτητη έρευνα στο διαδίκτυο. Στα Γραφεία της Κρατικής Εγκληματικής Αστυνομίας, οι ανακριτές χρησιμοποιούν σχεδόν όλες τις υπηρεσίες διαδικτύου για να αναζητήσουν ύποπτο περιεχόμενο, προκειμένου να επιτύχουν ποινική δίωξη, πρόληψη κινδύνου και εγκλημάτων[67].

Επιπλέον, οι πολίτες πρέπει να έχουν εμπιστοσύνη, ότι το κράτος και οι δημόσιοι θεσμοί θα προστατεύσουν την ασφάλειά τους. Είναι σημαντικό να αισθάνονται ότι το κράτος δικαίου λειτουργεί αποτελεσματικά, ότι τα ποινικά αδικήματα διώκονται και ότι υπάρχει σεβασμός στους κανόνες συνύπαρξης στην κοινωνία. Επίσης, πρέπει να εμπιστεύονται ότι η αστυνομία είναι κατάλληλα εξοπλισμένη και ικανή να αντιμετωπίζει τα καθήκοντά της σε ένα δυναμικά μεταβαλλόμενο περιβάλλον με βιώσιμο τρόπο. Οι κυβερνοεπιθέσεις έχουν τον δυνητικό κίνδυνο να προκαλέσουν σημαντική ζημιά, τόσο στην οικονομία, τη ζωή και την ασφάλεια των ανθρώπων όσο και στο ίδιο το κράτος. Η πρόληψη των κινδύνων στον κυβερνοχώρο είναι καθήκον της ομοσπονδιακής και της πολιτειακής αστυνομίας. Ωστόσο, είναι σημαντικό η δράση να είναι συναρμολογημένη και να μην παραμελούνται η δυνατότητα παρουσίας και προσβασιμότητας της αστυνομίας στον φυσικό κόσμο.

Στην Ελλάδα λειτουργεί από το 2013 το Ελληνικό Κέντρο για το Κυβερνοέγκλημα (GCC), με στόχο τη βελτίωση πρόληψης και αντιμετώπισης, την εκπαίδευση και την έρευνα

[66] Wernert M. (2021), σελ. 64.
[67] Deutscher Bundestag (2011), https://dserver.bundestag.de/btd/17/058/1705835.pdf.

στο αναπτυσσόμενο, με γοργούς ρυθμούς, έγκλημα στον κυβερνοχώρο, συμπληρώνοντας διακρατικά έργα[68]. Το σύστημα προστασίας στη Γερμανία που βασίζεται σε διαδικτυακή πλατφόρμα προορίζεται να ανταποκρίνεται σε αυτή τη νέα αντίληψη σχετικά με την αντιμετώπιση του ηλεκτρονικού εγκλήματος. Επιπλέον, για περισσότερα από 40 χρόνια, το αστυνομικό πρόγραμμα πρόληψης του εγκλήματος των ομοσπονδιακών πολιτειών και της ομοσπονδιακής κυβέρνησης (Polizeiliche Kriminalprävention der Länder und des Bundes - ProPK) επιδιώκει τον στόχο της εκπαίδευσης του πληθυσμού, των πολλαπλασιαστών, των μέσων ενημέρωσης και άλλων υπηρεσιών πρόληψης σχετικά με τις μορφές εγκλήματος και τους τρόπους πρόληψής τους. Η πλατφόρμα πληροφορικής *"Polizei 2020"*[69], μια πλατφόρμα ψηφιακής συνεργασίας, παρέχει την τεχνική βάση για αυτό. Υπάρχουν, ακόμα, πανευρωπαϊκές προσπάθειες με το σύστημα SIRIUS[70], μια πλατφόρμα για επαγγελματικές ανταλλαγές, για βέλτιστες πρακτικές, τεχνογνωσία, τεχνικές πληροφορίες και εμπειρία στον τομέα των ερευνών στο διαδίκτυο.

Ευρωπαϊκός στόχος είναι, διάφορα καθήκοντα σχετιζόμενα με την καταπολέμηση και την έρευνα των εγκλημάτων στον κυβερνοχώρο να εκτελούνται από εξειδικευμένες υπηρεσίες συνεργαζόμενες με τις αστυνομικές και δικαστικές αρχές. Θα πρέπει να επιτελούν λειτουργίες εξυπηρέτησης και υποστήριξης πολιτών και αστυνομικών υπηρεσιών, διοικητικών και δικαστικών αρχών. Εκτός από τη διεξαγωγή ανεξάρτητης έρευνας στο διαδίκτυο και την ανάληψη και επεξεργασία πολύπλοκων διαδικασιών έρευνας, θα δύναται να αναπτύσσονται βασικές έννοιες στρατηγικού ελέγχου. Η εντατική και συνεχής παρατήρηση της αγοράς χρησιμεύει στον εντοπισμό των πιο πρόσφατων τεχνολογιών και εξελίξεων. Τα ευρήματα αναγνώρισης και έρευνας χρησιμεύουν για την ανάπτυξη αποτελεσματικών αντιλήψεων μάχης και προσεγγίσεων πρόληψης. Η μόνιμη μελέτη των νέων εξελίξεων στον τομέα της πληροφορικής καταλαμβάνει χώρο παράλληλα με τα άλλα καθήκοντα.

Στο επίκεντρο της έρευνας και της ανάπτυξης αυτής βρίσκεται ο τομέας της ανάλυσης φορέων δεδομένων. Στη συντριπτική πλειονότητα των διερευνητικών υποθέσεων που σχετίζονται με την τεχνολογία πληροφοριών, το καθήκον είναι να καταστούν αναγνώσιμες οι

[68] Greek Cybercrime Center, https://www.cybercc.gr/el/poioi-eimaste/.
[69] BKA, https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/ElektronischeFahndungsInformationssysteme/Polizei2020/Polizei2020_node.html.
[70] Eurojust, https://www.eurojust.europa.eu/sirius.

πληροφορίες που είναι αποθηκευμένες σε φορείς δεδομένων. Τα στοιχεία περιλαμβάνουν φορείς δεδομένων σε αμέτρητες μορφές, μαγνητικές ταινίες, κασέτες μαγνητικής ταινίας, σκληρούς και αφαιρούμενους δίσκους, κάρτες μνήμης όλων των μορφών, συσκευές ανάγνωσης ηλεκτρονικών βιβλίων, κονσόλες παιχνιδιών, κάρτες τσιπ, οπτικά μέσα, καθώς και κινητά τηλέφωνα/έξυπνα τηλέφωνα και κάρτες SIM. Παρωχημένα ηλεκτρονικά στοιχεία, όπως PDA και κάρτες με μαγνητικές λωρίδες ή ηλεκτρονικά ημερολόγια, βρίσκονται επίσης μεταξύ των κατασχέσεων και απαιτούν έρευνα και επεξεργασία. Οι χώροι αποθήκευσης στο διαδίκτυο, η λεγόμενη αποθήκευση cloud, συναντώνται όλο και πιο συχνά, δημιουργώντας νέες προκλήσεις και δυσχέρειες στην έρευνα.

4.6 Εκπαίδευση προσωπικού και τεχνικός εξοπλισμός

Ένα ακόμα ζήτημα είναι ότι προκειμένου η αστυνομία να είναι σε θέση να παρακολουθεί την τεχνική πρόοδο στην εγκληματική πλευρά, απαιτείται ολοκληρωμένη και ενημερωμένη εξειδικευμένη γνώση για την αποτελεσματική καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Οι ειδικά εκπαιδευμένοι αστυνομικοί θα πρέπει να διαθέτουν τις απαραίτητες γνώσεις πληροφορικής και την απαραίτητη *"ανακριτική τεχνογνωσία"*. Εμπειρογνώμονες πληροφορικής που αποκτήθηκαν για τις ανακριτικές αρχές, π.χ. μηχανικοί και ειδικοί πληροφορικής και αντίστοιχα, οι απόφοιτοι κατάλληλων πανεπιστημιακών μαθημάτων ενσωματώνονται στην αστυνομική υπηρεσία[71].

Στη Γερμανία, η εκπαίδευση και η εξειδίκευση σε θέματα ψηφιακής εγκληματολογίας πραγματοποιούνται σε πανεπιστημιακές σχολές σε συνεργασία με τις αστυνομικές αρχές[72]. Ένας αναδυόμενος τομέας της ιατροδικαστικής πληροφορικής διακρίνεται σε δύο κατηγορίες, την μεταθανάτια ανάλυση και τη ζωντανή εγκληματολογία. Το κριτήριο διάκρισης μεταξύ των δύο αυτών είναι ο χρονικός παράγοντας της εξέτασης. Στη μεταθανάτια ανάλυση, τα ίχνη εξετάζονται μετά την εκδήλωση ενός περιστατικού (συνήθως χρησιμοποιώντας εικόνες δίσκου, γνωστές ως εικόνες), ενώ στη ζωντανή εγκληματολογία, η εξέταση μπορεί να πραγματοποιηθεί κατά τη διάρκεια του περιστατικού, αλλά τουλάχιστον όσο το σύστημα είναι λειτουργικό. Στη ζωντανή εγκληματολογία, η έμφαση δίνεται ιδιαίτερα στη δημιουργία αντιγράφων ασφαλείας ασταθών δεδομένων, που αναφέρονται κυρίως σε δεδομένα που χάνονται όταν το σύστημα απενεργοποιείται. Αυτά τα δεδομένα

[71] Wernert M. (2021), σελ. 66.
[72] LKA Βάδης-Βυρτεμβέργης (2016), https://im.baden-wuerttemberg.de/de/service/publikation/did/cybercrimedigitale-spuren.

περιλαμβάνουν πληροφορίες για τη μνήμη, διεργασίες που εκτελούνται, κρυπτογραφημένα δεδομένα που αποκρυπτογραφούνται κατά τη διάρκεια της εκτέλεσης, καθώς και τις υφιστάμενες συνδέσεις του συστήματος σε ένα δίκτυο[73].

Τα ψηφιακά ίχνη αποτελούν διαρκώς κινούμενα στοιχεία και είναι επιρρεπή στην συγκαλυψιμότητα. Ως αποτέλεσμα, η άμεση δημιουργία αντιγράφων ασφαλείας και η αξιολόγηση αυτών των ιχνών γίνονται όλο και πιο κρίσιμες. Στο μέλλον, οι σύγχρονες τεχνολογίες πιθανότατα θα επηρεάσουν το κλασικό έργο της αστυνομίας ακόμη περισσότερο από ό,τι μπορούμε να φανταστούμε σήμερα. Το ηλεκτρονικό έγκλημα προκαλεί όχι μόνο προβλήματα ποιότητας, αλλά και ποσότητας για τις αστυνομικές αρχές. Ο συνεχώς αυξανόμενος όγκος δεδομένων που πρέπει να αξιολογηθεί αποτελεί μια διαρκώς αυξανόμενη πρόκληση.

Παρόλα αυτά, οι εξειδικευμένοι φορείς και οι εμπειρογνώμονες μόνο τους δεν αποτελούν ικανοποιητική απάντηση στο έγκλημα στον κυβερνοχώρο. Αυτοί οι ειδικοί απαιτούν όχι μόνο συνεργασία μεταξύ του κράτους, των επιχειρήσεων και της έρευνας, αλλά και την ενσωμάτωση βασικών εξειδικευμένων γνώσεων σε κάθε αστυνομικό τμήμα. Είναι αναγκαίο να διδαχθούν οι νεαροί αστυνομικοί τις βασικές γνώσεις και δεξιότητες σχετικά με τον τομέα της εγκληματικότητας στις τεχνολογίες της πληροφορίας και των επικοινωνιών, έτσι ώστε να μπορούν να αντιμετωπίσουν επαγγελματικά το θέμα από την πρώτη στιγμή. Αυτό περιλαμβάνει, για παράδειγμα, την κατανόηση των διάφορων μορφών εγκληματικότητας, την αξιολόγησή τους από ποινικής άποψης, καθώς και την ενασχόληση με την εγκληματολογία και την πρόληψη στον χώρο των τεχνολογιών της πληροφορίας και των επικοινωνιών. Οι βασικές γνώσεις θα πρέπει επίσης να συνδέονται με την οργανωτική δομή και τις αρμοδιότητες της αστυνομίας.

Για να πραγματοποιηθεί αποτελεσματική επαγγελματική δίωξη των αντίστοιχων μορφών εγκληματικότητας, απαιτείται συνεχής ενημέρωση του υλικοτεχνικού εξοπλισμού των ερευνητικών αστυνομικών αρχών. Είναι αυτονόητο ότι ο υψηλής απόδοσης υλικός εξοπλισμός με πρόσβαση στο διαδίκτυο πρέπει να είναι διαθέσιμος σε όλους τους τομείς. Εκτός από την κλασική χειρόγραφη εργασία, απαιτείται επίσης λογισμικό αξιολόγησης σε ορισμένα τμήματα. Η αστυνομία πρέπει να είναι ικανή και παρούσα στην επικοινωνία στο διαδίκτυο. Επιπλέον, θα πρέπει να αντιλαμβάνεται ανοιχτά τα μέσα κοινωνικής δικτύωσης ως χώρο εργασίας για την πρόληψη και την επικοινωνία με τον χρήστη, και όχι απλώς ως τόπο

[73] Wernert M. (2021), σελ. 67.

δίωξης του εγκλήματος. Στο μέλλον, όλοι οι αστυνομικοί, εξοπλισμένοι με smartphone ή, ακόμη καλύτερα, tablet PC, θα μπορούσαν να υπηρετήσουν διαδραστικά το καθήκον τους ακόμη και από πραγματικό περιπολικό. Με αυτόν τον τρόπο, οι αστυνομικοί θα γίνονταν αξιωματικοί της εικονικής περιοχής επαφής. Επιπλέον, θα μπορούσαν να δημιουργηθούν εικονικοί διαδικτυακοί φύλακες σε σχετικά ηλεκτρονικά μέσα και εφαρμογές[74].

Συγχρόνως, οι περισσότερες πολιτειακές αστυνομικές δυνάμεις στην Ευρώπη εκπροσωπούνται στο διαδίκτυο. Οι σελίδες των χρηστών στο Facebook, οι λογαριασμοί στο Twitter και λογαριασμοί αστυνομικών στο Instagram και στο Snapchat δίνουν τη δυνατότητα για επικοινωνία με την αστυνομία, ενώ παράλληλα παρέχουν στην αστυνομία την δυνατότητα να μεταδίδει πληροφορίες κατά τη διάρκεια των επιχειρήσεών της. Αυτό λαμβάνεται επίσης υπόψη από τον οργανωτικό τρόπο λειτουργίας, περιλαμβάνονται οδηγίες για την παροχή υπηρεσιών, κεντρικός συντονισμός από τους διαχειριστές και υπαλλήλους των μέσων κοινωνικής δικτύωσης, καθώς και κρατικός συντονισμός.

4.7 Εισαγγελέας ηλεκτρονικού εγκλήματος

Επιπροσθέτως των παραπάνω, είναι φανερό πλέον και πολλάκις έχει επαληθευτεί στην πράξη, ότι για τη διερεύνηση ηλεκτρονικών εγκλημάτων και την αξιοποίηση των αποδεικτικών μέσων και πειστηρίων είναι απαραίτητες εξειδικευμένες γνώσεις πληροφορικής. Δυστυχώς, οι εισαγγελείς και τα δικαστήρια συχνά στερούνται των απαιτούμενων εξειδικευμένων γνώσεων, οι οποίες αποτελούν αποφασιστικό πλεονέκτημα για την υπεράσπιση και την εν γένει καταπολέμηση των εγκλημάτων στον κυβερνοχώρο. Η γνώση των σύγχρονων τεχνικών, νομικών και πρακτικών εξελίξεων στον τομέα των σύγχρονων τεχνολογιών πληροφοριών και επικοινωνιών είναι ουσιαστικής σημασίας για την ορθή διεκπεραίωση των ποινικών ερευνών από την εισαγγελία.

Με στόχο την ενίσχυση της αρμοδιότητας των εισαγγελικών αρχών για τη δίωξη των εγκλημάτων στον κυβερνοχώρο, έχει προταθεί η θέσπιση του Εισαγγελέα ηλεκτρονικού εγκλήματος. Η πρόταση αυτή αφορά ουσιαστικά τη σύσταση μιας νέας υπηρεσίας ηλεκτρονικού εγκλήματος. Έργο αυτής αποτελεί η συνεργασία με τις αρχές επιβολής του νόμου, όπως η αστυνομία και η υπηρεσίες κυβερνοασφάλειας, για την ανίχνευση και τη δίωξη εγκλημάτων, η παροχή συμβουλών και η ενημέρωση σχετικά με τις απειλές του ηλεκτρονικού εγκλήματος και τον τρόπο προστασίας των προσωπικών τους δεδομένων, η

[74] Wernert M. (2021), σελ. 67.

αξιολόγηση των σχετικών πληροφοριών και η ενημέρωση της εισαγγελίας για τις εξελίξεις που είναι σημαντικές για την αποτελεσματική ποινική δίωξη σε αυτόν τον τομέα.

Προκειμένου, ο εισαγγελέας, να διεκπεραιώνει τις διαδικασίες σε αυτόν τον τομέα του εγκλήματος με ομοιόμορφο και αποτελεσματικό τρόπο, η υπηρεσία αυτή δημιουργεί βοηθήματα εργασίας, όπως απαιτείται - π.χ. φυλλάδια, έντυπα για υποθέσεις που εμφανίζονται συχνά - και θα τα θέτει στη διάθεση της εισαγγελίας. Η υπηρεσία ηλεκτρονικού εγκλήματος είναι αρμόδια, να έρχεται σε επαφή με όσους ασχολούνται με την καταπολέμηση του εγκλήματος πληροφορικής και με ζητήματα σύγχρονης ενημέρωσης και τεχνολογίες επικοινωνιών. Η συνεχής περαιτέρω ανάπτυξη των σύγχρονων τεχνολογιών πληροφοριών και επικοινωνιών ανοίγει τακτικά περαιτέρω δυνατότητες στις αρχές ποινικής δίωξης για τη διασάφηνση των γεγονότων. Εάν υπάρχει ανάγκη αξιολόγησης του θεμελιώδους νομικού παραδεκτού ενός ερευνητικού εργαλείου μιας συγκεκριμένης έρευνας, η υπηρεσία ηλεκτρονικού εγκλήματος θα πρέπει να διενεργήσει αντίστοιχη έρευνα. Για το αποτέλεσμα της έρευνας θα πρέπει να ενημερώνεται η Εισαγγελία.

Στην Γερμανία, υπηρεσία ηλεκτρονικού εγκλήματος λειτουργεί από την 1η Ιουλίου 2011 στο Γραφείο του Γενικού Εισαγγελέα στη Στουτγάρδη στη Βάδη-Βυρτεμβέργη[75]. Ακόμα, στη Βαυαρία, και τα 25 γραφεία εισαγγελικών υπηρεσιών που υπάρχουν, έχουν δημιουργήσει ειδικά τμήματα ή επαφές με εξωτερικούς επιστήμονες πληροφορικής που χειρίζονται επιτόπου διαδικασίες σε αυτόν τον τομέα του εγκλήματος. Από τον Ιανουάριο του 2010, η πολιτεία της Έσσης διαθέτει την πρώτη οργανωτική μονάδα γενικής εισαγγελίας στη Γερμανία, την «Κεντρική Υπηρεσία για την Καταπολέμηση του Εγκλήματος στο διαδίκτυο» (Zentralstelle zur Bekämpfung der Internetkriminalität - ZIT), η οποία χρησιμοποιείται αποκλειστικά για τη δίωξη ποινικών αδικημάτων που διαπράττονται μέσω διαδικτύου και είναι ιδρυτικό μέλος του Δικτύου Δικαστικού Κυβερνοεγκλήματος, ενός ευρωπαϊκού δικτύου δικαστικών αρχών για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο[76] [77].

Μαζί με τα τμήματα καταπολέμησης ηλεκτρονικού εγκλήματος στην Έσση, υπάλληλοι της εισαγγελίας της Φρανκφούρτης αναλαμβάνουν δράση κατά των εγκληματιών στο διαδίκτυο. Ταυτόχρονα, οι εμπειρογνώμονες του δικτύου είναι στη διάθεση των εισαγγελιών και των αστυνομικών τμημάτων της Έσσης ως αρμόδιες επαφές και παρέχουν

[75] Διάταγμα του Υπουργείου Δικαιοσύνης περί σύστασης κεντρικής υπηρεσίας για την καταπολέμηση του εγκλήματος της πληροφορίας και επικοινωνίας της 21ης Ιουνίου 2011 - Az.: 4100/0252.
[76] Staatsanwaltschaften Hessen, GStA Generalstaatsanwaltschaft Frankfurt am Main, https://gsta-frankfurt-justiz.hessen.de.
[77] Wernert M. (2021), σελ. 101.

την απαραίτητη τεχνογνωσία για αποτελεσματική καταπολέμηση του ηλεκτρονικού εγκλήματος. Επιπλέον, η ZIT, η οποία εδρεύει στο Gießen ως παράρτημα της εισαγγελίας της Φρανκφούρτης, είναι το γραφείο έκτακτης ανάγκης δημόσιας εισαγγελίας για διαδικασίες διαδικτύου της ομοσπονδιακής αστυνομίας, όπου η τοπική δικαιοδοσία είναι ακόμη ασαφής ή για μαζικές διαδικασίες εναντίον μεγάλου αριθμού υπόπτων σε όλη τη χώρα. Ως επιχειρησιακό κεντρικό γραφείο, η ZIT επεξεργάζεται ιδιαίτερα περίπλοκες και εκτενείς έρευνες από τους τομείς του εγκλήματος, όπως αυτές τις παιδικής πορνογραφίας και σεξουαλικής κακοποίησης παιδιών που σχετίζεται με το διαδίκτυο, εγκλήματα στο Darknet (καταπολέμηση εγκληματικών πλατφορμών Darknet και εμπόριο όπλων, ναρκωτικών και απομιμήσεων προϊόντων στο Darknet), επιθέσεις χάκερ, κλοπή δεδομένων και απάτη υπολογιστών κ.α..

Στην Ελλάδα, ο διάλογος σχετικά με τον ορισμό του Εισαγγελέα Ηλεκτρονικού Εγκλήματος έχει γίνει όλο και πιο έντονος. Το 2019, η Εισαγγελία του Αρείου Πάγου εξέδωσε εγκύκλιο με οδηγίες σχετικά με τη λειτουργία και τις αρμοδιότητες της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος. Στην εγκύκλιο αυτή, έγινε έκκληση για την αποστολή ποινικών δικογραφιών και εισαγγελικών παραγγελιών που αφορούν μόνο σοβαρές υποθέσεις κυβερνοεγκλημάτων και εφόσον αυτές απαιτούν εξειδικευμένη τεχνική ή ψηφιακή έρευνα και υπάγονται στην αρμοδιότητα της υπηρεσίας[78].

Σύμφωνα με την Εισαγγελία, στέλνονταν στην Υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, αν όχι όλες, οι πλείστες των υποθέσεων που σχετίζονται καθ' οιονδήποτε τρόπο με Τεχνολογίες Πληροφορικής και Επικοινωνιών, ανεξαρτήτως πολυπλοκότητας, σοβαρότητας ή απαίτησης εξειδικευμένων γνώσεων και έρευνας για τη διενέργεια προκαταρκτικής έρευνας ή προανάκρισης. Αυτή η εξέλιξη έχει αρνητικές επιπτώσεις στο έργο της υπηρεσίας, επιβαρύνοντας δυσμενώς το συνολικό της έργο με τη διαχείριση και τη διερεύνηση υποθέσεων μικρότερης σημασίας, δημιουργώντας προβλήματα στην αποτελεσματική λειτουργία της υπηρεσίας και την αντιμετώπιση σοβαρών περιπτώσεων κυβερνοεγκλημάτων.

[78] Lawspot (2019), https://www.lawspot.gr/nomika-nea/kyvernoegklima-poies-ypotheseis-prepei-na-parapempontai-sti-dioxi-ilektronikoy-egklimatos.

Ο Εισαγγελέας ηλεκτρονικού εγκλήματος, πράγματι θα μπορούσε να οδηγήσει σε μειωμένη γραφειοκρατία και λειτουργικά κόστη και αποφυγή της απώλειας κρίσιμου χρόνου για την εξέλιξη υποθέσεων που βρίσκονται υπό διερεύνηση. Για την ορθή και ταχεία αξιολόγηση ψηφιακών πειστηρίων, είναι απαραίτητες εξειδικευμένες γνώσεις και η ταχύτητα, τόσο κατά το στάδιο συλλογής των αποδεικτικών στοιχείων, όσο και κατα την αξιολόγησή τους. Είναι γνωστή η αξία του ρόλου του εισαγγελέα καθ' όλη την ποινική διαδικασία και είναι σημαντικό ο εισαγγελέας να έχει σφαιρική γνώση και άποψη επί των θεμάτων και υποθέσεων που επιλαμβάνεται, ενώ ο όγκος των υποθέσεων που σχετίζονται με το κυβερνοέγκλημα διαρκώς αυξάνεται.

Για τον λόγο αυτό, μάλιστα, τα τελευταία χρόνια στη Γερμανία εφαρμόζεται και συνεχίζεται η βασική και προηγμένη εκπαίδευση υποψηφίων εισαγγελέων και δικαστών προσανατολισμένη στην συγκεκριμένη κατεύθυνση, προκειμένου στο μέλλον, για τις υποθέσεις ηλεκτρονικών εγκλημάτων, αποκλειστικά αρμόδιοι να είναι εισαγγελείς που καλύπτουν τόσο το φάσμα των γνώσεων νομικής, όσο και πληροφορικής. Αυτό θα βελτιώσει την ανακριτική διαδικασία, την εξακρίβωση και αξιολόγηση των πειστηρίων, ενώ θα επιταχυνθεί η επίλυση και διαλεύκανση των εγκλημάτων στον κυβερνοχώρο.

4.8 Διακρατική συνεργασία - Διασυνοριακός έλεγχος

Οι διεθνείς διαστάσεις των ηλεκτρονικών εγκλημάτων δημιουργούν την ανάγκη για συνεργασία και συντονισμό μεταξύ χωρών και την εφαρμογή μέτρων, όχι μόνο εθνικών, αλλά και με την οργανωμένη διασυνοριακή δράση, σύμφωνα με τα διεθνή πρότυπα. Η καταπολέμηση των εγκλημάτων στον κυβερνοχώρο αποτελεί μια διεθνή πρόκληση, ειδικότερα λόγω του διασυνοριακού τους χαρακτήρα, με κοινό στόχο την αποτελεσματική πρόληψη των κινδύνων και την αποτελεσματική ποινική τους δίωξη[79]. Ορισμένες από τις κύριες παραμέτρους που έχουν τεθεί για την ισχυροποίηση του πλαισίου αυτού περιλαμβάνουν:

- Ενδελεχής αξιολόγηση των αναμενόμενων τεχνολογικών εξελίξεων και προοπτική ανάλυση των αναγκών για δράση.

- Επανεξέταση και επέκταση των υποδομών για την καταπολέμηση του ηλεκτρονικού εγκλήματος.

[79] Wernert M. (2021), σελ. 95.

- Επέκταση της τεχνικής εμπειρογνωμοσύνης των αστυνομικών και διαρκής κατάρτιση και εκπαίδευση του προσωπικού.

- Προσαρμογή των νομικών μέσων και επέκταση των ευκαιριών συνεργασίας στο πλαίσιο της διεθνούς νομικής συνδρομής.

- Ανάπτυξη νέων μεθόδων έρευνας και διατήρησης αποδεικτικών στοιχείων με βάση τις ανάγκες, συμπεριλαμβανομένων ειδικών επιλογών για την αξιολόγηση μαζικών δεδομένων.

- Ενίσχυση της εθνικής και διεθνούς συνεργασίας.

- Συνεργασία με ειδικούς από επιχειρήσεις, εταιρείες έρευνας, επιστήμης και τηλεπικοινωνιών για την ανάπτυξη αρχών ασφαλείας.

- Ολοκληρωμένη προστασία των πληροφορικών υποδομών των αρχών ασφαλείας και προστασία ευαίσθητων δεδομένων.

- Διασφάλιση μιας ασφαλούς ψηφιακής ταυτότητας.

- Μείωση των ευκαιριών για ποινικά αδικήματα μέσω της τεχνικής ασφάλειας των διαδρομών μετάδοσης.

- Πρόληψη μέσω ευαισθητοποίησης, ενημέρωσης και προειδοποίησης των πολιτών, φορέων και οργανισμών.

Αυτές οι παράμετροι και στόχοι αποτελούν τμήμα της προσπάθειας για τη δημιουργία ενός διεθνούς πλαισίου που να διευκολύνει την αποτελεσματική αντιμετώπιση των κυβερνοεγκλημάτων και τη διασφάλιση της ασφάλειας του ψηφιακού χώρου.

Το ηλεκτρονικό έγκλημα είναι, πράγματι, διεθνές και απαιτεί στενή συνεργασία σε διεθνές επίπεδο για την αποτελεσματική αντιμετώπισή του. Η Europol και η Interpol αναλαμβάνουν καίριο ρόλο σε αυτόν τον τομέα και έχουν θέσει σε εφαρμογή συντονισμένες προσεγγίσεις για τον σκοπό αυτό επιδιώκοντας μια συνολική, συντονισμένη και συνεργατική προσέγγιση για την καταπολέμηση του ηλεκτρονικού εγκλήματος, με τη συμμετοχή δημοσίων και ιδιωτικών φορέων. Για το σκοπό αυτό, ιδρύθηκαν το Ευρωπαϊκό Κέντρο για το

Έγκλημα στον Κυβερνοχώρο (European Cybercrime Centre - EC3) και το Κέντρο Ψηφιακού Εγκλήματος της Interpol (Interpol Digital Crime Centre - IDCC).

Το Ευρωπαϊκό Κέντρο για Εγκλήματα στον Κυβερνοχώρο (EC3)[80] με έδρα τη Χάγη αποτελεί σημαντική πρωτοβουλία της Ευρωπαϊκής Επιτροπής για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και ιδρύθηκε, κατόπιν ανάθεσης, από την Europol. Στόχος του EC3 είναι να υποστηρίξει τα κράτη μέλη της Ευρωπαϊκής Ένωσης στην καταπολέμηση διάφορων μορφών κυβερνοεγκλημάτων, συμπεριλαμβανομένων των επιθέσεων από βασικούς χάκερ, της διαδικτυακής απάτης, της σεξουαλικής κακοποίησης παιδιών, και της απάτης με πιστωτικές κάρτες. Ένα από τα κύρια χαρακτηριστικά του είναι η εξουσιοδότησή του να επικεντρωθεί σε εγκλήματα που έχουν τη δυνατότητα να προκαλέσουν σοβαρή ζημία στα θύματά τους ή να επηρεάσουν κρίσιμες υποδομές και πληροφοριακά συστήματα στην Ευρωπαϊκή Ένωση. Το EC3 δρα σε συνεργασία με αρχές επιβολής του νόμου, ερευνητικά εργαστήρια, πανεπιστήμια και άλλους εταίρους για να αντιμετωπίσει την απειλή του κυβερνοεγκλήματος σε ευρωπαϊκό επίπεδο.

Το Κέντρο Ψηφιακού Εγκλήματος της Interpol (IDCC) εδρεύει στη Σιγκαπούρη, στις εγκαταστάσεις της Interpol Global Complex for Innovation (IGCI) και λειτουργεί ως ερευνητική και αναπτυξιακή μονάδα για την ταυτοποίηση εγκλημάτων και εγκληματών, εκπαίδευση, επιχειρησιακή υποστήριξη και συνεργασίες στον τομέα της κυβερνοασφάλειας, συμπληρώνοντας τη Γενική Γραμματεία της Interpol στη Λυών και ενισχύοντας την παρουσία του οργανισμού στην Ασία[81].

Η συνεργασία μεταξύ αυτών των δύο οργανισμών είναι κρίσιμη για τη διασφάλιση της διεθνούς ασφάλειας στον κυβερνοχώρο, καθώς καλύπτουν διάφορες γεωγραφικές περιοχές και προσφέρουν σημαντικές εργαλειοθήκες και εμπειρογνωμοσύνη για την αντιμετώπιση των κυβερνοεγκλημάτων. Η ενίσχυση της παγκόσμιας συνεργασίας σε αυτόν τον τομέα είναι αναγκαία για την αποτελεσματική προστασία των δικτύων και των πολιτών από τις κυβερνοαπειλές.

Επιπροσθέτως, η συνεργασία μεταξύ υφιστάμενων και νέων συνεργατών είναι κρίσιμη για την επιτυχία των προσπαθειών καταπολέμησης του εγκλήματος στον κυβερνοχώρο. Η Europol, το Ευρωπαϊκό Κέντρο για Εγκλήματα στον Κυβερνοχώρο (EC3)

[80] Ευρωπαϊκή Επιτροπή (2014), https://ec.europa.eu/commission/presscorner/detail/el/IP_14_129.
[81] Interpol (2014), https://www.interpol.int/News-and-Events/News/2014/INTERPOL-coordinated-operation-strikes-back-at-sextortion-networks.

και άλλοι εθνικοί και διεθνείς οργανισμοί συνεργάζονται ενεργά με ιδιωτικούς και δημόσιους φορείς για να αντιμετωπίσουν τις κυβερνοαπειλές. Επίσης, η συνεργασία με διεθνείς τεχνολογικές εταιρείες όπως το Facebook, η Google, η Microsoft, το Twitter, η Symantec, η Trend Micro, η McAfee, καθώς και με τον μη κερδοσκοπικό οργανισμό International Cyber Security Protection Alliance (ICSPA), είναι ουσιώδης για την καταπολέμηση των κυβερνοεγκλημάτων. Με τον τρόπο αυτό επιτρέπεται η ανταλλαγή πληροφοριών, την ανάπτυξη κοινών προγραμμάτων, και την ανάληψη συλλογικών δράσεων για την αντιμετώπιση των κυβερνοαπειλών. Τέλος, επιτυχημένα παραδείγματα συνεργασίας μεταξύ διαφόρων ενδιαφερομένων φορέων, όπως το παράδειγμα με τη Microsoft, το FBI, το EC3 και ορισμένους ιδιωτικούς οργανισμούς για τη διακοπή του botnet ZeroAccess, αποδεικνύουν τη σημασία της ομαδικής προσπάθειας στην καταπολέμηση του κυβερνοεγκλήματος και την ανάγκη για συνεχή συνεργασία μεταξύ των διαφόρων φορέων[82].

Ο Ευρωπαϊκός Μήνας Κυβερνοασφάλειας (European Cybersecurity Month - ECSM) αποτελεί μια σημαντική πρωτοβουλία που συνεισφέρει στην ευαισθητοποίηση των πολιτών και των οργανισμών σχετικά με την ασφαλή και υπεύθυνη χρήση του κυβερνοχώρου. Η πρωτοβουλία αυτή ξεκίνησε ως πιλοτικό έργο με την υποστήριξη του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (European Union Agency for Cybersecurity - ENISA) και της Ευρωπαϊκής Επιτροπής και στη συνέχεια εξελίχθηκε σε μια τακτική πανευρωπαϊκή εκστρατεία που συμμετέχουν πολλές χώρες σε όλη την Ευρώπη. Ο ECSM διοργανώνεται κάθε χρόνο τον Οκτώβριο και περιλαμβάνει εκδηλώσεις, εκστρατείες ευαισθητοποίησης, και δράσεις που στοχεύουν στην ενημέρωση του κοινού σχετικά με θέματα κυβερνοασφάλειας. Συμμετέχουν τόσο δημόσιοι οργανισμοί όσο και ιδιωτικοί φορείς, και οι εκστρατείες ποικίλλουν ανάλογα με τον τομέα και το κοινό που στοχεύουν. Η πρωτοβουλία αυτή συμβάλλει σημαντικά στην αυξημένη ευαισθητοποίηση και ενημέρωση του κοινού για τους κυβερνοασφαλειακούς κινδύνους και τις βέλτιστες πρακτικές για την προστασία των διαδικτυακών δραστηριοτήτων[83].

Στη σύνοδο κορυφής του ΝΑΤΟ στη Λισαβόνα τον Νοέμβριο του 2010, η συμμαχία αποφάσισε να συμπεριλάβει τις διαδικτυακές επιθέσεις σε στρατηγικά δίκτυα στις νέες απειλές και να ενισχύσει τη δυνατότητά της να αντιμετωπίζει τέτοιες απειλές. Αυτό οδήγησε στη διεξαγωγή του εικονικού ελιγμού *"Cyber Coalition 2010",* όπου προσκλήθηκαν όλοι οι εταίροι της συμμαχίας για να δοκιμάσουν και να αξιολογήσουν τη συνεργασία και την

[82] Wernert M. (2021), σελ. 98.
[83] Wernert M. (2021), σελ. 93.

ικανότητά τους στον τομέα της κυβερνοασφάλειας. [84]Κατά τη διάρκεια αυτού του ελιγμού, το ΝΑΤΟ πραγματοποίησε πολλαπλές ταυτόχρονες διαδικτυακές επιθέσεις στον κυβερνοχώρο των κρατών μελών της συμμαχίας. Σκοπός αυτών των επιθέσεων ήταν να δοκιμάσουν την αποτελεσματικότητα της συνεργασίας μεταξύ των αρχών, των ειδικών μονάδων και να προσομοιώσουν στρατηγικές διαδικασίες λήψης αποφάσεων σε περίπτωση κυβερνοασφάλειας. Παράλληλα, πολλοί φορείς, συμπεριλαμβανομένων αρχών, εταιρειών και ενώσεων, παρείχαν πληροφορίες και συμβουλές σχετικά με την ασφάλεια των υπολογιστών, την προστασία από ακατάλληλο περιεχόμενο και άλλα θέματα κυβερνοασφάλειας. Οι πηγές αυτές παρουσιάζονται στο παράρτημα για περαιτέρω ανάγνωση και πληροφόρηση.

Το πεδίο της ψηφιακής ασφάλειας αποτελεί κρίσιμη πτυχή στον αγώνα ενάντια στο ηλεκτρονικό έγκλημα και στην προστασία του κυβερνοχώρου. Η δημιουργία ενός εγκληματολογικού εργαστηρίου για την υποστήριξη ψηφιακών αξιολογήσεων, η έρευνα για τη δοκιμή πρωτοκόλλων, εργαλείων και υπηρεσιών, καθώς και η ανάλυση των τάσεων επιθέσεων στον κυβερνοχώρο είναι ζωτικής σημασίας. Αυτές οι δραστηριότητες συμβάλλουν στην ανάπτυξη και εφαρμογή πρακτικών λύσεων που βελτιώνουν την ασφάλεια στο διαδίκτυο και προστατεύουν τόσο τα άτομα όσο και τα συστήματα και τις δομές πληροφορικής από κυβερνοαπειλές. Η διακρατική συνεργασία μεταξύ αστυνομικών αρχών, ερευνητικών εργαστηρίων, πανεπιστημίων και δημόσιου και ιδιωτικού τομέα είναι απαραίτητη για την επίτευξη αυτών των στόχων. Η διακυβέρνηση της ασφάλειας στο διαδίκτυο είναι ένα σημαντικό θέμα, καθώς πρέπει να διασφαλιστεί ότι υπάρχουν αποτελεσματικοί μηχανισμοί και πρακτικές για την προστασία των ψηφιακών περιουσιών και των δεδομένων. Η συνεχής έρευνα, ανάπτυξη και συνεργασία είναι απαραίτητες για να ανταποκριθούμε στην αυξανόμενη πολυπλοκότητα των κυβερνοαπειλών και να διασφαλιστεί την ασφάλεια στον ψηφιακό κόσμο.

4.9 Το διαδίκτυο ως μέσο έρευνας

Το διαδίκτυο αποτελεί μια ιδανική πλατφόρμα για την πρόσβαση σε πληροφορίες και γνώση από όλον τον κόσμο. Οι μηχανές αναζήτησης όπως το Google, το Bing, το Yahoo και άλλες, καθιστούν δυνατή την εύκολη και ελεύθερη πρόσβαση σε πληροφορίες απλώς εισάγοντας λέξεις-κλειδιά ή φράσεις στο πεδίο αναζήτησης. Τα αποτελέσματα αναζήτησης προέρχονται από την ενδεχόμενα ανεξάρτητη διαδικτυακή βάση δεδομένων και παρέχουν

[84] ο.π.: Wernert M. (2021).

πληροφορίες, ιστοσελίδες, εικόνες, βίντεο και άλλο περιεχόμενο που σχετίζεται με το ερώτημα του χρήστη. Αξίζει να σημειωθεί, ότι η ακρίβεια και η συναισθηματική αξιολόγηση των πληροφοριών που παρέχονται μέσω των μηχανών αναζήτησης μπορεί να ποικίλει, και είναι σημαντικό υπάρχει κριτική σκέψη όταν αναζητούνται πληροφορίες.

Ακόμα τα Metasearch Engines είναι εργαλεία που συγκεντρώνουν αποτελέσματα από πολλές διαφορετικές μηχανές αναζήτησης ταυτόχρονα. Αυτό κάνει τη διαδικασία αναζήτησης πιο αποδοτική και επιτρέπει στους χρήστες να προβάλουν αποτελέσματα από πολλές πηγές σε μια μόνο διεπαφή. Αυτό είναι χρήσιμο για ανθρώπους που θέλουν να εντοπίσουν πληροφορίες από διάφορες πηγές χωρίς να χρειάζεται να επισκεφτούν κάθε μηχανή αναζήτησης ξεχωριστά. Ωστόσο, είναι σημαντικό να ελέγχεται η αξιοπιστία των πληροφοριών και να επαληθεύονται οι πληροφορίες από αξιόπιστες πηγές.

Για παράδειγμα, οι ιστοσελίδες αναζήτησης ατόμων, όπως το www.123people.com και το www.yasni.de, συλλέγουν πληροφορίες σχετικά με μεμονωμένα άτομα από τον Ιστό, συμπεριλαμβανομένων κειμένων, φωτογραφιών και βίντεο, καταχωρήσεων τηλεφωνικού καταλόγου και προφίλ από κοινωνικά δίκτυα. Ο ιστότοπος http://web.archive.org λειτουργεί ως αρχείο ιστού και διατηρεί πληροφορίες για διευθύνσεις διαδικτύου που ίσως δεν είναι πλέον διαθέσιμες στον Ιστό. Το Street View και το Google Earth είναι εργαλεία που μπορούν να χρησιμοποιηθούν για την προετοιμασία αποστολής και την αναγνώριση αντικειμένων σε διάφορες τοποθεσίες.

Ωστόσο, για την επαγγελματική αντιμετώπιση του εγκλήματος, απαιτείται η χρήση πιο σύγχρονων τεχνικών στον τομέα της τεχνολογίας επιτήρησης και βιντεοεπιτήρησης. Η τεχνολογία ψηφιακής καταγραφής και μετάδοσης προσφέρει πλείστες δυνατότητες για αστυνομικές επιχειρήσεις. Ο ιστότοπος www.tineye.com συνδράμει στον εντοπισμό ατόμων που συνδέονται με περιστατικά στα οποία εμπλέκεται η αστυνομία, οδηγίες για τον εντοπισμό της προέλευσης ενός αριθμού τηλεφώνου αναφέρονται στον ιστότοπο www.fonefinder.net. Επίσης, ο όρος OSINT αναφέρεται στη *“Νοημοσύνη ανοιχτού κώδικα (Open-source intelligence)”*, προερχόμενος από την στρατιωτική πρακτική της παρακολούθησης πληροφοριών από δημόσια προσβάσιμες πηγές. Για τις αστυνομικές αρχές, αυτός αφορά επίσης την αξιολόγηση προσβάσιμων πηγών πληροφοριών που σχετίζονται με μια υπόθεση, ενώ ο ιστότοπος https://osintframework.com παρέχει πληροφορίες για ιστότοπους και εργαλεία που μπορούν να χρησιμοποιηθούν για την ενίσχυση της έρευνας.

Η δημιουργία κοινωνικών δικτύων πρέπει να εξεταστεί πιο προσεκτικά με σκοπό να αξιολογηθεί η προστιθέμενη αξία αυτών των πλατφορμών από αστυνομική άποψη. Δεδομένης της διαρκούς αύξησης της χρήσης των μέσων κοινωνικής δικτύωσης από τους νέους, μπορεί να προβλεφθεί ότι οι έρευνες στα κοινωνικά δίκτυα θα μπορούσαν να γίνουν ένα ασφαλές και αποτελεσματικό εργαλείο αστυνομικών ερευνών στο προσεχές μέλλον.

4.9.1 Προσδιορισμός της διεύθυνσης IP

Ένα ιδιαίτερο μέσο που μπορεί να βοηθήσει στην έρευνα αποτελεί η διεύθυνση IP. Η συντομογραφία *"IP"* αναφέρεται στη διεύθυνση IP (Internet Protocol), που είναι ένα μοναδικό αριθμητικό αναγνωριστικό που ανατίθεται σε κάθε συσκευή που συνδέεται στο διαδίκτυο ή σε ένα δίκτυο της IP. Οι διευθύνσεις IP χρησιμοποιούνται για να αναγνωρίσουν και να επικοινωνήσουν με συσκευές σε μια δικτυακή υποδομή. Υπάρχουν δύο κύριες εκδόσεις της διεύθυνσης IP:

A. IPv4 (Internet Protocol version 4): Είναι το πιο διαδεδομένο πρωτόκολλο διεύθυνσης IP και αποτελείται από μια σειρά αριθμών, όπως *"194.157.1.1"*. Το IPv4 χρησιμοποιείται παγκοσμίως, αλλά η περιορισμένη ποσότητα διαθέσιμων διευθύνσεων IP έχει οδηγήσει στην ανάπτυξη του IPv6.

B. IPv6 (Internet Protocol version 6): Είναι η επόμενη γενιά του πρωτοκόλλου διεύθυνσης IP και χαρακτηρίζεται από πολύ μεγαλύτερες διευθύνσεις, που περιέχουν ακόμη περισσότερους χαρακτήρες από το IPv4, όπως *"2001:0cd8:76f3:0000:0000:8a2e:0410:7224"*. Ο στόχος του IPv6 είναι να αντικαταστήσει σταδιακά το IPv4 και να προσφέρει αρκετά περισσότερες διευθύνσεις IP για τη συνεχή ανάπτυξη του διαδικτύου.

Οι διευθύνσεις IP είναι κρίσιμες για τη λειτουργία του διαδικτύου, καθώς επιτρέπουν την προσδιορισμό και την επικοινωνία μεταξύ συσκευών. Κάθε διεύθυνση IP εκχωρείται μόνο μία φορά στο παγκόσμιο δίκτυο. Για την ευκολότερη απομνημόνευσή τους, αντικαθίστανται με αλφαριθμητικούς χαρακτήρες. Όταν επισκέπτεται ένας χρήστης το διαδίκτυο, αυτές οι διευθύνσεις μετακινούνται αυτόματα στο παρασκήνιο χρησιμοποιώντας ένα *"Σύστημα Ονομάτων Τομέα (Domain Name System - DNS)"*[85].

[85] Ford M., Boucadair M., Durand A., Levis P., Roberts P. (2011), https://www.rfc-editor.org/rfc/rfc6269.html.

Η μετάβαση από το πρότυπο IPv4 στο IPv6 είναι ένα σημαντικό βήμα προς τη διασφάλιση ότι θα υπάρχουν επαρκείς διευθύνσεις IP για τη συνεχή ανάπτυξη του διαδικτύου και τη σύνδεση όλο και περισσότερων συσκευών. Ο αριθμός των διευθύνσεων που προσφέρει το IPv6 είναι πραγματικά εντυπωσιακός και υπερβαίνει κατά πολύ τον αριθμό των διευθύνσεων που προσφέρει το IPv4. Η μετάβαση στο IPv6 προχωρά σε διάφορες φάσεις και απαιτεί συνεργασία από πολλούς φορείς, συμπεριλαμβανομένων των ιστότοπων, των παρόχων υπηρεσιών Internet (ISPs) και άλλων παραγόντων του διαδικτύου. Στη διάρκεια αυτής της μετάβασης, τόσο το IPv4 όσο και το IPv6 θα υπάρχουν παράλληλα, και η αναγνώριση των διευθύνσεων IP που χρησιμοποιούνται σε κάθε περίπτωση θα γίνεται αυτόματα. Με τον καιρό, αναμένεται ότι το IPv6 θα κυριαρχήσει καθώς οι διευθύνσεις IPv4 εξαντλούνται και οι νέες συσκευές και υπηρεσίες θα υιοθετούν αποκλειστικά το IPv6.

Ο Κανονισμός που περιγράφεται παραπάνω αναφέρεται στον τρόπο με τον οποίο οι πάροχοι υπηρεσιών διαδικτύου (ISPs) διαχειρίζονται τις διευθύνσεις IP που αναθέτουν στους πελάτες τους. Η πρακτική της εκχώρησης δυναμικών διευθύνσεων IP είναι κοινή και συμβάλλει στη βέλτιστη χρήση των διευθύνσεων IP, καθώς οι διευθύνσεις δεν δεσμεύονται μόνιμα από έναν συγκεκριμένο χρήστη. Οι ISPs διατηρούν καταγραφές των διευθύνσεων IP που εκχωρούνται σε κάθε σύνδεση για λόγους χρέωσης και διαχείρισης του δικτύου. Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για να προσδιοριστεί ποιος πελάτης χρησιμοποίησε μια συγκεκριμένη διεύθυνση IP σε μια συγκεκριμένη χρονική στιγμή. Αυτή η πληροφορία μπορεί να είναι χρήσιμη σε περιπτώσεις εγκληματικής δραστηριότητας ή για να αποκαλυφθεί η πηγή ενός συγκεκριμένου δικτυακού επεισοδίου[86]. Είναι σημαντικό το γεγονός ότι η προστασία της ιδιωτικότητας και η τήρηση των νόμων περί προστασίας δεδομένων είναι θεμελιώδεις πτυχές στη χρήση αυτών των πληροφοριών.

Στην Ελλάδα, υπάρχουν νομοθετικές ρυθμίσεις που αφορούν τη διατήρηση δεδομένων επικοινωνίας από τους παρόχους υπηρεσιών διαδικτύου. Οι ρυθμίσεις αυτές είναι συμμορφωμένες με την Ευρωπαϊκή Ένωση και περιλαμβάνουν τις απαιτήσεις 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. Σύμφωνα με τον Ν. 4577/2018, οι πάροχοι υπηρεσιών διαδικτύου υποχρεούνται να διατηρούν δεδομένα επικοινωνίας για συγκεκριμένη περίοδο, αλλά αυτή η περίοδος διαφέρει ανάλογα με τον τύπο των δεδομένων. Για παράδειγμα, οι

[86] ο.π.: Ford M., Boucadair M., Durand A., Levis P., Roberts P. (2011).

πληροφορίες κίνησης (όπως η διεύθυνση IP και οι χρόνοι σύνδεσης) διατηρούνται για έναν συγκεκριμένο χρόνο. Επίσης, το ελληνικό νομικό πλαίσιο συμπεριλαμβάνει προστατευτικά μέτρα για την ιδιωτικότητα των πολιτών και περιορίζει την πρόσβαση σε αυτά τα δεδομένα με σαφείς κανόνες και διαδικασίες. Η πρόσβαση σε αυτά τα δεδομένα συνήθως πρέπει να γίνεται με απόφαση δικαστηρίου και με σεβασμό προς την νομική διαδικασία.

Στην Γερμανία σύμφωνα με τον κανονισμό για τη διατήρηση δεδομένων επικοινωνίας από τους παρόχους υπηρεσιών διαδικτύου, οι πάροχοι ήταν αρχικά υποχρεωμένοι να αποθηκεύουν τα δεδομένα επικοινωνίας για έξι μήνες και να παρέχουν πρόσβαση στις διωκτικές αρχές κατόπιν αιτήματος. Ωστόσο, αυτή η πρακτική αντικρίσθηκε με κριτική σχετικά με την προστασία της ιδιωτικής ζωής και την πιθανότητα κατάχρησης των δεδομένων. Με την απόφαση του Ομοσπονδιακού Συνταγματικού Δικαστηρίου για τη διατήρηση δεδομένων της 02.03.2010, θεσπίστηκε νέος νόμος Τηλεπικοινωνιών (Telekommunikationsgesetz - TKG), ο οποίος τέθηκε σε ισχύ στις 18 Δεκεμβρίου 2015 και σύμφωνα με τον οποίο ο χρόνος διατήρησης των δεδομένων περιορίζεται με στόχο την ιδιωτικότητα των πολιτών. Πιο συγκεκριμένα, σύμφωνα με το άρθρο 113b TKG, οι πάροχοι υπηρεσιών πρέπει να αποθηκεύουν τα δεδομένα κίνησης των πελατών τους για δέκα εβδομάδες, ενώ τα δεδομένα τοποθεσίας πρέπει να διατηρούνται για ένα μήνα. Αυτές οι περίοδοι διατήρησης είναι σημαντικά μικρότερες από τις προηγούμενες. Επίσης, η Ομοσπονδιακή Υπηρεσία Δικτύων επιβλέπει την εφαρμογή των διατάξεων του νόμου και εκδίδει εντολές και μέτρα για την τήρηση του νόμου.

Οι διευθύνσεις IP, οι οποίες εκχωρούνται παγκοσμίως από τις ΗΠΑ και διαχειρίζονται μέσω βάσεων δεδομένων που βρίσκονται σε διάφορες ηπείρους, όπως η ευρωπαϊκή βάση δεδομένων RIPE. Η κατοχή μιας διεύθυνσης IP συνιστά το ψηφιακό στίγμα της σύνδεσης στο διαδίκτυο. Σε περίπτωση που η αναζήτηση στη βάση δεδομένων της RIPE δεν παρέχει ικανοποιητικά αποτελέσματα, απαιτείται διεθνές αίτημα για περαιτέρω παρακολούθηση. Μετά την επιβεβαίωση της εγγραφής, το αποτέλεσμα περιλαμβάνει το όνομα του παρόχου της σύνδεσης. Βάσει της χρονικής σήμανσης που καθορίζεται στην κεφαλίδα, είναι δυνατό να ανιχνευθεί ποια σύνδεση είχε ανατεθεί στην εν λόγω διεύθυνση IP.

Τέλος, ο κάτοχος του δρομολογητή που χρησιμοποιείται μπορεί να ανιχνευθεί μέσω της δημόσιας διεύθυνσης IP. Ωστόσο, για να δυσκολέψει αυτή την διαδικασία, ο χρήστης έχει πολλές επιλογές για να κρύψει τη δημόσια διεύθυνση IP. Ένας τρόπος για να το πετύχει είναι να χρησιμοποιήσει έναν ενδιάμεσο σταθμό μεταξύ του παρόχου διαδικτύου του και του

προορισμού των αιτημάτων του, μέσω του οποίου δρομολογούνται τα πακέτα δεδομένων. Στον αυτόν τον ενδιάμεσο σταθμό, η δημόσια διεύθυνση IP ανταλλάσσεται με τη δημόσια διεύθυνση IP του ενδιάμεσου σταθμού, που ονομάζεται ανώνυμος διακομιστής μεσολάβησης.

Συνεπώς, καθίσταται σαφές ότι οι διευθύνσεις IP αποτελούν ένα σημαντικό μέσο έρευνας στον κυβερνοχώρο και στον τομέα του διαδικτύου. Γενικότερα, λοιπόν, χρησιμοποιούνται για τον ανιχνευτικό και τον δρομολογητικό ρόλο του διαδικτύου, και μπορούν να παρέχουν πολλές πληροφορίες κατά τη διερεύνηση διαδικτυακών προβλημάτων ή εγκλημάτων, εφόσον υπάρχουν τα κατάλληλα μέσα, εργαλεία και γνώσεις.

4.9.2 Έρευνες Domain

Ένα ακόμα σημαντικό εργαλείο έρευνας είναι η έρευνα domain (domain research), η οποία αναφέρεται στην διαδικασία ανάλυσης και εξαγωγής πληροφοριών σχετικά με ένα συγκεκριμένο τομέα (domain) στο διαδίκτυο. Ένας τομέας αντιπροσωπεύει την ηλεκτρονική ταυτότητα ενός ιστότοπου ή μιας ιστοσελίδας και περιέχει πληροφορίες όπως το όνομα του ιστότοπου (π.χ., www.example.com), την διεύθυνση IP που συσχετίζεται με αυτόν τον τομέα, και πληροφορίες σχετικά με τον καταχωρητή (domain registrar) και τον κάτοχο του τομέα. Η έρευνα domain είναι σημαντική για πολλούς σκοπούς, συμπεριλαμβανομένης της ανίχνευσης πληροφοριών σχετικά με την ασφάλεια, την ανταγωνιστική ανάλυση, την εξάρτηση του τομέα, και άλλους σχετικούς τομείς. Οι χαρακτήρες *“www.”* αναφέρονται στον Παγκόσμιο Ιστό, οι τελευταίοι χαρακτήρες *“.com”* είναι ο κωδικός χώρας ή το διακριτικό του σκοπού (για παράδειγμα, το *".gr"* είναι ο κωδικός χώρας για την Ελλάδα και το *“.de”* για τη Γερμανία, το *".com"* σημαίνει εμπορικό, το *".org"* μη κερδοσκοπικό και το *".edu"* εκπαιδευτικό ίδρυμα) και το κεντρικό όνομα *“example”* αντιπροσωπεύει τον τομέα[87].

Η έρευνα domain μπορεί να περιλαμβάνει τα ακόλουθα στοιχεία:

- Πληροφορίες WHOIS: Η έρευνα αυτή συχνά αρχίζει με την αναζήτηση των πληροφοριών WHOIS, οι οποίες παρέχουν πληροφορίες σχετικά με τον καταχωρητή του τομέα, τον κάτοχο, την διεύθυνση επικοινωνίας, και την ημερομηνία λήξης της κατοχής.

- Διεύθυνση IP: Η αντιστοίχιση του domain με μια διεύθυνση IP μπορεί να αποκαλύψει ποιος φιλοξενεί τον ιστότοπο και την φυσική του τοποθεσία.

[87] Satoh, A.; Fukuda, Y.; Kitagata, G.; Nakamura (2021).

- Ιστορικό τομέα: Η έρευνα domain μπορεί να περιλαμβάνει την ανάκτηση ιστορικών πληροφοριών σχετικά με τον τομέα, όπως προηγούμενοι καταχωρητές, αλλαγές στις διευθύνσεις IP, και αλλαγές ιδιοκτησίας.

- Ανάλυση DNS: Μπορεί να περιλαμβάνει την ανάλυση του Domain Name System (DNS) για τον τομέα, που παρέχει πληροφορίες σχετικά με τις διαφορετικές υπηρεσίες που σχετίζονται με αυτόν, όπως τα υπο-τομέα, τα MX (Mail Exchange) records για το email, και άλλα.

Το ICANN (Internet Corporation for Assigned Names and Numbers) αποφάσισε το 2011 να διευρύνει τον χώρο των διευθύνσεων στο διαδίκτυο. Αυτή η απόφαση επέτρεψε τη χρήση σχεδόν οποιασδήποτε λέξης ως Top-Level Domains (TLDs), δηλαδή τον τομέα ανωτάτου επιπέδου σε μια διεύθυνση ιστού. Εκτός από τις παραδοσιακές διευθύνσεις όπως τα *".com"* ή *".net"* προστέθηκαν γενικοί όροι TLD όπως *".auto"* ή *".travel"* (gTLD). Οι πρώτες από αυτές τις νέες επεκτάσεις τομέα ήταν διαθέσιμες από τις αρχές του 2014. Αυτοί οι νέοι gTLD περιλαμβάνουν παραδείγματα όπως *".shop", ".love", ".email"* και *".bayern"* προσφέροντας περισσότερες επιλογές στους κατόχους ιστοσελίδων για την επιλογή μιας διεύθυνσης που ανταποκρίνεται καλύτερα στο περιεχόμενο ή τον σκοπό τους[88].

Οι τομείς καταγράφονται κεντρικά στη βάση δεδομένων *"Whois."* Για κάθε ιστότοπο, πρέπει να υπάρχει ένα υπεύθυνο άτομο, γνωστό ως κάτοχος του τομέα (Admin-C), που είναι εγγεγραμμένο στην αντίστοιχη καταχώρηση. Είναι σημαντικό να σημειωθεί ότι τα δεδομένα διεύθυνσης του κατόχου του τομέα μπορεί να είναι λανθασμένα ή μη επικαιροποιημένα σε ορισμένες περιπτώσεις. Σε αυτές τις περιπτώσεις, μπορεί να απαιτηθούν περαιτέρω έρευνες και επικοινωνία με τον υπεύθυνο γραμματέα του τομέα για να διορθωθούν τα δεδομένα. Αναζήτηση τομέων μπορεί να γίνει μέσω του ιστότοπου https://www.whois.com/whois/checkdomain.com.

Με πολλές υπηρεσίες ερωτημάτων, προβάλλονται μόνο τα τρέχοντα δεδομένα Whois για έναν τομέα. Εύρεση πληροφοριών σχετικά με προηγούμενους ιδιοκτήτες ή σχετικά με όλες τις αλλαγές από την εγγραφή ενός ιστότοπου, υπάρχει η δυνατότητα έρευνας στη διεύθυνση www.who.is. Κατά τη χρήση αυτού του ιστότοπου, απαιτείται η εισαγωγή του ονόματος τομέα, της διεύθυνση URL ή της διεύθυνση IP, και παρουσιάζονται πληροφορίες σχετικά με την τοποθεσία του διακομιστή web σε έναν χάρτη, καθώς και πληροφορίες σχετικά με το ιστορικό εγγραφής του τομέα.

[88] Wernert M. (2021), σελ. 140.

Επομένως, οι έρευνες domain αποτελούν ένα κρίσιμο εργαλείο για την καταπολέμηση του ηλεκτρονικού εγκλήματος. Η παρακολούθηση των domain και η ανάλυση των πληροφοριών σχετικά με αυτά μπορεί να χρησιμοποιηθεί για να εντοπιστούν δραστηριότητες που σχετίζονται με απάτες, αναξιόπιστους ιστοτόπους, κλοπή ψηφιακών ταυτοτήτων, και άλλες μορφές ηλεκτρονικού εγκλήματος.

5. Ηλεκτρονικά εγκλήματα στην πράξη

5.1 Κλοπή ψηφιακών ταυτοτήτων

5.1.1 Γενικές Πληροφορίες

Η ψηφιακή ταυτότητα αναφέρεται στον ψηφιακό αναπαραστατικό χαρακτήρα μιας πραγματικής ή εικονικής οντότητας, όπως ένα άτομο, μια επιχείρηση, μια οργάνωση ή ακόμη και ένα αντικείμενο, μέσα στον κόσμο του διαδικτύου και των ψηφιακών υπηρεσιών. Περιλαμβάνει τις πληροφορίες, τις δραστηριότητες και τα ίχνη που αφήνει ο χρήστης κατά την πλοήγησή του στο διαδίκτυο. Αποτελείται από διάφορα στοιχεία, όπως πληροφορίες προσωπικού χαρακτήρα (όπως ονοματεπώνυμο, ηλεκτρονική διεύθυνση, τηλέφωνο), προφίλ σε κοινωνικά δίκτυα, δημοσιεύσεις σε ιστολόγια, σχόλια, αξιολογήσεις, αγορές προϊόντων και υπηρεσιών, καθώς και άλλες δραστηριότητες που αφορούν την παρουσία της οντότητας στον ψηφιακό κόσμο.

Πιο αναλυτικά αφορά όλους τους τύπους λογαριασμών χρηστών:

➔ Λογαριασμοί σε εφαρμογές πώλησης προϊόντων-υπηρεσιών, δηλαδή πλατφόρμες ηλεκτρονικού εμπορίου (ταξιδιωτικές, ενοικίασης ή αγοράς οχημάτων και πλατφόρμες όπως το eBay και το Amazon).

➔ Λογαριασμοί σε μέσα κοινωνικής δικτύωσης, για παράδειγμα facebook, youtube.

➔ Λογαριασμοί ηλεκτρονικού ταχυδρομείου και υπηρεσιών ανταλλαγής μηνυμάτων.

➔ Τραπεζικοί λογαριασμοί και χαρτοφυλάκια μετοχών (ηλεκτρονικές τραπεζικές συναλλαγές και διαδικτυακή μεσιτεία).

➔ Λογαριασμοί μαθητών και φοιτητών στην πλατφόρμα του εκάστοτε εκπαιδευτικού ιδρύματος και τα κλειδιά για την ασφαλή σύνδεση σε σελίδες με απομακρυσμένους πόρους (π.χ. εσωτερικά πανεπιστημιακά δίκτυα).

➔ Λογαριασμοί σε εφαρμογές ηλεκτρονικής διακυβέρνησης (π.χ. ηλεκτρονικές φορολογικές δηλώσεις).

➔ Λογαριασμοί Cloud Computing.

➔ Πληροφορίες που σχετίζονται με πληρωμές (ιδίως δεδομένα πιστωτικών καρτών, συμπεριλαμβανομένων των διευθύνσεων πληρωμής και άλλων πληροφοριών).

Η κλοπή ψηφιακών ταυτοτήτων, γνωστή και ως ταυτοποίηση ή απάτη στο διαδίκτυο, αναφέρεται στη διαδικασία κακόβουλων ατόμων ή οργανώσεων να αποκτήσουν παράνομη πρόσβαση σε προσωπικές πληροφορίες και δεδομένα των ψηφιακών ταυτοτήτων άλλων ατόμων ή εταιρειών. Ο στόχος τους είναι συνήθως να εκμεταλλευτούν αυτές τις πληροφορίες για οικονομικό όφελος ή για πραγματοποίηση ανεπιθύμητων δραστηριοτήτων. Επιπλέον από την παραπάνω καθίσταται σαφές ότι ο όρος *"κλοπή ψηφιακής ταυτότητας"* καλύπτει ένα πολύ ευρύ πεδίο πρακτικών, καθώς οι δράστες μπορούν να χρησιμοποιήσουν πλήθος μεθόδων για να κλέψουν ψηφιακές ταυτότητες. Ενδεικτικά αναφέρονται οι εξής:

- Phishing: Οι απατεώνες αποστέλλουν ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα κειμένου ή διαδικτυακές σελίδες που μοιάζουν με νόμιμες πηγές (όπως τράπεζες, κοινωνικά δίκτυα), προσπαθώντας να πείσουν τα θύματα να αποκαλύψουν τα προσωπικά τους δεδομένα.

- Κακόβουλο λογισμικό (Malware): Οι απατεώνες μπορούν να χρησιμοποιήσουν κακόβουλο λογισμικό, όπως ιούς, δούρειους ίππους[89], για να κλέψουν προσωπικές πληροφορίες από τον υπολογιστή ή τη συσκευή του θύματος.

- Κλοπή ταυτότητας σε δημόσιες ασύρματες συνδέσεις (Public Wi-Fi): Οι απατεώνες μπορούν να εκμεταλλευτούν ανοιχτές δημόσιες ασύρματες συνδέσεις για να παρακολουθήσουν τη δραστηριότητα του θύματος και να κλέψουν προσωπικές πληροφορίες.

Οι κλεμμένες ταυτότητες συνήθως συλλέγονται αυτόματα από το κακόβουλο λογισμικό που χρησιμοποιείται σε ειδικές τοποθεσίες αποθήκευσης στο διαδίκτυο (τα λεγόμενα drop zones), στις οποίες μπορούν να έχουν πρόσβαση οι δράστες ή οι πελάτες τους[90]. Τα κλεμμένα δεδομένα συνήθως προσφέρονται προς πώληση ως εμπορεύματα στην *"διασυνοριακή, διαδικτυακή, μαύρη αγορά"*, με σκοπό την δόλια χρήση τους. Σημαντικά κέρδη υπάρχουν τόσο στο επίπεδο της πώλησης, όσο και σε αυτό της χρήσης[91].

---

[89] Οι *"Δούρειοι Ίπποι"* στον κόσμο της κυβερνοασφάλειας αναφέρονται σε κακόβουλα προγράμματα που παριστάνουν κάτι ανυποψίαστο, όπως ένα αναβαθμιστικό πρόγραμμα ή μια χρήσιμη εφαρμογή, αλλά στην πραγματικότητα προκαλούν ζημία στον υπολογιστή του χρήστη. Μόλις εκτελεστεί, ο ιός επιτρέπει στους επιτιθέμενους να αποκτήσουν πρόσβαση και έλεγχο στον υπολογιστή, κλέβοντας προσωπικά δεδομένα, παρακολουθώντας τη δραστηριότητα του χρήστη ή προκαλώντας άλλες ζημιές. Είναι σημαντικό να έχετε αντι-ιό λογισμικό και να είστε προσεκτικοί με τα αναβαθμιστικά ή λήψεις από αναξιόπιστες πηγές για να αποφύγετε τέτοιου είδους απειλές. (βλ. McAffee, https://www.mcafee.com/learn/understanding-trojan-viruses-and-how-to-get-rid-of-them/).

[90] Bundeslagebild, BKA (2015), https://www.bka.de/DE/Home/home_node.html.

[91] Bundeslagebild, BKA (2015), ο.π.

Στον Ευρωπαϊκό χώρο, και ιδιαιτέρως στις δύο χώρες που αποτελούν αντικείμενο μελέτης επί της παρούσας, δηλαδή στην Ελλάδα και στην Γερμανία, η κλοπή ψηφιακής ταυτότητας και άλλες παρόμοιες δραστηριότητες που σχετίζονται με την κυβερνοασφάλεια και τον ψηφιακό εγκληματικό χώρο ρυθμίζονται από τον ποινικό κώδικα κάθε χώρας κυρίως στα άρθρα περί απάτης και συγκεκριμένα με υπολογιστής - 386Α ΠΚ στην πρώτη και 263a StGB στην δεύτερη -, στις διατάξεις περί παράνομης συλλογή και επεξεργασία προσωπικών δεδομένων - 370 επ. ΠΚ και 202a StGB αντίστοιχα -, ενώ εφαρμογή βρίσκει ανά περίπτωση και ο ευρωπαϊκός νόμος περί προστασίας προσωπικών δεδομένων, αφού ο όρος *''κλοπή ταυτότητας''*[92] είναι ένας ευρύς όρος που περιγράφει, εκτός των άλλων, και την κατάχρηση προσωπικών δεδομένων ενός ατόμου από τρίτους. Οι ποινές για τις παραβάσεις αυτές μπορεί να κυμαίνονται ανάλογα με τη σοβαρότητα της επίθεσης, την ζημία που προκλήθηκε και άλλους παράγοντες. Όπως σε κάθε περίπτωση, η ακριβής εφαρμογή του ποινικού δικαίου εξαρτάται από τις συγκεκριμένες λεπτομέρειες και τις περιστάσεις κάθε υπόθεσης.

Η διαχείριση και προστασία της ψηφιακής ταυτότητας είναι σημαντικές, καθώς οι πληροφορίες που κυκλοφορούν στο διαδίκτυο μπορούν να έχουν επιπτώσεις στην ιδιωτικότητα, την ασφάλεια και τη φήμη του ατόμου ή της επιχείρησης. Οι πρακτικές όπως η επιλεκτική διανομή προσωπικών πληροφοριών, η χρήση ισχυρών κωδικών πρόσβασης, η προσεκτική κοινοποίηση πληροφοριών και η επιλογή να συμμετέχετε ή όχι σε συγκεκριμένες ψηφιακές πλατφόρμες και υπηρεσίες είναι σημαντικά βήματα για την ασφαλή διαχείριση της ψηφιακής σας παρουσίας.

Ακολούθως, με σκοπό την καλύτερη κατανόηση των όσων αναφέρθηκαν παραπάνω, αναλύονται ορισμένες από τις συνηθέστερες πρακτικές κλοπής ψηφιακών ταυτοτήτων, το carding, το phishing και το skimming, οι οποίες μπορούν να λειτουργούν και συνδυαστικά.

5.1.2.1 Carding

Το *"carding"* αναφέρεται στην γενικότερη πρακτική της αγοράς και χρήσης παράνομα αποκτηθεισών πιστωτικών καρτών ή χρεωστικών καρτών, με σκοπό την προμήθεια προϊόντων ή υπηρεσιών, χωρίς την έγκριση του πραγματικού κατόχου της κάρτας. Αυτή η δραστηριότητα αποτελεί μια μορφή απάτης με υπολογιστή.

Οι άνθρωποι που ασχολούνται με το carding, γνωστοί ως *"carders"*, αναζητούν και αποκτούν πιστωτικές κάρτες ή χρεωστικές κάρτες και τις χρησιμοποιούν για να

[92] Borges G./ Schwenk J./ Stuckenberg C.F./ Wegener C. (2011), σελ. 234.

πραγματοποιήσουν αγορές ή να κάνουν συναλλαγές σε διάφορες πλατφόρμες, ενδεχομένως χωρίς τη γνώση των κατόχων των καρτών. Οι carders συνήθως αποκτούν τα δεδομένα των καρτών μέσω διαφόρων μεθόδων, όπως κλοπή δεδομένων από ηλεκτρονικές αγορές, ψεύτικες ιστοσελίδες, κλοπή προσωπικών πληροφοριών μέσω phishing και κακόβουλο λογισμικό. Αφού αποκτήσουν αυτά τα δεδομένα, μπορούν να τα χρησιμοποιήσουν για να πραγματοποιήσουν online αγορές, να αναλάβουν ελέγχους λογαριασμών ή να προσπαθήσουν να αντλήσουν χρήματα από τους λογαριασμούς των θυμάτων. Συνήθως δεν υπάρχουν άμεσες διαδικτυακές διαθέσεις περιουσιακών στοιχείων που βασίζονται στα κλεμμένα δεδομένα των καρτών. Τα δεδομένα αυτά χρησιμοποιούνται για την αρχική αγορά προϊόντων μέσω διαδικτύου, τα οποία στη συνέχεια μεταπωλούνται μέσω νόμιμων διαδικτυακών πλατφόρμων αγοράς και καταστημάτων.

Ιδιαίτερα διαδεδομένο είναι, επίσης, το *"carding on demand"*, το οποίο αναφέρεται σε μια πρακτική όπου κάποιος αγοράζει υπηρεσίες που σχετίζονται με το carding, δηλαδή την παράνομη απόκτηση και χρήση πιστωτικών καρτών ή χρεωστικών καρτών με σκοπό την απάτη και την προμήθεια προϊόντων ή υπηρεσιών χωρίς την έγκριση των κατόχων των καρτών.

Στο *"carding on demand"*, οι ατίθασοι χρήστες μπορούν να πληρώσουν κάποιους ειδικευμένους απατεώνες για να παρέχουν υπηρεσίες που σχετίζονται με το carding. Αυτό μπορεί να περιλαμβάνει την προμήθεια κλεμμένων πιστωτικών καρτών. Οι *"προμηθευτές"* μπορούν να παρέχουν κλεμμένα δεδομένα πιστωτικών καρτών, συμπεριλαμβανομένου του αριθμού της κάρτας, της ημερομηνίας λήξης και του κωδικού ασφαλείας, σε άτομα που θέλουν να προβούν σε απάτες. Λόγω της ευρείας χρήσης κακόβουλου λογισμικού, τα δεδομένα πιστωτικών καρτών που είναι διαθέσιμα στο διαδίκτυο αξιοποιούνται μαζικά από εγκληματίες και αποθηκεύονται σε διακομιστές που χρησιμοποιούνται για το σκοπό αυτό. Τα δεδομένα πιστωτικών καρτών που έχουν αποκτηθεί με δόλιο τρόπο αποτελούν αντικείμενο ενεργού εμπορίου μέσω διαδικτυακών πυλών και φόρουμ. Τα αρχεία δεδομένων μπορούν συνήθως να αγοραστούν για 3 έως 5 ευρώ. Λόγω της συνεχούς και εκτεταμένης διαθεσιμότητας αξιόπιστων δεδομένων πιστωτικών καρτών, η εμπορία και η χρήση παράνομα αποκτηθέντων δεδομένων πιστωτικών καρτών γίνεται ευρέως διαδεδομένη[93].

Ακόμα παρέχονται υπηρεσίες αγορών. Οι ατίθασοι χρήστες μπορούν να πληρώσουν για την εκτέλεση αγορών προϊόντων ή υπηρεσιών με κλεμμένες πιστωτικές κάρτες. Οι

[93] Bundeslagebild, BKA (2010), https://www.bka.de/DE/Home/home_node.html.

"προμηθευτές" μπορούν να αναλάβουν τη διαδικασία της αγοράς και να παραδώσουν τα αγαθά στον πελάτη. Σε ορισμένες περιπτώσεις, ο προμηθευτής χρησιμοποιεί αρχικά τους δικούς του *"reshippers"* (άτομα που προωθούν τα εμπορεύματα), στους οποίους αποστέλλονται αρχικά τα εμπορεύματα και οι οποίοι διασφαλίζουν την τελική αποστολή στη διεύθυνση που έχει ορίσει ο πελάτης. Ο προμηθευτής λαμβάνει, συνήθως, μεταξύ 25% και 40% της πραγματικής τιμής του προϊόντος ως προμήθεια. Στη συνέχεια, ο πελάτης χρησιμοποιεί το παρανόμως αποκτηθέν προϊόν για δικούς του σκοπούς ή συχνά το μεταπουλά στο διαδίκτυο.

Τέλος, πολύ χρήστες-πελάτες αναζητούν την παροχή συμβουλών και οδηγιών, σχετικά με το πώς να εκμεταλλευτούν κλεμμένες κάρτες, να αποφύγουν ανίχνευση και να επιτύχουν επιτυχημένες απάτες, πράγμα που παρέχεται επίσης ως υπηρεσία.

Ένα ρεαλιστικό παράδειγμα των παραπάνω, αποτελεί μια έρευνα του 2015 σχετικά με μία πλατφόρμα φορέα εκμετάλλευσης ψηφιακών ταυτοτήτων με λογισμικό κατασκοπείας, η οποία αποκάλυψε περισσότερα από 7,4 εκατομμύρια αρχεία δεδομένων που περιείχαν λογαριασμούς χρηστών από διάφορους φορείς εκμετάλλευσης τηλεπικοινωνιών. Μεταξύ άλλων, το σύνολο δεδομένων περιείχε πληροφορίες σχετικά με αποθηκευμένους λογαριασμούς πιστωτικών καρτών και τραπεζικούς λογαριασμούς. Από την εν λόγω έρευνα διαπιστώθηκε, ότι τα περισσότερα από τα δεδομένα πρόσβασης ήταν έγκυρα τη στιγμή που προστατεύονταν. Εφαρμόστηκαν αμέσως προληπτικά μέτρα για την προστασία των χρηστών σε διεθνή συνεργασία με παγκοσμίως ενεργούς παρόχους υπηρεσιών και αρχές ασφαλείας[94].

5.1.2.2 Phishing

Η πιο συνηθισμένη μέθοδος κλοπής ψηφιακής ταυτότητας είναι το λεγόμενο *"phishing"*. Ο όρος προέρχεται από την αγγλική λέξη *"fishing"*, που σημαίνει ψάρεμα, και τη χρήση του δίφθογγου *"ph"* αντί του γράμματος *"f"*, όπως συνηθίζουν να κάνουν οι προγραμματιστές και οι άνθρωποι που ασχολούνται με την πληροφορική. Το *"phishing*", λοιπόν, είναι μια μορφή κυβερνοαπάτης, όπου κακόβουλοι χρήστες προσπαθούν να αποκτήσουν προσωπικές πληροφορίες, όπως δεδομένα από πιστωτικές κάρτες, κωδικούς πρόσβασης, και άλλες ευαίσθητες πληροφορίες, παρουσιάζοντας τους εαυτούς τους ως νόμιμες και αξιόπιστες πηγές.

[94] Bundeslagebild, BKA (2015), https://www.bka.de/DE/Home/home_node.html.

Οι δράστες που εφαρμόζουν το phishing δημιουργούν συνήθως ψεύτικες ιστοσελίδες, ηλεκτρονικά μηνύματα ή μηνύματα κειμένου που μοιάζουν με αυτά που αποστέλλονται από νόμιμους οργανισμούς ή υπηρεσίες. Ο στόχος τους είναι να πείσουν τα θύματα να αποκαλύψουν προσωπικές πληροφορίες.

Υπάρχουν διάφορες μορφές phishing, συμπεριλαμβανομένων:

- Email Phishing: Οι κακόβουλοι χρήστες αποστέλλουν ψεύτικα email που φαίνονται να προέρχονται από γνωστούς οργανισμούς, όπως τράπεζες, κοινωνικά δίκτυα, κυβερνητικές υπηρεσίες κ.ά., ζητώντας από τα θύματα να κάνουν κλικ σε συνδέσμους και να αποκαλύψουν προσωπικές πληροφορίες.

- Spear Phishing: Παρόμοιο με το email phishing, αλλά είναι πιο εξειδικευμένο. Οι δράστες στοχεύουν σε συγκεκριμένα άτομα ή οργανισμούς, συλλέγοντας προσωπικές πληροφορίες για να δημιουργήσουν ψεύτικα μηνύματα με μεγαλύτερη πιθανότητα επιτυχίας.

- Ιστοσελίδες Phishing: Δημιουργούνται ψεύτικες ιστοσελίδες που μοιάζουν με πραγματικές, συχνά αντιγράφοντας τον σχεδιασμό και τα γραφικά προκειμένου να αποπλανήσουν τα θύματα να εισαγάγουν προσωπικές πληροφορίες.

5.1.2.2.1 Man-in-the-Middle (MITM)

Παρά τα ποικίλα και ισχυρά μέτρα προστασίας και πρόληψης που προσπαθούν να εφαρμόσουν οι τράπεζες, οι δράστες προσαρμόζονται διαρκώς τεχνικά στις αλλαγές του πλαισίου προστασίας και αναπτύσσουν νέα ή καλύτερα λογισμικά επίθεσης. Μία τέτοια σύγχρονη μορφή phishing είναι η επίθεση *"Man-in-the-Middle"* (MITM), γνωστή και ως *"Άνθρωπος στη Μέση",* όπου ένας επιτιθέμενος παρεμβαίνει μεταξύ δύο επικοινωνούντων μερών, με τη χρήση κάποιου κακόβουλου λογισμικού, με σκοπό να παρακολουθεί, παραβιάζει ή ακόμα και να παραποιήσει την επικοινωνία τους. Αυτό συνήθως γίνεται χωρίς τη γνώση των εμπλεκομένων μερών.

Η επίθεση MITM εκμεταλλεύεται, συνήθως, την έλλειψη κρυπτογράφησης ή την αδυναμία επαλήθευσης της ταυτότητας των επικοινωνούντων μερών. Ο επιτιθέμενος δημιουργεί ένα ενδιάμεσο σημείο επικοινωνίας και ενδιάμεσου υποκείμενου όπου η επικοινωνία διέρχεται μέσα από αυτό. Με αυτόν τον τρόπο, ο δράστης μπορεί να

παρακολουθεί και να καταγράφει τις πληροφορίες που ανταλλάσσονται μεταξύ των δύο μερών.

Επιπλέον, οι επιτιθέμενοι μπορούν να προσθέσουν, να τροποποιήσουν ή να διαγράψουν πληροφορίες μεταξύ της επικοινωνίας του πραγματικού κατόχου του λογαριασμού με το εκάστοτε τραπεζικό ίδρυμα, παραπλανώντας ή προκαλώντας κακόβουλη συμπεριφορά. Οι μολυσμένοι υπολογιστές εκτελούν ουσιαστικά πρόσθετες λειτουργίες ανεξάρτητα από τη γνώση καιτης προθέσεις του χρήστη και κατεβάζουν πρόσθετο κακόβουλο λογισμικό χωρίς αυτό να δύναται να ανιχνευθεί. Το κακόβουλο λογισμικό σε έναν μολυσμένο υπολογιστή μπορεί να μην ενεργοποιηθεί μέχρι ο χρήστης να αποκτήσει πρόσβαση σε έναν διαδικτυακό τραπεζικό ιστότοπο και να ενεργοποιείται τη στιγμή που ο χρήστης διαβιβάζει μια εντολή εμβάσματος στην τράπεζα. Κατά τη διάρκεια της διαδικασίας μεταφοράς, το κακόβουλο λογισμικό τροποποιεί τα δεδομένα μεταφοράς και καταλαμβάνει μια ενδιάμεση θέση στην επικοινωνία σε πραγματικό χρόνο, η οποία δεν μπορεί να εντοπιστεί από εργαλεία ασφαλείας (π.χ. λογισμικό προστασίας από ιούς ή πιστοποιητικά). Παρόλα αυτά, επειδή το υπόλοιπο του λογαριασμού που είναι ορατό στον χρήστη αλλάζει,σε πολλές περιπτώσεις η συναλλαγή μπορεί να εντοπιστεί μόνο με την εκτύπωση εντύπου κίνησης λογαριασμού.

Μερικές από τις μορφές MITM επιθέσεων περιλαμβάνουν:

- Επίθεση ARP Spoofing: Ο δράστης ψευδοκαταχωρεί διευθύνσεις MAC στο τοπικό δίκτυο, προκειμένου να αποστείλει την επικοινωνία μέσω του δικού του συστήματος, ελέγχοντας τη ροή των δεδομένων.

- Επίθεση σε Δικτυακό Επίπεδο (Network Layer): Ο επιτιθέμενος δράστης μπορεί να εισαχθεί μεταξύ δύο σημείων σε ένα δίκτυο, κερδίζοντας πρόσβαση και ελέγχο της επικοινωνίας.

- Επίθεση σε Επίπεδο Εφαρμογής (Application Layer): Ο δράστης μπορεί να δημιουργήσει ψευδοδεδομένα, όπως ψεύτικες ιστοσελίδες, για να παραπλανήσει τα θύματα να δώσουν ευαίσθητες πληροφορίες.

Για να προστατευτεί κανείς από επιθέσεις MITM, θα πρεπει να προβεί στην χρήση ασφυκτικών συνδέσεων (HTTPS) για την ασφαλή επικοινωνία, στην ενεργοποίηση της δυνατότητας αυθεντικοποίησης διπλής παρακολούθησης (Two-Factor Authentication) και να είναι ιδιαίτερα προσεκτικός με τα δίκτυα Wi-Fi στα οποία συνδέεται.

5.1.2.2.2 Κοινωνική μηχανική χειραγώγηση

Ωστόσο, οι δράστες δεν βασίζονται μόνο σε καθαρά τεχνικές λύσεις, αλλά προσπαθούν επίσης να λάβουν τις απαραίτητες πληροφορίες για τους πελάτες μέσω της λεγόμενης κοινωνικής μηχανικής χειραγώγησης[95], επηρεάζοντας ένα άτομο να αποκαλύψει εμπιστευτικές πληροφορίες[96]. Σε επιθέσεις στον κυβερνοχώρο που χρησιμοποιούν κοινωνική μηχανική, οι δράστες προσποιούνται ότι είναι αξιόπιστοι εκπρόσωποι μιας εταιρείας ή ενός οργανισμού και παρακινούν τους χρήστες να αποκαλύψουν ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης ή πιστωτικές πληροφορίες, παρακάμπτοντας προστατευτικά μέτρα ή εγκαθιστώντας οι ίδιοι κακόβουλο κώδικα στα συστήματά τους, αξιοποιώντας ανθρώπινες αδυναμίες και ανασφάλειες, όπως η περιέργεια ή ο φόβος και, επομένως, η πρόσβαση σε ευαίσθητα δεδομένα και πληροφορίες, προκειμένου να υπονομεύσουν τους μηχανισμούς εξουσιοδότησης του χρήστη.

5.1.2.3 Pharming

Το Pharming είναι μια περαιτέρω εξέλιξη του κλασικού phishing. Είναι μια μορφή κυβερνοεπίθεσης όπου οι δράστες ανακατευθύνουν την κυκλοφορία της ηλεκτρονικής επικοινωνίας (όπως αιτήσεις πρόσβασης σε ιστοσελίδες) προς ψεύτικες διευθύνσεις IP ή ιστοσελίδες, με σκοπό να αποκτήσουν προσωπικές πληροφορίες από τα θύματα. Οι δράστες των επιθέσεων pharming διατηρούν τις δικές τους μεγάλες φάρμες διακομιστών στις οποίες αποθηκεύονται ψεύτικοι ιστότοποι. Σε αντίθεση με το *"phishing"*, όπου οι χρήστες παραπλανούνται να εισαγάγουν τα δεδομένα τους σε ψεύτικες ιστοσελίδες, το *"pharming*" είναι μια επίθεση σε επίπεδο δικτύου που μπορεί να επηρεάσει πολλούς χρήστες.

Υπάρχουν δύο είδη *"pharming"*:

A. DNS Pharming: Σε αυτήν τη μέθοδο, οι επιτιθέμενοι καταφέρνουν να αλλοιώσουν τον λειτουργικό τρόπο που λειτουργούν τα DNS (Domain Name System). Το DNS είναι υπεύθυνο για τη μετάφραση των ονομάτων των ιστοσελίδων σε αντίστοιχες διευθύνσεις IP (αντιστοίχιση της εισαγόμενης διεύθυνσης URL στην αντίστοιχη διεύθυνση IP). Οι δράστες μπορούν να εισάγουν ψεύτικες καταχωρήσεις

[95] Ως κοινωνική χειραγώγηση ή "social manipulation" γενικότερα νοείται η πρακτική όπου άτομα ή ομάδες εκμεταλλεύονται τις ανθρώπινες κοινωνικές σχέσεις, συμπεριλαμβανομένων των αδυναμιών, των ανησυχιών και των πεποιθήσεων, προκειμένου να επηρεάσουν και να ελέγξουν τη συμπεριφορά άλλων ατόμων (βλ. BSI Gefährdungskataloge).

[96] BSI (2015), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf%3F__blob%3DpublicationFile.

DNS ή να αλλοιώσουν τις υπάρχουσες, με αποτέλεσμα, μόνο ψεύτικοι ιστότοποι μπορούν να καλούνται από αυτό το σύστημα, ακόμα κι αν η διεύθυνση ιστού έχει εισαχθεί σωστά. Εάν το θύμα εισάγει δεδομένα στον ψεύτικο ιστότοπο, ο δράστης μπορεί να χρησιμοποιήσει τα δεδομένα για πράξεις κατάχρησης και κλοπής ταυτότητας[97].

B. Hosts File Pharming: Σε αυτήν την περίπτωση, οι δράστες τροποποιούν το αρχείο *"hosts"* στον υπολογιστή του θύματος. Το αρχείο *"hosts"* αντιστοιχεί ονόματα domain με αντίστοιχες διευθύνσεις IP και χρησιμοποιείται για την προτεραιότητα αναζήτησης κατά τη σύνδεση με ιστοσελίδες. Οι επιτιθέμενοι τροποποιούν αυτό το αρχείο προκειμένου να ανακατευθύνουν τα θύματα σε παραπλανητικές ιστοσελίδες.

Ο στόχος των επιθέσεων *"pharming"* είναι να παρακολουθήσουν την κυκλοφορία της επικοινωνίας και να αποκτήσουν ευαίσθητες πληροφορίες, όπως χρησιμοποιούμενα ονόματα χρήστη και κωδικοί πρόσβασης. Οι χρήστες πρέπει να είναι προσεκτικοί όταν συνδέονται σε ιστοσελίδες, να χρησιμοποιούν ασφυκτικές συνδέσεις (HTTPS) και να αποφεύγουν την παρακολούθηση των ιστοσελίδων που επισκέπτονται.

5.1.2.4 Μέτρα αντιμετώπισης

Η πρόληψη του phishing περιλαμβάνει την προσεκτική ανάγνωση και αξιολόγηση ηλεκτρονικών μηνυμάτων και συνδέσμων που λαμβάνονται. Επίσης, είναι σημαντική η ενημέρωση για τις πρακτικές ασφάλειας στον κυβερνοχώρο και η χρήση δυνατών κωδικών πρόσβασης και διαδικασιών ελέγχου ταυτότητας. Πιο συγκεκριμένα:

➔ Επιβεβαίωση Ιστοσελίδας (URL Verification). Πριν την επίσκεψη σε ιστοσελίδα από σύνδεσμο που έχει λάβει κάποιος μέσω email ή μηνύματος, είναι απαραίτητος ο έλεγχος της διεύθυνσης URL και στα στοιχεία μορφοποίησης του συνδέσμου (τυπογραφία, σημεία στίξης κλπ.) για την ανίχνευση ύποπτων στοιχείων.

➔ Προσοχή σε ανεπιθύμητα e-mails. Email από άγνωστες πηγές ή με αιτήματα για ευαίσθητες πληροφορίες είναι ύποπτα. Απαιτείται άμεση επικοινωνία με τον αποστολέα μέσω επίσημων μέσων επικοινωνίας για επιβεβαίωση.

➔ Χρήση αξιόπιστων πηγών και ιστοσελίδων, ειδικά για τις τραπεζικές συναλλαγές, αγορές και άλλες ευαίσθητες ενέργειες.

---

[97] LKA Βάδης-Βυρτεμβέργης (2016), https://im.baden-wuerttemberg.de/de/service/publikation/did/cybercrimedigitale-spuren.

➔ Ενεργοποίηση συστήματος διπλής ταυτοποίησης (Two-Factor Authentication - 2FA), καθώς αυτό προσθέτει ένα επιπλέον επίπεδο ασφαλείας πέραν του κωδικού πρόσβασης.

➔ Ενημέρωση του λογισμικού και του λειτουργικού συστήματος, των προγραμμάτων περιήγησης και των προγραμμάτων ασφαλείας.

➔ Χρήση κρυπτογραφημένης σύνδεσης (HTTPS) στις ιστοσελίδες που ζητούν προσωπικές πληροφορίες. Η διεύθυνση URL θα πρέπει να ξεκινά με *"https://"* και όχι μόνο *"http://"*. Η κρυπτογραφημένη σύνδεση προστατεύει τα δεδομένα του χρήστη από παρεμβολές.

➔ Ενημέρωση σχετικά με τις επιθέσεις phishing.

➔ Χρήση προγραμμάτων αντι-phishing.

➔ Άμεση επικοινωνία με την τράπεζα ή τον εκάστοτε οργανισμό, σε περίπτωση τηλεφωνικής κλήσης ή μηνύματος που φαίνεται να προέρχεται από την τράπεζά σας, μέσω των επίσημων στοιχείων επικοινωνίας.

5.1.3.1 Skimming

Το *"skimming"* είναι μια μέθοδος απάτης που στοχεύει στην απόκτηση προσωπικών πληροφοριών από πιστωτικές κάρτες ή χρεωστικές κάρτες των θυμάτων. Οι δράστες χρησιμοποιούν διάφορες μεθόδους για να αποκτήσουν τις πληροφορίες αυτές και στη συνέχεια να τις χρησιμοποιήσουν για απάτη ή κλοπή. Οι συνηθέστερες μέθοδοι skimming περιλαμβάνουν:

- Συσκευές Ανάγνωσης Καρτών (Card Readers): Οι δράστες τοποθετούν κρυφές συσκευές ανάγνωσης καρτών (skimmers) σε αυτόματες μηχανές ανάληψης μετρητών, πληρωτές και άλλες συσκευές που δέχονται κάρτες. Αυτές οι συσκευές καταγράφουν τα δεδομένα της κάρτας και τον PIN κώδικα του θύματος όταν αυτός εισάγει την κάρτα του.

- Καταγραφή Καρτών με Κρυφές Κάμερες: Ως συμπληρωματική μέθοδος, οι επιτιθέμενοι τοποθετούν κρυφές κάμερες στις συσκευές για να καταγράψουν τη διαδικασία εισαγωγής των πληροφοριών της κάρτας.

- Εσωτερική Απάτη (Internal Fraud): Αυτή η μέθοδος εμπλέκει τους εργαζόμενους σε καταστήματα, εστιατόρια ή άλλα καταστήματα που δέχονται πληρωμές με κάρτες. Οι εργαζόμενοι μπορούν να αντικαταστήσουν τη συσκευή ανάγνωσης καρτών με μια παραπλανητική, προκειμένου να κλέψουν τις πληροφορίες των καρτών.

Ενώ στην Ελλάδα τα εν λόγω αδικήματα τιμωρούνται σύμφωνα με τα άρθρα για την απάτη με υπολογιστή (386Α ΠΚ) και την παράνομη πρόσβαση σε πληροφοριακό σύστημα (370Γ ΠΚ), στην Γερμανία τα εν λόγω ποινικά αδικήματα τυποποιούνται πέραν αυτών και σε επιπλέον άρθρα ως ειδικότερες και ξεχωριστές περιπτώσεις και συγκεκριμένα με την διάταξη περί δολιοφθορών υπολογιστών (§ 303b StGB) και τις διατάξεις για την πλαστογραφία καρτών πληρωμής (§§ 152b, 149 StGB).

5.1.3.2 Μέτρα αντιμετώπισης

➔ Επιλογή ασφαλούς τραπεζικής συναλλαγής σε ασφαλή περιβάλλοντα.

➔ Έλεγχος των συσκευών ανάγνωσης καρτών για ασυνήθιστα εξαρτήματα.

➔ Χρήση χειροκίνητης εισαγωγής PIN με κάλυψη του χεριού που το πληκτρολογεί.

➔ Άμεση καταγγελία και ενημέρωση των αρμόδιων αρχών σε περίπτωση που διαπιστωθεί ύποπτη συσκευή ή και αντιγραφή στοιχείων κάρτας.

➔ Επιθεώρηση του ATM για τον προσδιορισμό της χειραγώγησης - τεχνική skimming, σημάδια εργαλείων, υπολείμματα κόλλας στις άκρες της οθόνης, μικρές κάμερες σε φωτεινές οθόνες πάνω από το πληκτρολόγιο, θήκες για φυλλάδια, ανιχνευτές καπνού, ρολόγια κ.λπ., προσαρτημένα εικονικά πληκτρολόγια.

➔ Εξασφάλιση άμεσης αξιολόγησης των ημερολογίων του μηχανήματος (οι δράστες χρησιμοποιούν αντίγραφα που έχουν δημιουργηθεί σε ξένα ATM λίγες μόνο ώρες μετά την υποκλοπή των δεδομένων)

➔ Εντοπισμός μαρτύρων

➔ Ασφάλιση του υλικού βίντεο της κάμερας παρακολούθησης.

➔ Ασφάλιση αποδεικτικών στοιχείων, ίχνη DNA στην περιοχή υποδοχής κάρτας, και στις αυτοκόλλητες ταινίες για τη σύνδεση του μηχανισμού αντιγραφής.

➔ Προσοχή στην τεχνολογία και τα εργαλεία skimming (καλύμματα, πληκτρολόγια, ανοιχτήρια θυρών, εξοπλισμός συγκόλλησης, ηλεκτρονικά εξαρτήματα, κολλητική ταινία διπλής όψης, υπερκόλλα κ.λπ.).

Εάν υπάρχει υποψία ότι ένα ATM υπόκειται σε χειραγώγηση, συνήθως οι δράστες παραμένουν κοντά στον τόπο τέλεσης, προκειμένου να παρακολουθήσουν τη διαδικασία, αλλά και να πάρουν πίσω τον εξοπλισμό που χρησιμοποίησαν και να καλύψουν τα ίχνη τους. Συχνά φορούν ρουχισμό που καλύπτει το πρόσωπο τους όταν χρησιμοποιείται βιντεοπαρακολούθηση.

5.2 Το ηλεκτρονικό ταχυδρομείο ως μέσο εγκληματικότητας

5.2.1 Γενικές Πληροφορίες

Το φαινόμενο του spam email έχει κατακλύσει την ηλεκτρονική αλληλογραφία και αναπόφευκτα προκαλεί αναστάτωση στους παραλήπτες. Τα ανεπιθύμητα μηνύματα spam είναι ηλεκτρονικά μηνύματα που αποστέλλονται μαζικά σε παραλήπτες, χωρίς την προηγούμενη συγκατάθεσή τους, και συνήθως περιέχουν εμπορικό ή διαφημιστικό περιεχόμενο. Αυτό το πρόβλημα επηρεάζει χρήστες σε όλο τον κόσμο και αποτελεί μία από τις μεγαλύτερες προκλήσεις της ηλεκτρονικής επικοινωνίας. Το spam αναφέρεται σε οποιοδήποτε ανεπιθύμητο μήνυμα που αποστέλλεται μαζικά. Συνήθως, αυτά τα μηνύματα περιέχουν διαφημίσεις για προϊόντα ή υπηρεσίες, αλλά μπορεί επίσης να περιέχουν ανεπιθύμητο περιεχόμενο, όπως προσβλητικά ή απάτης μηνύματα. Οι αποστολείς spam στοχεύουν να προωθήσουν τα προϊόντα ή τις υπηρεσίες τους, αλλά και να συλλέξουν προσωπικά δεδομένα ή να διαπράξουν απάτες[98].

Όσον αφορά τις μορφές του spam, μπορούν να αναφερθούν οι εξής[99]:

- Διαφημιστικά Μηνύματα: Τα διαφημιστικά μηνύματα αποτελούν την πιο συνηθισμένη μορφή spam. Στόχος τους είναι η προώθηση προϊόντων και υπηρεσιών.

- Απάτες Phishing: Τα μηνύματα phishing είναι κακόβουλα μηνύματα που στοχεύουν στην απόκτηση προσωπικών δεδομένων των χρηστών, όπως ονόματα χρήστη, κωδικοί πρόσβασης και αριθμοί πιστωτικών καρτών.

- Απάτες Scamming: Οι απάτες scamming αποστέλλονται με σκοπό την οικονομική εξαπάτηση των χρηστών. Συνήθως προσφέρουν πλαστές υπηρεσίες ή προϊόντα με στόχο να αποσπάσουν χρήματα από τα θύματά τους.

- Κακόβουλο Λογισμικό Malware: Τα μηνύματα που περιέχουν κακόβουλο λογισμικό αποτελούν μια επικίνδυνη μορφή spam. Μπορεί να περιέχουν συνδέσμους που οδηγούν σε ιστοσελίδες με κακόβουλο κώδικα, ο οποίος μπορεί να προκαλέσει ζημιές στον υπολογιστή του χρήστη.

---

[98] Αρχή Προστασίας Δεδομένων, https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/proothisiproiontwn/hlektronika_mesa_proothisi/sumvoules_spam.

[99] BSI, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Spam/Woran-erkennt-man-Spam/woran-erkennt-man-spam.html.

Η επίπτωση του spam στους παραλήπτες είναι αρνητική και πολλαπλή. Καταρχάς, είναι χρονοβόρο και ενοχλητικό να λαμβάνει κανείς μεγάλο όγκο ανεπιθύμητων μηνυμάτων, τα οποία πρέπει να διαγράψει ή να τα μεταφέρει σε φακέλους spam. Επιπλέον, το spam μπορεί να περιέχει κακόβουλο λογισμικό (malware) που απειλεί την ασφάλεια των συστημάτων των χρηστών. Επιπλέον, οι απάτες που συνδέονται με το spam μπορούν να οδηγήσουν σε οικονομική απώλεια ή κλοπή ταυτότητας.

Οι πάροχοι ηλεκτρονικού ταχυδρομείου και οι υπηρεσίες διαχείρισης ηλεκτρονικού ταχυδρομείου έχουν αναπτύξει μηχανισμούς φιλτραρίσματος spam για να περιορίσουν την είσοδο ανεπιθύμητων μηνυμάτων στα εισερχόμενα των χρηστών. Αυτοί οι μηχανισμοί χρησιμοποιούν διάφορες τεχνικές και κριτήρια για να αναγνωρίσουν το spam και να το αποκλείσουν. Ένας από τους πιο συνηθισμένους μηχανισμούς φιλτραρίσματος είναι ο έλεγχος της αυθεντικότητας του αποστολέα. Οι υπηρεσίες φιλτραρίσματος spam ελέγχουν τη διεύθυνση IP του αποστολέα, την ταυτότητα του διακομιστή και άλλα στοιχεία για να καθορίσουν εάν το μήνυμα προέρχεται από έγκυρη πηγή. Επίσης, οι μηχανισμοί φιλτραρίσματος εξετάζουν το περιεχόμενο του μηνύματος για στοιχεία που υποδηλώνουν διαφήμιση ή απάτη. Επιπλέον, οι υπηρεσίες φιλτραρίσματος spam χρησιμοποιούν μηχανισμούς μηχανικής μάθησης για να εκπαιδεύσουν το σύστημα να αναγνωρίζει τα χαρακτηριστικά του spam με βάση τα παρελθόντα δεδομένα. Αυτό επιτρέπει στο σύστημα να είναι ευέλικτο και να προσαρμόζεται στις νέες μορφές spam που εμφανίζονται συνεχώς.

Για να μπορέσουν να στείλουν εκατομμύρια e-mail, οι δράστες-spammers χρειάζονται διευθύνσεις., τις οποίες μπορούν να προμηθευτούν από αντιπροσώπους διευθύνσεων. Ωστόσο, οι εμπορικοί spammers διατηρούν συχνά βάσεις δεδομένων με εκατομμύρια διευθύνσεις. Οι διευθύνσεις διατίθενται γρήγορα μέσω της στοχευμένης - με αυτοματοποιημένο πρόγραμμα - αναζήτησης ομάδων συζήτησης, ιστοσελίδων ή καταλόγων e-mail, αλλά και δοκιμάζοντας κοινές διευθύνσεις (info@... κ.λπ.). Λόγω του μεγάλου όγκου διευθύνσεων, δεν έχει σημασία αν πολλές είναι άκυρες. Η αποστολή πραγματοποιείται συνήθως πλήρως αυτόματα μέσω ειδικών προγραμμάτων και είναι σχεδόν ανέξοδη. Ο αποστολέας πρέπει μόνο να ξεκινήσει το πρόγραμμα. Καθώς, λοιπόν, τα μαζικά μηνύματα ηλεκτρονικού ταχυδρομείου είναι σχετικά φθηνά για τον αποστολέα, υπάρχει σημαντικό κέρδος, ακόμα και αν μόνο λίγοι αποδέκτες αγοράσουν ένα προϊόν. Συχνά τα προϊόντα που διαφημίζονται είναι παράνομα, παρόλο που σύμφωνα με τη νομοθεσία, τόσο την ελληνική, όσο και τη γερμανική, αυτό απαγορεύεται.

5.2.2.1 Hoaxes

Τα λεγόμενα hoaxes ή μηνύματα αποπληροφόρησης διαδίδονται επίσης ως αλυσιδωτά μηνύματα spam και αφορούν ψευδείς πληροφορίες που διαδίδονται εσκεμμένα με σκοπό να παραπλανήσουν και να προκαλέσουν βλάβη. Για παράδειγμα, πλαστά δημοσιεύματα ειδήσεων και πολιτική προπαγάνδα.

Τα περισσότερα *"hoaxes"* περιέχουν τα ακόλουθα στοιχεία:

- Ένα ζήτημα που πρέπει να εκφράζει σοβαρότητα (π.χ. μια αναφορά από μια σημαντική τράπεζα)
- Δήθεν πραγματικές πληροφορίες σχετικά με ένα γεγονός ιδιαίτερης σημασίας (π.χ. εμφάνιση σφάλματος υπολογιστή) ή εντυπωσιακές δυνατότητες κερδών (π.χ. υποτιθέμενες προμήθειες από μεγάλες εταιρείες λογισμικού για προώθηση e-mail), αναφορές σε καταστροφές (π.χ. τσουνάμι) ή θεωρίες συνωμοσίας.
- Ελλιπή δεδομένα, αλλά γενικευμένες αναφορές όπως *"χθες"* ή *"μόλις τώρα"* που υποδηλώνουν χρόνο.
- Επείγον αίτημα να σταλεί η πληροφορία ή η προειδοποίηση σε όσο το δυνατόν περισσότερους φίλους.

Ένα τέτοιο e-mail μπορεί να δημιουργήσει χιονοστιβάδα σε χιλιάδες ανθρώπους για εβδομάδες, μήνες ή και χρόνια. Οι αλυσιδωτές επιστολές που διανέμονται μέσω της υπηρεσίας άμεσων μηνυμάτων WhatsApp έχουν επίσης ενοχλήσει τους χρήστες σε αρκετές περιπτώσεις. Συχνά στους παραλήπτες-θύματα δημιουργείται τεράστια οικονομική ζημία, καθώς στόχος των περισσότερων δραστών είναι η παρανόμως εισροή χρημάτων.

5.2.2.2 Κακόβουλο λογισμικό - Malware

Τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου χρησιμοποιούνται επίσης για τη διάδοση κακόβουλου λογισμικού. Οι σύνδεσμοι που περιέχονται στα email οδηγούν σε διάφορους ιστότοπους, ορισμένοι από τους οποίους είναι μολυσμένοι με κακόβουλο λογισμικό. Εάν ο παραλήπτης ακολουθήσει τον σύνδεσμο, το κακόβουλο λογισμικό φορτώνεται στον υπολογιστή. Ορισμένα ανεπιθύμητα μηνύματα μεταμφιέζονται σε μηνύματα γνωστών εταιρειών (πληροφοριακές επιστολές, τιμολόγια κ.λπ.). Τα ιογενή μηνύματα που περιέχουν ψευδείς πληροφορίες μπορούν εύκολα να κοινοποιηθούν σε

εφαρμογές ανταλλαγής μηνυμάτων όπως το WhatsApp και το Messenger. Αν γνωρίζετε το άτομο που το μοιράστηκε, ίσως το πιστέψετε περισσότερο[100].

Οι πελάτες των τραπεζών γίνονται επανειλημμένα στόχος προσπαθειών κατασκοπείας μέσω ηλεκτρονικών μηνυμάτων ηλεκτρονικού ψαρέματος-phishing. Στην Γερμανία, για παράδειγμα, με ένα πρόσφατο ηλεκτρονικό μήνυμα ηλεκτρονικού ψαρέματος, οι εγκληματίες ισχυρίζονταν ότι το πρόσφατα εγκεκριμένο πακέτο οικονομικής τόνωσης της κυβέρνησης θα καταργήσει τα μηνιαία τέλη διαχείρισης λογαριασμού στην τράπεζα Sparkasse. Για να μπορούν οι πελάτες χρησιμοποιήσουν αυτό το πλεονέκτημα, οι παραλήπτες των μηνυμάτων θα έπρεπε να κάνουν κλικ σε ένα κουμπί και να ακολουθήσουν ορισμένα βήματα. Το email με αυθεντική εμφάνιση, ωστόσο, δεν προερχόταν από τον φερόμενο αποστολέα. Όταν κανείς πατούσε στον σύνδεσμο, άνοιγε ένας ψεύτικος ιστότοπος που δεν ανήκε στην τράπεζα. Τα δεδομένα που ζητούνταν πήγαιναν απευθείας στους δράστες, οι οποίοι αποκτούσαν έτσι πρόσβαση στον λογαριασμό του θύματος[101]. Σε αυτές τις περιπτώσεις, απαιτείται διαβούλευση με τον υπεύθυνο για το έγκλημα στον κυβερνοχώρο ή τον υπεύθυνο διατήρησης αποδεικτικών στοιχείων πληροφορικής - μέτρα μόνο μετά από διαβούλευση, η απώλεια δεδομένων θέτει σε κίνδυνο την ποινική διαδικασία.

Ένα ασφαλές μέσο ηλεκτρονικής αλληλογραφίας αποτελεί το webmail, το οποίο είναι μια εξαιρετικά χρήσιμη online εφαρμογή που επιτρέπει στον χρήστη να αποστέλλει και να λαμβάνει email μέσω ενός προγράμματος περιήγησης web, χωρίς να χρειάζεται να εγκαταστήσει έναν ειδικό πελάτη email στον προσωπικό του υπολογιστή. Αυτό σημαίνει ότι η πρόσβαση στον λογαριασμό μπορεί να πραγματοποιηθεί από οπουδήποτε και από οποιαδήποτε συσκευή έχει πρόσβαση στο διαδίκτυο.

Σχετικά με το λειτουργικό σύστημα του webmail, τα email αποθηκεύονται στους διακομιστές του παρόχου ή του διαδικτυακού φιλοξενητή. Για παράδειγμα, η υπηρεσία Gmail, το Comcast ή η GoDaddy παρέχουν webmail στους χρήστες τους. Όταν αποστέλλεται ένα email, αυτό αποθηκεύεται στους διακομιστές αυτών των υπηρεσιών. Για να μπορέσει ο χρήστης να διαχειριστεί τα email του, εισέρχεται σε μια ιστοσελίδα που σχετίζεται με τον λογαριασμό του. Αυτή η ιστοσελίδα μπορεί να είναι ο επίσημος ιστότοπος του παρόχου ή του φιλοξενητή, και συνήθως θα ζητηθεί να γίνει σύνδεση με τα διαπιστευτήρια του χρήστη,

[100] BSI (2020), https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html.
[101] Wernert M. (2021), σελ. 128-129.

δηλαδή όνομα χρήστη και κωδικός. Επομένως, δεν απαιτείται κάποιο ειδικό πρόγραμμα αλληλογραφίας όπως π.χ Β. το Outlook, το Outlook Express δεν απαιτείται. Χρησιμοποιώντας ειδικό λογισμικό (πρόγραμμα e-mail), τα email μπορούν επίσης να ανακτηθούν από τον διακομιστή του παρόχου διαδικτύου και να αποθηκευτούν τοπικά στον υπολογιστή του παραλήπτη.

Ένα email αποτελείται από πολλά μέρη. Αν το συγκρίνετε με ένα συμβατικό γράμμα, υπάρχει ένας φάκελος (ο λεγόμενος «φάκελος SMTP»), ένα επιστολόχαρτο (το λεγόμενο *"header"* ή το *"headers"*) και το κείμενο ή περιεχόμενο της επιστολής (το λεγόμενο «σώμα»). Ο χρήστης, συνήθως, δεν παρατηρεί τον "*φάκελο"* και οι πληροφορίες του χάνονται όταν ταξινομούνται στο γραμματοκιβώτιο του παραλήπτη. Τα δεδομένα διεύθυνσης στο "επιστολόχαρτο" του email είναι συχνά ανώνυμα. Για να μπορέσει ο παραλήπτης να προσδιορίσει τον αποστολέα απαιτούνται τα δεδομένα της *"κεφαλίδας"*[102]. Αυτό πρέπει πρώτα να γίνει ορατό. Η διαδικασία που απαιτείται για αυτό εξαρτάται από το λογισμικό που χρησιμοποιείται ή τον πάροχο που χρησιμοποιείται.

Οι πληροφορίες που μπορούν να γίνουν αντιληπτές σχετικά με την *"κεφαλίδα"* και είναι απαραίτητες σε περίπτωση καταγγελίας είναι η διεύθυνση IP του αποστολέα, ημερομηνία και ώρα αποστολής, ο διακομιστής που χρησιμοποιήθηκε μέσω του δικτύου. Για περαιτέρω έρευνες, επομένως, είναι απαραίτητη η αποθήκευση των δεδομένων της *"κεφαλίδας"*. Για να γίνει αυτό, τα δεδομένα τής "*κεφαλίδας"* πρέπει να επισημανθούν με το ποντίκι, να αντιγραφούν και στη συνέχεια να εισαχθούν σε ένα έγγραφο κειμένου. Σε καμία περίπτωση δεν πρέπει να αποστέλλονται στην αστυνομία με τη λειτουργία *"Προώθηση",* διότι κατ' αυτόν τον τρόπο τα αρχικά δεδομένα θα διαγραφούν.

Ακόμα, οι κεφαλίδες email μπορούν να πλαστογραφηθούν, εισάγοντας ψεύτικες γραμμές πάνω από την υπάρχουσα κεφαλίδα πριν από την αποστολή. Για την αξιολόγηση της γνησιότητας χρησιμοποιούνται αναγνωρίσιμα χαρακτηριστικά πλαστογραφίας[103].

5.2.3 Μέτρα αντιμετώπισης

Για να ενισχυθεί το φιλτράρισμα του spam στην ηλεκτρονική αλληλογραφία, μπορούν να γίνουν ορισμένες ενέργειες για τον περιορισμό και έλεγχό τους:

[102] th-h.de (2019), https://th-h.de/net/usenet/faqs/headerfaq/.
[103] Kleile M. (2016), κεφ. E- Mail.

➔ Έλεγχος της πολιτικής ιδιωτικότητας των ιστοσελίδων στις οποίες είναι απαραίτητη η χρήση και καταχώρηση διεύθυνσης ηλεκτρονικού ταχυδρομείου και των όρων χρήσης των εταιρειών που αποστέλλουν μηνύματα, προκειμένου να γνωρίζει ο παραλήπτης πώς χρησιμοποιούν τα προσωπικά του δεδομένα.

➔ Αποφυγή δημοσιοποίησης της διεύθυνσης σε διαδικτυακούς τόπους, μηχανές αναζήτησης, ηλεκτρονικές λίστες, καταλόγους ή chat rooms.

➔ Ενίσχυση φίλτρου spam στην ηλεκτρονική αλληλογραφία

➔ Επιλογή καλού παρόχου ηλεκτρονικού ταχυδρομείου με προηγμένους μηχανισμούς φιλτραρίσματος spam.

➔ Δημιουργία λίστας με τις διευθύνσεις email των επαφών, ώστε να μην αποκλείονται από τα φίλτρα.

➔ Έλεγχος και άδειασμα του φακέλου spam.

➔ Αναφορά οποιουδήποτε spam email στον πάροχο του ηλεκτρονικού ταχυδρομείου, ώστε να βελτιώσει τα φίλτρα του.

➔ Αποφυγή απάντησης στα spam μηνύματα ή ανοίγματος των συνδέσμων που περιέχονται σε αυτά.

➔ Αποφυγή αναγραφής προσωπικών ή ευαίσθητων δεδομένων σε μηνύματα από άγνωστους αποστολείς.

➔ Χρήση ενημερωμένου λογισμικού καταπολέμησης ιών.

5.3 Happy Slapping και Snuff film

5.3.1 Γενικές πληροφορίες

Το *"happy slapping"* αναφέρεται σε μια ανήθικη και επιθετική πρακτική όπου άτομα επιτίθενται σε άλλα άτομα με σκοπό να τους εκφοβίσουν, να τους τρομοκρατήσουν, ή ακόμη και να τους πειράξουν, την στιγμή που οι στιγμές αυτές καταγράφονται, συνήθως, με κάμερες κινητών τηλεφώνων. Τα βίντεο αυτά στη συνέχεια συνήθως δημοσιεύονται στο διαδίκτυο ή μεταφορτώνονται σε πλατφόρμες στο διαδίκτυο και κοινοποιούνται σε άλλους χρήστες. Ο όρος *"happy slapping"* προήλθε από την Αγγλία και είναι σύνθετος, με το *"happy"* να αναφέρεται στην αδιακρίτως χαρούμενη στάση των δραστών κατά τη διάρκεια των επιθέσεων, και το *"slapping"* στις σωματικές επιθέσεις που συνήθως συμπεριλαμβάνουν χτυπήματα, χαστούκια και άλλες μορφές σωματικής βίας[104]. Οι δράστες εγκλημάτων *"happy*

[104] Ιντζεσίλογλου Ν. (2009), σελ.49-108.

slapping" είναι κυρίως έφηβοι μαθητές. Τα θύματα επιλέγονται τυχαία ή σκόπιμα, ενώ έχουν αναφερθεί ακόμη και περιπτώσεις βιασμού μαθητριών[105].

Τα *"snuff film"* αναφέρονται σε βίντεο όπου απεικονίζεται η τέλεση πραγματικών φόνων ή η άσκηση άλλων μορφών βίας σε άτομα, σε βίντεο με πορνογραφικό περιεχόμενο, αλλά και στην ηχογράφηση ιδιωτικών και προσωπικών συνομιλιών, ιδίως δασκάλων, με σκοπό την ενθάρρυνση του εκφοβισμού, του σοκ και της αηδίας. Είναι σημαντικό να σημειωθεί ότι οι περισσότερες αναφορές σε *"snuff film"* έχουν αποδειχθεί ψευδείς ή εξαπατητικές. Ο όρος *"snuff"* προέρχεται από τον μύθο ότι τέτοια βίντεο δημιουργούνται για εμπορικούς σκοπούς, κυρίως για να πωλούνται και να απολαμβάνονται από συλλέκτες[106] [107].

Και στις δύο αυτές πρακτικές η βία απεικονίζεται με τρόπο που είτε ωραιοποιείται είτε υποβαθμίζεται, παραβιάζοντας παράλληλα την ανθρώπινη αξιοπρέπεια και ζωή. Είναι πρακτικές επικίνδυνες και παράνομες, καθώς μπορούν να προκαλέσουν σωματική και ψυχολογική βλάβη στα θύματα.

Πιθανά εγκλήματα που θα πρέπει να ελεγχθούν ανάλογα με την περίσταση αποτελούν:

- Αδικήματα περί σωματικής βλάβης
- Διακίνηση πορνογραφικού υλικού
- Εγκλήματα κατά της τιμής
- Προσβολή δικαιωμάτων προστασίας προσωπικών δεδομένων και της ιδιωτικής σφαίρας
- Εκβίαση, απειλή
- Ποινικά αδικήματα κατά της σεξουαλικής αυτοδιάθεσης
- Τρομοκρατικά εγκλήματα

5.3.2 Μέτρα αντιμετώπισης

➔ Καταγγελία
➔ Κατάσχεση του κινητού τηλεφώνου
➔ Ταυτοποίηση και ανάκριση δραστών
➔ Ταυτοποίηση θυμάτων και μαρτύρων

[105] Mag. phil. Michael Weber (2014), σελ 43.
[106] Barbara Mikkelson (2021), https://www.snopes.com/fact-check/a-pinch-of-snuff/.
[107] Mag. phil. Michael Weber (2014), σελ 43.

➔ Έλεγχος παρακολούθησης (π.χ. αναζήτηση κατ' οίκον, διερεύνηση σκηνής εγκλήματος, έρευνα στον τόπο του εγκλήματος)

➔ Ιατρική και ψυχολογική υποστήριξη θυμάτων

Συχνό φαινόμενο αποτελεί πλέον επίσης η βιντεοσκόπηση βίαιων επιθέσεων κατά αστυνομικών και τη μεταφόρτωσή τους σε πλατφόρμες στο διαδίκτυο, κυρίως με σκοπό την αυτοπροβολή των δραστών. Στο πλαίσιο αυτό, εκτός από τα προαναφερόμενα ποινικά αδικήματα, τιμωρούνται οι πράξεις αντίστασης (αντίσταση κατά αστυνομικών, σωματική επίθεση σε αξιωματικούς επιβολής του νόμου)[108].

5.4 Ψηφιακή εκβίαση - Ransomware

5.4.1 Γενικές Πληροφορίες

Το ransomware είναι μια μορφή κακόβουλου λογισμικού (κακόβουλου προγράμματος) που κρατά ομήρους τα δεδομένα ή τον υπολογιστή ενός χρήστη και απαιτεί από τον χρήστη να πληρώσει ένα λύτρο (ransom) για να αποκαταστήσει την πρόσβαση στα δεδομένα ή τη συσκευή του και σχετίζεται με τα εγκλήματα του εκβιασμού, της παραποίησης δεδομένων και της δολιοφθοράς μέσω υπολογιστή. Ο τρόπος λειτουργίας του ransomware συνήθως περιλαμβάνει την κρυπτογράφηση των αρχείων του θύματος ή τον περιορισμό της πρόσβασης στον υπολογιστή του, και στη συνέχεια, οι επιτιθέμενοι απαιτούν και λαμβάνουν χρήματα για την αποκρυπτογράφηση των δεδομένων ή την αποκατάσταση της πρόσβασης[109] [110].

Υπάρχουν διάφορα είδη ransomware, αλλά τα κυριότερα είδη είναι τα εξής:

---

[108] Εφημερίδα Frankfurter Allgemeine Sonntagszeitung (2020), https://abo.faz.net/frankfurter-allgemeine-sonntagszeitung/fas.html?dwvar_fas_medium=FAP_DGT&dwvar_fas_referencePeriodicityGroup=SOABO&dwvar_fas_subscriptionType=REG_SX_PO&affiliate=IP23015&pac=IP23015&pacmedium=FAP_DGT&campID=SEA_BG-BM_PERF_PAY_FAS-FAP_DGT_ABO_SO_REG_UN_PO_standard_IP23015&campaign=_BG-BM_&campID=SEA_BG-BM&s_kwcid=AL!9053!3!463549399339!b!!g!!frankfurter%20allgemeine%20sonntagszeitung%20online&gclid=Cj0KCQjwl8anBhCFARIsAKbbpyR_-PfOxgqyv7SDsPKeAq1HubULjC5x4ZicR-8MtIQ6Zp-_mK5eHREaArtUEALw_wcB.

[109] Microsoft Support, https://support.microsoft.com/el-gr/windows/%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1-%CF%84%CE%BF%CF%85-%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE-%CF%83%CE%B1%CF%82-%CE%B1%CF%80%CF%8C-%CF%84%CE%BF-ransomware-08ed68a7-939f-726c-7e84-a72ba92c01c3.

[110] Writers S. (2022), https://www.crn.com.au/feature/ransomware-protection-has-become-a-critical-channel-upsell-583756.

- Encrypting Ransomware: Αυτό το είδος κρυπτογραφεί τα αρχεία του θύματος με ένα ισχυρό κρυπτογραφικό αλγόριθμο. Οι χρήστες δεν μπορούν πλέον να ανοίξουν τα αρχεία τους μέχρι να πληρώσουν τα λύτρα ώστε να λάβουν το κλειδί αποκρυπτογράφησης.

- Locker Ransomware: Αυτό το είδος κλειδώνει την πρόσβαση του χρήστη στον υπολογιστή του, εμποδίζοντας τον από την είσοδο στο λειτουργικό σύστημα ή τα αρχεία του. Στη συνέχεια, ζητά αντίτιμο για να ελευθερώσει την πρόσβαση.

- Scareware Ransomware: Αυτό το είδος παρουσιάζει ψευδείς κινδύνους ή προβλήματα στον υπολογιστή του θύματος και ζητά την πληρωμή για την απομάκρυνσή τους, αν και οι απειλές είναι φανταστικές.

- Leakware (Doxware): Αυτό το είδος απειλεί ότι θα δημοσιεύσει προσωπικά δεδομένα του θύματος στο διαδίκτυο αν δεν πληρώσει το λύτρο. Στόχος είναι η εξαναγκασμένη πληρωμή για να μην διαρρεύσουν ευαίσθητες πληροφορίες.

Τα συνηθέστερα μέσα επίθεσης αποτελούν τα μηνύματα ηλεκτρονικού ταχυδρομείου που φέρουν ως συνημμένο το κακόβουλο λογισμικό (υποτιθέμενα τιμολόγια, επιβεβαιώσεις παραγγελιών, αποδείξεις, σαρωμένα έγγραφα, χρησιμοποιώντας ακόμα και πραγματικά ονόματα και διευθύνσεις εταιρειών και σε τέλεια απομίμηση πραγματικών εταιρικών e-mail), ή οι μολυσμένοι ιστότοποι και τα διαφημιστικά banner, στα οποία ο χρήστης-θύμα οδηγείται επίτηδες από τον δράστη. Επίσης αξίζει να σημειωθεί ότι το 95% των επιθέσεων γίνεται με κρυπτογράφηση[111]. Από τον Δεκέμβριο του 2015 μέχρι και σήμερα, η Ομοσπονδιακή Υπηρεσία για την Ασφάλεια στην Τεχνολογία Πληροφορικής στην Γερμανία (Bundesamt für Sicherheit in der Informationstechnik - BSI) έχει καταγράψει τεράστιο αριθμό ανεπιθύμητων μηνυμάτων, τα οποία χρησιμοποιούνται για τη διάδοση ransomware σε μαζική κλίμακα[112].

Σε κάποια διαδικτυακά φόρουμ της παραοικονομίας, είναι δυνατό να αποκτηθεί κακόβουλο λογισμικό ή ακόμη και μια ολόκληρη υπηρεσία που εκτελεί δραστηριότητες ψηφιακής εκβίασης. Αυτό δίνει τη δυνατότητα σε άτομα που στερούνται ειδικών γνώσεων πληροφορικής να δημιουργήσουν ransomware χωρίς μεγάλη δυσκολία, χρησιμοποιώντας μία *"εργαλειοθήκη κακόβουλου λογισμικού"* (το λεγόμενο *"malware toolkit"*). Αυτή η υπηρεσία παρέχεται στο Darknet από το 2015 και επιτρέπει στους χρήστες, ακόμα και αρχάριους, να

[111] Wernert M. (2021), σελ. 221-222.
[112] BSI (2022), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html.

συνθέτουν δωρεάν ransomware με ελάχιστη προσπάθεια. Οι υπεύθυνοι της υπηρεσίας λαμβάνουν μια μερίδα από τα λύτρα αν η πληρωμή πραγματοποιηθεί με επιτυχία, συνήθως μέσω ψηφιακού νομίσματος όπως το Bitcoin. Αυτή η υπηρεσία παρέχει μια πλατφόρμα ελέγχου στον χρήστη, που του επιτρέπει να δει τις προκληθείσες μολύνσεις και να λάβει ο ίδιος το υπόλοιπο των λύτρων. Η διάδοση του ransomware γίνεται ανεξάρτητα από τον πελάτη, χρησιμοποιώντας μια πλατφόρμα που παρέχεται από τον προμηθευτή του κακόβουλου λογισμικού[113].

Ένα ζήτημα που αντιμετωπίζει η Γερμανία την τελευταία πενταετία είναι ότι γερμανικές εταιρείες λαμβάνουν διαρκώς αληθοφανή μηνύματα e-mail από υποτιθέμενους αιτούντες, τα οποία είναι γραμμένα προσεκτικά. Οι δράστες προσποιούνται ότι είναι αιτούντες και γράφουν απευθείας στη διοίκηση ή το τμήμα ανθρώπινου δυναμικού της εταιρείας. Στόχος είναι να μολυνθεί ο υπολογιστής της εκάστοτε εταιρείας με κακόβουλο λογισμικό που κρυπτογραφεί τα δεδομένα της. Στη συνέχεια, οι δράστες ζητούν χρηματικό αντάλλαγμα για να αποκρυπτογραφήσουν αυτά τα δεδομένα και να αποκαταστήσουν τη ζημία που οι ίδιοι προκάλεσαν. Οι φερόμενοι ως αιτούντες συνήθως εξηγούν στη διοίκηση ότι ενδιαφέρονται για την εταιρεία είτε ως επενδυτές είτε ως εργαζόμενοι και αποστέλλουν περαιτέρω πληροφορίες για τους εαυτούς τους, για παράδειγμα κάποιο υποτιθέμενο βιογραφικό, μέσω ενός *"συνδέσμου Dropbox"*[114] που περιέχεται ως συνημμένος στο e-mail. Ωστόσο, μόλις ο χρήστης ανοίξει τον σύνδεσμο, το κακόβουλο λογισμικό εγκαθίσταται μόνο του και κρυπτογραφεί αμέσως τα δεδομένα της εταιρείας στον υπολογιστή. Επιπλέον, γίνεται λήψη ενός αρχείου *"σημείωσης λύτρων"* με τίτλο: *"Your_files_are_encrypted.html"*. Σε αυτό, ο ενδιαφερόμενος καλείται να πληρώσει ένα ποσό χρησιμοποιώντας το ψηφιακό νόμισμα Bitcoin. Σε αντάλλαγμα, οι δράστες υπόσχονται να παράσχουν τις πληροφορίες που απαιτούνται για την αποκρυπτογράφηση των προηγουμένως κρυπτογραφημένων δεδομένων. Οι ειδικοί της Κρατική Εγκληματολογικής Αστυνομίας της Βάδης-Βυρτεμβέργης (Landeskriminalamt Baden-Württemberg - LKA) συμβουλεύουν έντονα να μην αποδέχονται οι χρήστες-θύματα την προσφορά των δραστών, ενώ προειδοποιούν διαρκώς για απόπειρες απάτης μέσω ψηφιακού εκβιασμού[115].

---

[113] Bundeslagebild, BKA (2016), https://www.bka.de/DE/Home/home_node.html.

[114] Το Dropbox είναι μια αμερικανική υπηρεσία φιλοξενίας αρχείων, που αποτελεί επίσης μέσο αποθήκευσης cloud, που παρέχεται από την Dropbox Inc.

[115] LKA Βάδης-Βυρτεμβέργης (2015), https://www.bw.ihk.de/_Resources/Persistent/007c94cdbec8d10dc845679526f3002e538b296b/M%C3%A4rz-Warnmeldung%20ZAC_sch%C3%A4dliche-E-Mail-Anh%C3%A4nge.pdf.

5.4.2 Μέτρα αντιμετώπισης

Τα μέτρα προστασίας απέναντι σε επιθέσεις ransomware μπορούν να χωριστούν σε τρεις κατηγορίες, ακολουθώντας η μία σειρά διαδοχής της μίας σε σχέση με την άλλη. Αυτές είναι πρόληψη, αναγνώριση, αντιμετώπιση.

5.4.2.1 Πρόληψη

Τα κυριότερα μέτρα πρόληψης, προκειμένου να προστατευθεί ο χρήστης από πιθανή επίθεση ransomware είναι:

➔ Ενημέρωση του λογισμικού με τις τελευταίες εκδόσεις και ενημερώσεις ασφαλείας. Οι ενημερώσεις συνήθως περιλαμβάνουν βελτιώσεις ασφαλείας που μπορούν να προστατέψουν από τα ransomware.

➔ Ασφαλείς ευκαιρίες περιήγησης και αποφυγή ύποπτων συνδέσμων, με παράλληλη χρήση αξιόπιστου προγράμματος περιήγησης.

➔ Αποφυγή και διαγραφή ύποπτων email και συνδέσμων ή συνημμένων σε αυτά αρχείων από άγνωστες πηγές. Επίσης, προσοχή στην ορθογραφία και τη γραμματική των μηνυμάτων, καθώς πολλά κακόβουλα email περιλαμβάνουν ορθογραφικά λάθη.

➔ Δημιουργία αντιγράφων ασφαλείας, ώστε να μπορέσει ο χρήστης να επαναφέρει τα δεδομένα του σε περίπτωση μόλυνσης από ransomware. Αποθήκευση των αντιγράφων ασφαλείας σε ασφαλείς τοποθεσίες, εκτός του κυρίως δικτύου.

➔ Εκπαίδευση και ενημέρωση των χρηστών να αναγνωρίζουν τα ύποπτα μηνύματα, τους κακόβουλους συνδέσμους και τις κακόβουλες συνημμένες αρχεία. Ενημέρωσή τους για τις βασικές αρχές ασφαλούς περιήγησης στο διαδίκτυο και την αποφυγή κακόβουλων λογισμικών.

5.4.2.2 Αναγνώριση

Είναι σημαντικό να μπορεί κανείς να αναγνωρίζει τα ransomware, ώστε να μπορέσει να αντιδράσει γρήγορα και να προστατευθεί από αυτά. Ορισμένες ενδείξεις μόλυνσης από ransomware περιλαμβάνουν:

➔ Αιφνίδια κρυπτογράφηση αρχείων, τα οποία ο χρήστης-κάτοχος δεν μπορεί να ανοίξει.

➔ Απειλητικά μηνύματα που ζητούν την πληρωμή αντιτίμου για την αποκρυπτογράφηση των αρχείων του χρήστη. Αυτά τα μηνύματα συνήθως

περιλαμβάνουν οδηγίες σχετικά με την πληρωμή και δίνουν περιορισμένο χρονικό περιθώριο για αυτήν.

➔ Αλλαγές στις επεκτάσεις αρχείων με την προσθήκη μιας μορφής κωδικοποίησης στο τέλος. Για παράδειγμα, ένα αρχείο με το όνομα *"document.docx"* μπορεί να μετατραπεί σε *"document.docx.encrypted"*.

5.4.2.3 Αντιμετώπιση

Εάν παρόλα αυτά μολυνθεί ένας χρήστης από ransomware, υπάρχουν ορισμένα βήματα που οφείλει να ακολουθήσει προκειμένου να αντιμετωπίσει την κατάσταση:

➔ Απομόνωση του υπολογιστή και αποσύνδεση από το δίκτυο για να αποτραπεί η μετάδοση του ransomware σε άλλες συσκευές.

➔ Απενεργοποίηση του συστήματος για να αποτροπή περαιτέρω ζημιών.

➔ Επαναφορά δεδομένων και αρχείων από αντίγραφα ασφαλείας, εφόσον είναι ενημερωμένα και ασφαλή.

➔ Σε περιπτώσεις σοβαρής μόλυνσης, μπορεί να κριθεί απαραίτητη η επανεγκατάσταση του λειτουργικού συστήματος για την πλήρη εξάλειψη του ransomware.

➔ Αναφορά της επίθεση ransomware στις αρμόδιες αρχές και στις εταιρείες ασφαλείας, ώστε να αντιμετωπιστεί η κατάσταση και να προειδοποιηθούν οι υπόλοιποι χρήστες.

5.5 Διακίνηση πρνογραφικού υλικού ανηλίκων

5.5.1 Γενικές πληροφορίες

Ως παιδική πορνογραφία ορίζεται η αναπαράσταση, με κάθε μέσο, ανήλικου που απεικονίζεται σε πραγματικές ή εικονικές γενετήσιες δραστηριότητες ή η απεικόνιση των γενετήσιων οργάνων παιδιού, για σεξουαλικούς ή και κερδοσκοπικούς σκοπούς. Χάριν ευκολίας, ταχύτητας και διατήρησης της ανωνυμίας τους, το κύριο μέσο καταγραφής και διάδοσης του συγκεκριμένου εγκλήματος, αποτελεί το διαδίκτυο[116].

Κατά του όρου παιδική πορνογραφία έχουν διατυπωθεί κατά καιρούς πολλές ενστάσεις, οι οποίες σχετίζονται με τον ανθρώπινο σεβασμό, τα δικαιώματα των παιδιών,

[116] Συμεωνίδου-Καστανίδου Ε. (2020), σελ. 317.

καθώς και τις κοινωνικές, ηθικές και νομικές πτυχές του θέματος. Πιο συγκεκριμένα, επειδή ο όρος *"παιδική πορνογραφία"* αναφέρεται σε αποτρόπαιες πρακτικές που εκμεταλλεύονται παιδιά, υποστηρίζεται ότι η χρήση του όρου μπορεί να μειώσει τον βαθμό σοβαρότητας του εγκλήματος και να απομακρύνει την προσοχή από τον πραγματικό χαρακτήρα της κατάχρησης των παιδιών και πως μπορεί να προκαλέσει συγκεκριμένες εικόνες στο μυαλό των ανθρώπων, ενώ θα έπρεπε να χρησιμοποιείται μια πιο κατηγορηματική και λιγότερο αποσπασματική έννοια για να περιγράφει τη σοβαρότητα του εγκλήματος. Επιπλέον, υποστηρίζεται ότι ο όρος *"παιδική πορνογραφία"* μπορεί να αδυνατίσει την εστίαση στο γεγονός ότι πρόκειται για εκμετάλλευση ανυπεράσπιστων παιδιών. Ορισμένοι προτείνουν τη χρήση όρων όπως *"παιδική σεξουαλική εκμετάλλευση"* για να αποδώσουν πιο ακριβώς τη φύση του προβλήματος. Συνέπεια της προβληματικής αυτής ήτα να συμπεριληφθεί ο όρος *"υλικό παιδικής κακοποίησης"* (απεικόνιση σεξουαλικής κακοποίησης παιδιών) στο σχέδιο Οδηγίας της ΕΕ για την κατάργηση της απόφασης-πλαίσιο 2004/68/ΔΙ[117].

Πράγματι, το διαδίκτυο διευκολύνει σε πολύ μεγάλο βαθμό την καταγραφή και ταχύτατη διακίνηση οποιουδήποτε περιεχομένου πολυμέσων άνευ τοπικού περιορισμού. Παράλληλα, τόσο ο διακινητής, όσο και ο χρήστης διατηρούν την ανωνυμία τους, προσφέροντας αυτό την αίσθηση της ασφάλειας. Το περιεχόμενο των παιδοσεξουαλικών εικόνων και του περιεχομένου ταινιών ποικίλει από εικόνες και βίντεο ερωτικού περιεχομένου μέχρι σε κατηγορία που απεικονίζει σαδιστικές πράξεις σε ανηλίκους[118]. Επομένως, ειδικότερα για τον χρήστη η ευκολία εύρεσης τέτοιου υλικού στο διαδίκτυο τού προσφέρει την αίσθηση του φυσιολογικού, απενοχοποιεί την πράξη, ενώ ταυτοχρόνως ο ίδιος μπορεί να έρθει σε επικοινωνία με *"ομοϊδεάτες"* του, χωρίς να πρέπει να βγει από το σπίτι και να αναζητήσει αντίστοιχο υλικό σε κάποιο εξωτερικό χώρο, εκτεθειμένος σε τρίτους.

Οι επαναλαμβανόμενες περιπτώσεις σοβαρής κακοποίησης παιδιών και η διάδοσή τους στο διαδίκτυο έχουν επηρεάσει τη δημόσια συζήτηση και τις εκκλήσεις προς τον νομοθέτη για αυστηροποίηση των ποινών.Το διαδίκτυο διαδραματίζει καταλυτικό ρόλο σε αυτόν τον τομέα των αδικημάτων. Η φινλανδική ΜΚΟ Protect the Children διεξήγαγε μία σημαντικότατη έρευνα σχετικά με την παιδική πορνογραφία σε δείγμα 5.000 ατόμων τα οποία είχαν εμπλακεί σε περιπτώσεις παιδικής πορνογραφίας. Το 70% αυτών δήλωσε ότι είχε έρθει σε επαφή με τέτοιο υλικό ήδη πριν από την ενηλικίωση. Ποσοστό 40% του συνολικού αριθμού των συμμετεχόντων είχε εκτεθεί, μάλιστα, σε τέτοιες εικόνες πριν από την ηλικία

[117] Wernert M. (2021), σελ. 195-196.
[118] Freeman – Longo R. E. (1989).

των 13 ετών. Το 50% ισχυρίστηκε ότι πρώτη φορά ήρθε σε επαφή με το υλικό αυτό τυχαία. Το 45% δήλωσε ότι είχε αναζητήσει μέσω του Dark Web *"πορνογραφία που αφορά κορίτσια ηλικίας 4 έως 13 ετών"* και το 18% για αγόρια. Το πιο ανησυχητικό είναι ότι το υπόλοιπο 37% δήλωσε ότι έχουν αναζητήσει *"σαδιστικό και βίαιο υλικό που αφορούσε μικρά παιδιά κάτω των δυόμισι ετών"*, ενώ το 33% των ερωτηθέντων δήλωσε ότι είχε προσπαθήσει να έρθει επαφή με κακοποιημένα παιδιά.

5.5.2 Νομοθετικό πλαίσιο

Η ανάγκη προστασίας των ανήλικων απέναντι στα εγκλήματα που σχετίζονται με τη πορνογραφία οδήγησε σταδιακά στην δημιουργία ενός νομικού πλέγματος προστασίας στο πλαίσιο του διεθνούς και ευρωπαϊκού δικαίου. Στις 20 Νοεμβρίου 1989 υπογράφηκε και κυρώθηκε από συνολικά 191 χώρες η Σύμβαση των Ηνωμένων Εθνών για τα Δικαιώματα του Παιδιού, η οποία προωθεί τα δικαιώματα και την προστασία των παιδιών, συμπεριλαμβανομένης της προστασίας από εκμετάλλευση και κακοποίηση, όπως η παιδική πορνογραφία.

Αργότερα, το 2000 υπογράφηκε στη Σύνοδο Κορυφής του ΟΗΕ το Πρωτόκολλο των *"Ηνωμένων Εθνών για την Προστασία των Παιδιών από την Εμπορία και την Εκμετάλλευση"*, γνωστό και ως *"Πρωτόκολλο για την Εμπορία Παιδιών"*. Συνιστά ένα συμπληρωματικό προς την *"Σύμβαση των Ηνωμένων Εθνών κατά του Οργανωμένου Εγκλήματος"* και την *"Σύμβαση των Ηνωμένων Εθνών κατά της Διεθνούς Εγκληματικότητας"* κείμενο, το οποίο εστιάζει σε διάφορες πτυχές που σχετίζονται με την εμπορία και εκμετάλλευση παιδιών, συμπεριλαμβανομένης της πορνογραφίας. Επίσης, περιλαμβάνει διατάξεις που ενθαρρύνουν τη συνεργασία μεταξύ των κρατών, την ανταλλαγή πληροφοριών και την παροχή βοήθειας σε θύματα.

Στις 25 Μαΐου 2000 υιοθετήθηκε στη Βιέννη η "*Σύμβαση των Ηνωμένων Εθνών κατά της Παράνομης Κατασκευής και Διανομής Υλικού Παιδικής Σεξουαλικής Εκμετάλλευσης"*, γνωστή και ως *"Πρωτόκολλο για την Πρόληψη, Κατανομή και Τιμωρία της Παράνομης Κατασκευής και Διανομής Υλικού Παιδικής Σεξουαλικής Εκμετάλλευσης"*. Αυτή η σύμβαση σχετίζεται με το Πρωτόκολλο κατά της Διεθνούς Εμπορίας Ανθρώπων, ειδικά γυναικών και παιδιών, το οποίο αποτελεί μέρος της Σύμβασης των Ηνωμένων Εθνών κατά του Διεθνούς Εγκλήματος και της Διεθνούς Εμπορίας Ναρκωτικών, της Παράνομης Διακίνησης Εμπορευμάτων και της Καταστροφής των Πολεμικών Εξοπλισμών.

Ένα από τα σημαντικότερα, ωστόσο, νομικά κείμενα που αφορούν στην καταπολέμηση της παιδικής πορνογραφίας στο διαδίκτυο αποτελεί η *"Σύμβαση του Συμβουλίου της Ευρώπης κατά του εγκλήματος μέσω του διαδικτύου"*, επίσης γνωστή ως *"Σύμβαση του Βουδαπέστης για τον Κυβερνοεγκληματικό Ρυθμιστικό Πλαίσιο"*, η οποία υπογράφηκε στη Βουδαπέστη στη στις 23 Νοεμβρίου 2001. Η Σύμβαση αυτή έχει ως στόχο την αντιμετώπιση των εγκλημάτων που διαπράττονται μέσω του διαδικτύου, όπως η διαδικτυακή απάτη, η παιδική πορνογραφία και άλλα. Η σύμβαση διαθέτει διάφορα μέτρα και προσαρμοσμένες νομοθετικές προτάσεις προκειμένου να ενισχυθεί η συνεργασία μεταξύ των χωρών μελών του Συμβουλίου της Ευρώπης στον τομέα του κυβερνοεγκλήματος. Συμπεριλαμβάνει μέτρα για την αναγνώριση, την έρευνα, τη δίωξη και την τιμωρία των κυβερνοεγκλημάτων.

Γενικότερα, στο πλαίσιο του ευρωπαϊκού δικαίου υπάρχουν πλείστα νομικά κείμενα που σχετίζονται με την καταπολέμηση της παιδικής πορνογραφίας στο διαδίκτυο. Ένα από αυτά είναι η απόφαση-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου ΕΕ της 22ας Δεκεμβρίου 2003, που σχετίζεται με την καταπολέμηση της σεξουαλικής εκμετάλλευσης των παιδιών και της παιδικής πορνογραφίας, εγκρίθηκε το 2004 και αποσκοπεί στην εναρμόνιση των νομοθεσιών των κρατών μελών της ΕΕ για την καταπολέμηση αυτών των εγκλημάτων, περιέχοντας διατάξεις που αφορούν τον ορισμό και την τιμωρία των ποινικών πράξεων που σχετίζονται με την παιδική πορνογραφία και τη σεξουαλική εκμετάλλευση παιδιών.

Ακόμα, το 2007 υπογράφηκε στην Ισπανία η *"Σύμβαση του Συμβουλίου της Ευρώπης για την Προστασία των Παιδιών από την Σεξουαλική Εκμετάλλευση και την Σεξουαλική Κακοποίηση",* γνωστή και ως *"Σύμβαση της Λάνζαροτ"*, η οποία αποτελεί μια σημαντική πρωτοβουλία για την προστασία των παιδιών από την σεξουαλική εκμετάλλευση και κακοποίηση. Είναι μια πρωτοβουλία του Συμβουλίου της Ευρώπης και προσεγγίζει αυτά τα ζητήματα με διασυνοριακό τρόπο, ζητώντας τη συνεργασία των χωρών μελών για την καταπολέμησή τους.

Επιπροσθέτως, η Οδηγία 2011/92/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 2011, που αφορά την καταπολέμηση της παιδικής πορνογραφίας και αντικαθιστά την Οδηγία 2003/20/ΕΚ, θεσπίζει μέτρα για την εναρμόνιση της νομοθεσίας των κρατών μελών της Ευρωπαϊκής Ένωσης σχετικά με την παιδική πορνογραφία. Στόχος της Οδηγίας αυτής είναι η πρόληψη και η καταπολέμηση της παιδικής πορνογραφίας, καθώς και η προστασία των παιδιών από την εκμετάλλευση σε αυτόν τον

τομέα. Η Οδηγία καθορίζει ορισμένες ποινές για την παραγωγή, διάθεση, απόκτηση, κατοχή και διανομή υλικού παιδικής πορνογραφίας, καθώς και την προσπάθεια να διαπράξει κάποιος αυτές τις πράξεις. Επιπλέον, η Οδηγία περιλαμβάνει διατάξεις για την συνεργασία μεταξύ των κρατών μελών, τη διαγραφή και την αποκατάσταση του υλικού παιδικής πορνογραφίας, καθώς και μέτρα για την προστασία των παιδιών που θύματα αυτών των εγκλημάτων και συνεισφέρει στη δημιουργία ενιαίου νομικού πλαισίου στην Ευρωπαϊκή Ένωση για την καταπολέμηση της παιδικής πορνογραφίας και την προστασία των παιδιών από αυτούς τους κινδύνους.

Ο πιο πρόσφατος Κανονισμός σχετικά με την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών είναι ο προτεινόμενος *"Κανονισμός της ΕΕ για τη θέσπιση κανόνων για την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών"* του 2022 γνωστός και ως *"Κανονισμός CSA (Child Sexual Abuse)"* ή *"CSAR (Child Sexual Abuse Regulation)"*. Το περιεχόμενο του Κανονισμού εγείρει έντονους προβληματισμούς, καθότι από πολλούς θεωρείται ασυμβίβαστος με τα θεμελιώδη δικαιώματα και τη νομολογία της ΕΕ, ίσως περισσότερο από οποιαδήποτε άλλη ευρωπαϊκή νομοθεσία. Ενώ όλοι οι ενδιαφερόμενοι συμφωνούν ότι η προστασία των παιδιών είναι σημαντική, όλες οι επίσημες νομικές και τεχνικές αξιολογήσεις κατέληξαν στο συμπέρασμα ότι οι προτεινόμενες ενέργειες θα μπορούσαν να οδηγήσουν σε υπερβολικές παραβιάσεις του ιδιωτικού απορρήτου, των προσωπικών δεδομένων και της ελευθερίας έκφρασης στο διαδίκτυο, καθώς βασίζονται σε τεχνικά ανέφικτα ή επικίνδυνα μέτρα.

Πιο συγκεκριμένα, προβλέπεται η διενέργεια ελέγχων σε συνομιλίες στο διαδίκτυο για την ανίχνευση απεικονίσεων σεξουαλικής βίας κατά παιδιών. Ο Κανονισμός για την πρόληψη της σεξουαλικής κακοποίησης παιδιών ορίζει ότι, μεταξύ άλλων, οι πάροχοι υπηρεσιών συνομιλίας πρέπει να πραγματοποιούν ελέγχους στα προσωπικά μηνύματα των χρηστών τους. Αυτό αφορά και τα κρυπτογραφημένα μηνύματα, στα οποία είτε θα γίνεται από την πλευρά του χρήστη, είτε η ίδια η κρυπτογράφηση θα πρέπει να σπάσει.

Τον Φεβρουάριο του 2023, ο επικεφαλής ευρωβουλευτής της Επιτροπής Εσωτερικής Αγοράς και Προστασίας των Καταναλωτών (IMCO) του Ευρωπαϊκού Κοινοβουλίου, Alex Saliba, κατέθεσε σχέδιο γνωμοδότησης για τον κανονισμό CSA. Αντί να απαιτήσει την πλήρη απόσυρση της προτεινόμενης νομοθεσίας, όπως ζήτησαν η EDRi και άλλες 130 μη κυβερνητικές οργανώσεις, ανέπτυξε προτάσεις για τροποποίησή του, με στόχο την επίτευξη θετικών και εποικοδομητικών βημάτων. Επιπρόσθετα, οι ευρωβουλευτές Hahn, Körner,

Kolaja, Konečná, Lacapelle και Bielan, εκπροσωπώντας 6 από τις 7 ευρωπαϊκές πολιτικές ομάδες, εξέφρασαν σαφώς την αντίθεσή τους προς οποιαδήποτε προσπάθεια υπονόμευσης της κρυπτογράφησης.

Επιπλέον, σε όλο το φάσμα των πολιτικών αντιλήψεων, οι ευρωβουλευτές που υπέβαλαν τροπολογίες επέστησαν την προσοχή στην ανάγκη περιορισμού των προτεινόμενων μέτρων προκειμένου να διασφαλιστούν τα θεμελιώδη δικαιώματα όλων των χρηστών του διαδικτύου. Πολλοί από αυτούς εξέφρασαν ρητά την ανησυχία τους για τον επιβλαβή χαρακτήρα των προτεινόμενων μέτρων και τη σημασία της προστασίας του δικαιώματος στην ιδιωτική ζωή και του απορρήτου των επικοινωνιών.

Πολλοί ευρωβουλευτές προχώρησαν ακόμη περισσότερο και υπέβαλαν τροπολογίες με στόχο τη μη υποχρεωτική εφαρμογή των μέτρων επαλήθευσης της ηλικίας. Αυτοί οι ευρωβουλευτές επεσήμαναν ότι η επαλήθευση ηλικίας δεν αποτελεί πάντα θετικό μέτρο και όταν χρησιμοποιείται, πρέπει να γίνεται με προσεκτικά μελετημένο, ελεγχόμενο τρόπο, προκειμένου να αποφεύγονται πιθανές επιπτώσεις στα πολύ νέα άτομα. Ο Κανονισμός επιδιώκει να προστατεύσει, όμως, οι ειδικοί επισημαίνουν ότι όλες οι υπάρχουσες τεχνολογίες επαλήθευσης ηλικίας έχουν σοβαρά ζητήματα όσον αφορά την προστασία των δεδομένων, την ακρίβεια και την πιθανή διάκριση, καθώς και τους κινδύνους της ψηφιακής αποκλειστικότητας για τους νέους χρήστες στο διαδίκτυο.

Ένα σημαντικό πρόβλημα που ανακύπτει είναι ότι ο νόμος φαίνεται να υιοθετεί μια υπερβολικά ευρεία προσέγγιση και μπορεί να περιορίζει υπέρμετρα τα δικαιώματα και τις ελευθερίες των απλών χρηστών του διαδικτύου. Αυτό μπορεί να έχει ως αποτέλεσμα την αντιμετώπιση τους ως ύποπτους εγκληματίες, χωρίς να λαμβάνεται υπόψη η ανάγκη διαφύλαξης των δικαιωμάτων τους και της ελευθερίας τους στον ψηφιακό χώρο. Είναι σημαντικό να εξετάζονται τα μέτρα που λαμβάνονται προκειμένου να διασφαλιστεί ότι δεν υπάρχει υπερβολική παρέμβαση στα δικαιώματα και τις ελευθερίες των χρηστών, καθώς και να εξασφαλίζεται η συμμόρφωση με τα θεμελιώδη δικαιώματα. Η ισορροπία μεταξύ της ανάγκης προστασίας από εγκληματικές δραστηριότητες στο διαδίκτυο και του σεβασμού των προσωπικών ελευθεριών είναι πρωταρχικής σημασίας για τη διαμόρφωση της νομοθεσίας σε αυτόν τον τομέα.

Επιπροσθέτως, ο ευρωβουλευτής των Πράσινων Kolaja προέβη σε σημαντικές ενέργειες παρουσιάζοντας περισσότερες από 50 τροπολογίες προκειμένου να αναθεωρηθούν οι *"εντολές εντοπισμού"* που θεωρούνται υπερβολικές. Ο στόχος ήταν η αντικατάστασή τους

με πιο περιορισμένες και στοχευμένες *"εντολές έρευνας"*. Αυτές οι εντολές έρευνας εφαρμόζονται μόνο όταν υπάρχει πραγματική υποψία εγκληματικής δραστηριότητας, αντί να εφαρμόζονται σε εκτεταμένα τμήματα του πληθυσμού χωρίς εύλογη αιτία. Αυτή η προσέγγιση βοηθά στην διασφάλιση της ισορροπίας μεταξύ της ανάγκης για ασφάλεια και του σεβασμού των προσωπικών ελευθεριών και της ιδιωτικής ζωής των ανθρώπων. Αντί να υποβάλλονται σε μαζικούς ελέγχους και εντοπισμούς, οι χρήστες του διαδικτύου θα υφίστανται περιορισμένες παρεμβάσεις μόνο όταν υπάρχουν συγκεκριμένοι λόγοι που δικαιολογούν την ενέργεια αυτή.

Πράγματι, η διατήρηση της ισορροπίας μεταξύ της προστασίας της ιδιωτικής ζωής και της ασφάλειας στο διαδίκτυο είναι κρίσιμης σημασίας. Η πρόταση νόμου που υπονομεύει την ιδιωτική ζωή και επιτρέπει τη γενική και αδιάκριτη επεξεργασία μεταδεδομένων για ηλεκτρονικές επικοινωνίες θα μπορούσε να αποτελέσει ανησυχητική προηγούμενη για άλλες νομοθετικές προσπάθειες που αφορούν την προστασία των πολιτών από τις πλατφόρμες που συλλέγουν δεδομένα για εμπορικούς ή παρακολουθησιακούς σκοπούς. Επιπλέον, η γενική και αδιάκριτη επεξεργασία μεταδεδομένων για ηλεκτρονικές επικοινωνίες θα ήταν σε αντίθεση με τις αποφάσεις του Δικαστηρίου που αφορούν τη διατήρηση δεδομένων, οι οποίες έχουν καθορίσει όρια και προϋποθέσεις για τη συλλογή και αποθήκευση δεδομένων που αφορούν τις επικοινωνίες. Αυτό το ευρύ φάσμα διατήρησης και επεξεργασίας μεταδεδομένων χωρίς σαφείς περιορισμούς θα μπορούσε να δημιουργήσει σοβαρά ζητήματα προστασίας της ιδιωτικής ζωής και ασφάλειας των δεδομένων των πολιτών.

Όπως εύκολα μπορεί κανείς να διαπιστώσει, ιδιαίτερα στην Ευρωπαϊκή Ένωση, η προστασία των ανηλίκων από εγκλήματα σχετιζόμενα με την παιδική πορνογραφία στο διαδίκτυο είναι ένα ζήτημα που έχει απασχολήσει πολύ τα κράτη-μέλη, ενώ η ανάγκη διασυνοριακής συνεργασίας για την καταπολέμησή τους είναι αντιληπτή. Για τον λόγο αυτό, πέραν των σχετικών νομικών κειμένων, στην Ευρώπη υπάρχει το Ευρωπαϊκό Δικαστικό Δίκτυο (EJN) για το Ποινικό Δίκαιο και το Ποινικό Δίκαιο, το οποίο αποτελεί μια δομή συνεργασίας μεταξύ των κρατών-μελών για την διευκόλυνση της ανταλλαγής πληροφοριών και συνεργασίας σε θέματα ποινικού δικαίου. Το EJN δραστηριοποιείται με σκοπό την βελτίωση της διασυνοριακής συνεργασίας μεταξύ των δικαστικών αρχών των κρατών μελών και την ενίσχυση της εφαρμογής του ποινικού δικαίου σε ευρωπαϊκό επίπεδο και διευκολύνει την ανταλλαγή πληροφοριών και τη συνεργασία μεταξύ των δικαστικών αρχών των κρατών μελών σε θέματα όπως η έκδοση και η παράδοση καταδικασθέντων, η συνεργασία σε

έρευνες και ποινικές διώξεις, η ανταλλαγή πληροφοριών σχετικά με την ποινική νομοθεσία και την επικοινωνία μεταξύ των δικαστικών αρχών για την αποτελεσματικότερη επίλυση ποινικών υποθέσεων. Το EJN διαδραματίζει σημαντικό ρόλο στην προώθηση της διασυνοριακής συνεργασίας στον τομέα του ποινικού δικαίου και στη διευκόλυνση της εφαρμογής του ποινικού δικαίου στην ευρωπαϊκή νομοθεσία.

Ακόμα, το 1990 ιδρύθηκε το Ευρωπαϊκό Κέντρο Κατά της Παιδικής Σεξουαλικής Εκμετάλλευσης (ECPAT), μια μη κερδοσκοπική οργάνωση που ασχολείται με την καταπολέμηση της παιδικής σεξουαλικής εκμετάλλευσης και παιδικής πορνογραφίας, η οποία αποτελεί έναν από τους σημαντικότερους παράγοντες παγκοσμίως για την προστασία των παιδιών από την σεξουαλική εκμετάλλευση. Στόχος είναι να προάγει την καταπολέμηση της παιδικής σεξουαλικής εκμετάλλευσης μέσω της ενημέρωσης, της εκπαίδευσης, της έρευνας και της δράσης, συνεργαζόμενη με κυβερνήσεις, μη κυβερνητικές οργανώσεις, κατ' ιδίαν τομείς και άλλους φορείς για την αντιμετώπιση του προβλήματος της παιδικής σεξουαλικής εκμετάλλευσης, ενώ παράλληλα επιδιώκει την αυξημένη ευαισθητοποίηση του κοινού, των κυβερνήσεων και των οργανισμών για την προστασία των παιδιών από την παιδική σεξουαλική εκμετάλλευση, καθώς και την προώθηση της δημιουργίας και εφαρμογής αποτελεσματικών νομικών, κοινωνικών και πολιτικών μέτρων για την πρόληψη και την καταπολέμηση του προβλήματος.

5.5.2.1 Στην Ελλάδα

Στην Ελλάδα με το Ν. 3064/2002 εισήχθη στην ελληνική νομοθεσία το άρθρο 348Α ΠΚ, στο οποίο τυποποιείται για πρώτη φορά το έγκλημα της παιδικής πορνογραφίας, σε μία προσπάθεια εναρμόνισης του εγχώριου δικαίου με τις διατάξεις τη Σύμβαση του ΟΗΕ της 21.3.1950, τη Διεθνή Σύμβαση Εργασίας, άρ. 182, που κυρώθηκε με το Ν 2918/2001, τη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο (Βουδαπέστη 23.11.2001), τη Σύσταση R 1996/(1099) της Επιτροπής Υπουργών προς τα κράτη –μέλη της Ε.Ε, για τη σεξουαλική εκμετάλλευση των παιδιών, τη Σύσταση R 2000 (11) για κοινή δράση εναντίον της εμπορίας ανθρώπων για σεξουαλική εκμετάλλευση, τη Σύσταση R 2001 (16) για την προστασία των παιδιών από τη σεξουαλική εκμετάλλευση, την Απόφαση-Πλαίσιο του Συμβουλίου της Ε.Ε. για την καταπολέμηση της εμπορίας ανθρώπων (Επίσημη Εφημερίδα 27.2.2001) και την Απόφαση – Πλαίσιο για την καταπολέμηση της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας (Επίσημη Εφημερίδα 27.2.2001).

Αρχικά, με την διάταξη αυτή τιμωρούνταν όποιος με σκοπό το κέρδος παρήγαγε, κατείχε, διακινούσε, μετέφερε, προμηθευόταν ή αγόραζε υλικό πορνογραφικοού περιεχομένου με ανηλίκους. Στη συνέχεια, με τον Ν. 3625/2007 ο όρος της κερδοσκοπίας εξαλείφθηκε και το αξιόποινο της πράξης συνδέθηκε με την καθεαυτή ύπαρξη υλικού με πορνογραφικό περιεχόμενο, όπως ισχύει και σήμερα[119], ενώ με τον Ν. 3727/2008 κυρώθηκε η Σύμβαση του Συμβουλίου της Ευρώπης για την προστασία των παιδιών κατά της γενετήσιας εκμετάλλευσης και κακοποίησης[120].

Πιο συγκεκριμένα, σήμερα η διάταξη του άρθρου 348Α παρ. 1 ΠΚ έχει κωδικοποιηθεί ως εξής: *"Όποιος με πρόθεση παράγει, διανέμει, δημοσιεύει, επιδεικνύει, εισάγει στην Επικράτεια ή εξάγει από αυτήν, μεταφέρει, προσφέρει, πωλεί ή με άλλον τρόπο διαθέτει, αγοράζει, προμηθεύεται, αποκτά ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει ή μεταδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή."*.

Στην παράγραφο 2 του εν λόγω άρθρου ο ποινικός νομοθέτης αντιλαμβανόμενος το σημαντικό ρόλο των ηλεκτρονικών συστημάτων και του διαδικτύου στην τέλεση του εγκλήματος αυτού, στοιχειοθέτησε ένα υπαλλακτικώς μικτό έγκλημα το οποίο τιμωρείται σε αυτήν την περίπτωση βαρύτερα με ποινή φυλάκισης τουλάχιστον δύο ετών και χρηματική ποινή και αφορά στην τέλεση των παραπάνω πράξεων, μέσω πληροφοριακών συστημάτων. Ως πληροφοριακά συστήματα νοούνται, κατά βάση, οι ηλεκτρονικοί υπολογιστές και το διαδίκτυο, ενώ, συγχρόνως, ο νομοθέτης απαριθμεί αρκετά αναλυτικά τους τρόπους τέλεσης του εγκλήματος μέσω των συστημάτων πληροφορικής[121].

Ζήτημα, ωστόσο, ανέκυψε με οριοθέτηση του σημασιολογικού περιεχομένου του όρου της κατοχής σε σχέση με τα πληροφοριακά συστήματα, δεδομένου ότι εν προκειμένω το αντικείμενο δεν αφορά μόνο τον υλικό φορέα αλλά και το ψηφιακό περιεχόμενο[122], με αποτέλεσμα την δημιουργία δύο αποκλινουσών απόψεων. Σύμφωνα με την πρώτη, κατοχή πορνογραφικού υλικού υφισταται μόνο όταν υπάρχει φυσική κυριαρχία του δράστη στον υλικό φορέα των δεδομένων, υπό την απαραίτητη προϋπόθεση της γνώση και φυσικής βούλησης του δράστη για σταθερή ενσωμάτωση του περιεχομένου στον συγκεκριμένο υλικό φορέα του και της άσκησης πραγματικής εξουσίασης σε αυτόν[123]. Σύμφωνα με τη δεύτερη

[119] Ορφανός Σ. (2022),σελ. 50.
[120] Παρασκευόπουλος Ν./ Φυτράκης Ε. (2021), σελ 359.
[121] Συκιώτη Α./ Παπαγεωργίου-Γονατάς, Στ. Άρθρο 348Α ΠΚ σε: Χαραλαμπάκης, Α. (2021), σελ.2587 επ.
[122] Κουράκης Ν.Ε. (2012), σελ. 14 επ.
[123] Eckstein K. (2001), σελ. 122-125.

άποψη, η αξιόποινη κατοχή ηλεκτρονικών πορνογραφικών δεδομένων δεν υπάρχει μόνο στην περίπτωση εξουσίας του υλικού φορέα αποθήκευσης του αρχείου, αλλά και στη συλλογή και σταθερή ενσωμάτωσή του σε ξένο υλικό φορέα, με δυνατότητα ανεμπόδιστης πρόσβασης στο περιεχόμενό του και διάθεσής του[124].

Τέλος, στην έκτη παράγραφο, σύμφωνα με την οποία τιμωρείται με ποινή φυλάκισης έως τριών ετών η εν γνώσει πρόσβαση του δράστη σε υλικό παιδικής πορνογραφίας μέσω πληροφοριακών συστημάτων. Προστήθεται επομένως η ειδικότερη περίπτωση κατά την οποία ο δράστης ενεργεί με άμεσο δόλο α' βαθμού, ως προς την αναζήτηση του σχετικου υλικού, αποβλέποντας στην κατοχή του. Δεν αρκεί, επομενώς η απλή ή τυχαία επίσκεψη σε μια ιστοσελίδα με τέτοιο περιεχόμενο, χάριν προστασίας της ελεύθερης χρήσης του διαδικτύου[125].

5.5.2.2 Στη Γερμανία

Στο γερμανικό ποινικό δίκαιο, η διανομή, απόκτηση και κατοχή παιδικού πορνογραφικού περιεχομένου ποινικοποιείται στο άρθρο 184b StGB. Αξίζει να σημειωθεί, ότι σε σχέση με την έννοια της κατοχής η θεωρία φαίνεται ακόμα και σήμερα να ερμηνεύει τον όρο ως την πραγματική κυριαρχία επί του υλικού φορέα των δεδομένων[126].

Παράλληλα, μέχρι το 2015 η μέγιστη ποινή εγκλήματος σχετικού με τη παραγωγή ή διακίνηση τέτοιου υλικού ήταν δύο χρόνια φυλάκισης. Τον Ιανουάριο του 2014 ήρθε στο προσκήνιο η *"υπόθεση Edathy"*, ύστερα από έρευνες εναντίον του πολιτικού του SPD Sebastian Edathy. Η έρευνα αφορούσε την υποψία ότι ο Edathy είχε προμηθευτεί παράνομα σχετικό παιδικό πορνογραφικό υλικό[127]. Η υπόθεση εξελίχθηκε όπως ήταν αναμενόμενο σε κυβερνητική κρίση, με συνέπεια την καταστροφή της πολιτικής καριέρας του Edathy, ο οποίος, ωστόσο, δεν καταδικάστηκε[128]. Αποτέλεσμα όλου αυτού ήταν η σταδιακή αυστηροποίηση των διατάξεων του ποινικού κώδικα σχετικά με την παιδική πορνογραφία.

---

[124] Κιούπης Δ. (2007), στο Ιωαννίδου Α. (2007), σελ. 10.
[125] Συκιώτη Α./ Παπαγεωργίου-Γονατάς, Στ. Άρθρο 348Α ΠΚ σε: Χαραλαμπάκης, Α. (2021), σελ.2587 επ.
[126] Μπούρμπας Γ. (2016), http://crime-in-crisis.com/category/%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1-%CE%BA%CE%B1%CE%B9-%CE%BA%CF%81%CE%AF%CF%83%CE%B7/.
[127] Spiegel online (2014), https://www.spiegel.de/politik/deutschland/sebastian-edathy-filmbestellung-war-falsch-aber-legal-a-1009190.html.
[128] Florian Gathmann, Philipp Wittrock (2014), https://www.spiegel.de/politik/deutschland/kinderporno-ermittlungen-fall-edathy-bringt-friedrich-und-spd-in-not-a-953314.html.

Έτσι, πλέον για την κατοχή παιδικής πορνογραφίας προβλέπεται μέγιστη ποινή φυλάκισης έως και δέκα ετών. Εκτός από την πιθανή φυλάκιση, υπάρχουν και επαγγελματικές συνέπειες, όπως η ανάκληση της ιδιότητας του δημοσίου υπαλλήλου ή η απαγόρευση εργασίας.

.Επιπλέον, προκειμένου να ενισχυθεί η προστασία των παιδιών και επειδή ο νομοθέτης είχε πολύ περιορισμένες εξουσίες σχετικά με την παραγωγή και χρήση υλικού παιδικής πορνογραφίας που δημιουργείται από υπολογιστή για τη διενέργεια ποινικών ερευνών, θεσπίστηκε εξαίρεση σχετικά με την διάδοση και παραγωγή υλικού παιδικής πορνογραφίας κατά την ποινική δίωξη. Συγκεκριμένα, από τις 13 Μαρτίου 2020, η διάδοση και παραγωγή παιδικής πορνογραφίας παραμένει ατιμώρητη στην Γερμανία, εάν δημιουργήθηκε τεχνητά για επίσημες ενέργειες στο πλαίσιο ποινικών ερευνών (άρθρο 184β, παρ. 5, πρόταση 2 StGB), καθώς επίσης υπάρχει πλέον συγκεκριμένη ποινική δικονομική διαδικασία αδειοδότησης από το δικαστήριο, ή σε περίπτωση επικείμενου κινδύνου έγκρισης της εισαγγελικής αρχής. Σύμφωνα με το ως άνω άρθρο 110d StPO, το μέτρο πρέπει να τερματιστεί εάν το δικαστήριο δεν συμφωνήσει εντός τριών εργάσιμων ημερών. Η συγκατάθεση πρέπει να δίνεται γραπτώς και να είναι περιορισμένη[129].

5.5.3 Βάσεις δεδομένων κατακερματισμού

Ένα ακόμα ζήτημα που δυσχεραίνει την προστασία των ανηλίκων απέναντι στα εγκλήματα αυτά, είναι η ευκολία που χαρακτηρίζει, κατά κανόνα, τα ηλεκτρονικά εγκλήματα, τόσον όσον αφορά στην τέλεση, όσο και στην διάδοσή τους, και δη τα κυβερνοεγκλήματα, καθότι προσφέρεται στους έμπειρους δράστες το πλεονέκτημα ότι, με τα κατάλληλα εργαλεία, μπορούν να καλύψουν τα ίχνη τους. Ωστόσο, οι διαδικασίες που υποστηρίζονται από ψηφιακή τεχνολογία συνήθως καταγράφονται πολλάκις στο λειτουργικό σύστημα που χρησιμοποιείται. Επίσης, η γνώση ότι ορισμένες δραστηριότητες μπορεί να έχουν σκοπίμως αποκρυφθεί μπορεί επίσης να συμβάλει στην κατάλληλη αξιολόγηση της υπόθεσης[130].

Έτσι, τυχόν υποψίες για την τέλεση εγκλήματος σχετικού με την παιδική πορνογραφία μπορούν να διαπιστωθούν μέσω ειδικής βάσης δεδομένων για αυτοματοποιημένες συγκρίσεις. Με τη χρήση κατάλληλου λογισμικού επεξεργασίας των δεδομένων και την αξιολόγησή τους από τον υπεύθυνο τεχνικό εξέτασης και ανάλυσης των

[129] Νόμος για την τροποποίηση του γερμανικού Ποινικού Κώδικα (και του Κώδικα Ποινικής Δικονομίας) - Versuchsstrafbarkeit des Cybergroomings vom 03.03.2020 (BGBl. I S. 431).
[130] Stewen M. (2008).

πειστηρίων επιτυγχάνεται η στοχευμένη αξιολόγησή τους και ο περιορισμός των δεδομένων, προκειμένου ο αρμόδιος ο ανακριτής ή δικαστής να μην χρειάζεται να αντιμετωπίσει πληθώρα δεδομένων, π.χ. βίντεο, εικόνων κ.α., άσχετων με την συγκεκριμένη υπόθεση. Αυτός είναι ο μόνος τρόπος επιλογής και μείωσης του όγκου δεδομένων, έτσι ώστε να μειωθεί το ποσοστό της μη αυτόματης αξιολόγησης[131].

Στην Γερμανία υπάρχει ήδη μια εθνική βάση δεδομένων, η λεγόμενη *"βάση δεδομένων κατακερματισμού πορνογραφικού υλικού (Hashwerte Datenbank pornografische Schriften - HashDB PS)"*. Αυτή αφορά στη συλλογή, από την Ομοσπονδιακή Αστυνομία Εγκλημάτων (BKA), των τιμών κατακερματισμού όλων των γνωστών αρχείων πορνογραφικού περιεχομένου με παιδιά και νέους. Για κάθε πορνογραφικου περιεχομένου αρχείο υπολογίζεται, από τα Ομοσπονδιακά κρατίδια, ένας αλφαριθμητικός κωδικός, η λεγόμενη τιμή κατακερματισμού, η οποία είναι μοναδική και αποτελεί την ταυτότητά του, ένα ιδιαίτερο ψηφιακό δακτυλικό αποτύπωμα. Στη συνέχεια, η τιμή αυτή καταγράφεται μέσω μιας ψηφιακής πύλης στην βάση δεδομένων, ώστε να είναι προσβάσιμο στην BKA. ΜΕ τον τρόπο αυτό, το εξεταζόμενο υλικό μιας έρευνας ή το νέο υλικό που εισέρχεται μπορεί να συγκριθεί άμεσα με τις καταγεγραμμένες τιμές κατακερματισμού της βάσης δεδομένων. Με τον τρόπο αυτό, αρχεία καταγεγραμμένα στην βάση δεδομένων αναγνωρίζονται αυτόματα, χωρίς να χρειάζεται η χειροκίνητη προβολή και διαλογή τους. Πέραν της επιτάχυνσης και βελτιστοποίησης των διαδικασιών αξιολόγησης ψηφιακών αποδεικτικών στοιχείων, η εν λόγω πρακτική διευκολύνει την ανάπτυξη της συντονισμένης δράσης μεταξύ των ομοσπονδιακών κρατιδίων και της ομοσπονδιακής κυβέρνησης[132] [133].

5.5.4 Γραφεία πρόνοιας νέων

Στην Γερμανία, έχουν συσταθεί υπηρεσίες υποστήριξης νέων, τα λεγόμενα γραφεία πρόνοιας νέων. Σύμφωνα με την ενότητα 8α του Βιβλίου VIII του Κοινωνικού Κώδικα (Sozialgesetzbuch - SGB), τα γραφεία πρόνοιας νέων διαδραματίζουν σημαντικό ρόλο όσον αφορά στις καταγγελίες εγκλημάτων κατά της γενετήσιας ελευθερίας, καθώς υποχρεούνται να ενημερώνουν τις αρμόδιες αρχές, όταν διαπιστώνονται συγκεκριμένες ενδείξεις

[131] Δαλακούρας Θ. (2023), σελ. 73-83.
[132] Υπουργείο Εσωτερικών Β. Ρηνανίας-Βεστφαλίας, ετήσια έρευνα 2020, https://www.im.nrw/system/files/media/document/file/abschlussberichtkipost.pdf, σελ. 25-27.
[133] LKA Βάδης-Βυρτεμβέργης (2016),https://im.baden-wuerttemberg.de/de/service/publikation/did/cybercrimedigitale-spuren.

σεξουαλικής κακοποίησης, σωματικής κακοποίησης ή βλάβης σε βάρος ανηλίκου, ώστε να μπορέσουν οι αρχές να κινηθούν ταχύτερα[134].

Στο πλαίσιο καταπολέμησης των εγκλημάτων κατά της γενετήσιας ελευθερίας των ανηλίκων, το Υπουργείου Παιδιών, Οικογένειας, Ένταξης και Μετανάστευσης θεωρεί την τακτική ανταλλαγή πληροφοριών μεταξύ των υπηρεσιών ενός κράτους, ειδικότερα ενός ομοσπονδιακού κράτους, βασικό δομικό στοιχείο για την έγκαιρη διαπίστωση τέλεσης της εκάστοτε αξιόποινης πράξης και την πρόληψη της θυματοποίησης και αποβλέπει στην ενίσχυση του τομέα αυτού στις υπηρεσίες πρόνοιας νέων, με την θέσπιση και μονιμοποίηση υπαλλήλων αρμοδίων αποκλειστικά για τα θέματα αυτά.

5.5.5 Μέτρα αντιμετώπισης

➔ Η εξάλειψη παράνομων ηλεκτρονικών σελίδων, η οποία μπορεί να επιτευχθεί μέσω της επιβολής σαφών κανόνων πρακτικής που θα απαγορεύουν στους χρήστες του διαδικτύου να αποδέχονται συνειδητά παράνομο περιεχόμενο στις ηλεκτρονικές σελίδες και να τις διαγράφουν όταν ενημερώνονται για την ύπαρξή του.

➔ Η δημιουργία ηλεκτρονικών πλατφορμών διαμαρτυρίας και *"καυτών ζωνών"*, με τη δημιουργία ενός ψηφιακού χώρου όπου οι χρήστες μπορούν να καταγγείλουν παράνομες πράξεις, ερχόμενοι σε επικοινωνία με εταιρείες παροχής ηλεκτρονικών υπηρεσιών για τη διαβίβαση των καταγγελιών στις αρμόδιες αρχές.

➔ Η δημιουργία βάσεων δεδομένων κατακερματισμού, αντίστοιχο με αυτό της Γερμανίας, με σκοπό την βελτιστοποίηση και επιτάχυνση της διαδικασίας αξιολόγησης πειστηρίων και τις συνθήκες, όχι μόνο της εγχώριας, αλλά και της διακρατικής συνεργασίας, για την αντιμετώπιση εγκλημάτων σχετιζόμενων με την παιδική πορνογραφία.

➔ Η χρήση βαλβίδων αποκλεισμού κατά την περιήγηση στο διαδίκτυο, με τον εντοπισμό ύποπτων λέξεων-κλειδιών ή με την χρήση ειδικού λογισμικού-software.

➔ Η καταγραφή των στοιχείων των καταναλωτών υπηρεσιών του διαδικτύου για ερευνητικούς, ανακριτικούς και εγκληματολογικούς σκοπούς

➔ Η φραγή πιστωτικών καρτών από τις εταιρείες χορήγησής τους όταν διαπιστώνεται η αγορά πορνογραφικού υλικού.

---

[134] Υπουργείο Εσωτερικών Β. Ρηνανίας-Βεστφαλίας, ετήσια έρευνα 2020, https://www.im.nrw/system/files/media/document/file/abschlussberichtkipost.pdf, σελ. 24-25.

➔ Η θέσπιση κανόνων συμπεριφοράς στον εργασιακό χώρο και η επιβολή ποινών, παραδείγματος χάριν προστίμων, σε περιπτώσεις κακής ή ακατάλληλης χρήσης ηλεκτρονικών υπολογιστών από τους εργαζόμενους και η εφαρμογή ειδικών φίλτρων περιορισμού πρόσβασης σε ηλεκτρονικές ιστοσελίδες από τους υπαλλήλους.

➔ Η ενημέρωση και ενθάρρυνση του κοινού, κυρίως των γονέων, για τη χρήση λογισμικών φιλτραρίσματος και μηχανών εξιχνίασης παιδικής πορνογραφίας, για την αποτελεσματικότερη επίβλεψη και έλεγχο των ιστοσελίδων που επισκέπτονται οι ανήλικοι χρήστες.

➔ Η ενθάρρυνση του κοινού για καταγγελία στις αρμόδιες αρχές περιστατικών παιδικής πορνογραφίας, ώστε να μέσω των μεθόδων της ανάκρισης και της δικαστικής έρευνας, να αντληθούν πληροφορίες για την διαδικτυακή παιδική πορνογραφία από τους χρήστες, τους επειρογνώμονες τεχνικούς ηλεκτρονικών υπολογιστών και τα θύματα.

➔ Η ενημέρωση του κοινού σχετικά με την ορθή καταγραφή αποδεικτικών στοιχείων και τη μη αλλοίωσή τους, στην περίπτωση που υποπέσει στην αντίληψή τους σχετικό παράνομο υλικό: καταγραφή ημερομηνίας, δημιουργία αντιγράφου ασφαλείας των δεδομένων (π.χ. στιγμιότυπα οθόνης), καταγραφή διεύθυνσης ιστοτόπου όπου βρέθηκε το περιεχόμενο κ.α. Σε κάθε περίπτωση, θα πρέπει να τηρούνται οι κατευθυντήριες γραμμές της τοπικής εισαγγελίας σχετικά με την πιθανή ποινική ευθύνη του καταγγέλλοντος.

5.6 Παραβιάσεις πνευματικών δικαιωμάτων

5.6.1 Γενικές Πληροφορίες

Λόγω της συνεχούς εξέλιξης της τεχνολογίας και της εκτεταμένης χρήσης του διαδικτύου, όλο και περισσότερα προϊόντα πνευματικής ιδιοκτησίας εκτίθενται σε αυξημένη έκθεση και πολλαπλές προβολές και επεξεργασία με πλείστους νέους τρόπους. Αυτό έχει ως αποτέλεσμα τα πνευματικά δικαιώματα του δημιουργού ενός έργου να προσβάλλονται μέσω του διαδικτύου και επομένως να χρήζουν προστασίας. Ως προς την έννοια της προσβολής, προσβολή νοείται κάθε πράξη που επεμβαίνει στις εξουσίες του δημιουργού, περιουσιακές και ηθικές, η οποία συντελείται χωρίς την άδειά του ή χωρίς να συντρέχει άλλος λόγος που να άρει τον παράνομο χαρακτήρα της προσβολής.

Ο βασικός ευρωπαϊκός Κανονισμός που αναφέρεται στο αυτό το θέμα είναι η *"Οδηγία για την Εναρμόνιση Ορισμένων Πτυχών του Δικαιώματος της Πνευματικής Ιδιοκτησίας και*

Συγγενικών Δικαιωμάτων στην Πληροφορία" (2001/29/ΕΚ). Η Οδηγία θεσπίζει ένα πλαίσιο για την προστασία των πνευματικών δικαιωμάτων στον ψηφιακό κόσμο και καθορίζει τις προϋποθέσεις και τα όρια για τη χρήση έργων που προστατεύονται πνευματικά στην Ευρώπη, ενώ περιλαμβάνει διατάξεις για τα δικαιώματα των δημιουργών και των δικαιούχων συγγενικών δικαιωμάτων, το προνόμιο της ιδιωτικής χρήσης και την περιορισμένη χρήση έργων για εκπαιδευτικούς και επιστημονικούς σκοπούς, την προστασία των μέτρων προστασίας των τεχνολογιών.

Αναλυτικότερα, τα παραπάνω ζητήματα οριοθέτησε η Οδηγία 2004/48/ΕΚ της Ευρωπαϊκής Ένωσης σχετικά με την επιβολή των δικαιωμάτων πνευματικής ιδιοκτησίας. Βασικά σημεία τής Οδηγίας αφορούν την εναρμόνιση των διαδικασιών μεταξύ των κρατών-μελών της ΕΕ, κάνοντας ευκολότερο για τους κατόχους δικαιωμάτων να προστατεύουν τα δικαιώματά τους διασυνοριακά, τη θέσπιση προσωρινών μέτρων προστασίας, όπως αποκλεισμός, κατάσχεση και κατάσχεση προϊόντων, για την προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας, τον προσδιορισμό κριτηρίων για τον καθορισμό των αποζημιώσεων που οφείλονται στους κατόχους δικαιωμάτων από τους παραβάτες και την θέσπιση του δικαιώματος ενημέρωσης.

Το δικαίωμα ενημέρωσης αφορά το δικαίωμα των κατόχων πνευματικών δικαιωμάτων να αποκτούν πληροφορίες για τις παραβιάσεις των δικαιωμάτων τους και τα πρόσωπα που εμπλέκονται σε αυτές τις παραβιάσεις. Συγκεκριμένα, η Οδηγία προσφέρει τη δυνατότητα στους κατόχους πνευματικών δικαιωμάτων να ζητούν πληροφορίες από τα πρόσωπα που έχουν συμμετάσχει σε παραβιάσεις των δικαιωμάτων αυτών, συμπεριλαμβανομένης της αποκάλυψης του ονόματος και της διεύθυνσης των παραβατών, καθώς και άλλες σχετικές πληροφορίες. Η πρόσβαση σε αυτές τις πληροφορίες βοηθά τους κατόχους των πνευματικών δικαιωμάτων να αναλάβουν δράση για την προστασία των δικαιωμάτων τους, είτε αυτό συμπεριλαμβάνει νομικές ενέργειες είτε άλλα μέτρα για την αντιμετώπιση των παραβιάσεων και συμβάλλει στην αποτελεσματικότερη επιβολή των δικαιωμάτων πνευματικής ιδιοκτησίας στο πλαίσιο της Ευρωπαϊκής Ένωσης.

5.6.2 Νομοθετικό πλαίσιο

5.6.2.1 Στην Ελλάδα

Η Οδηγία 2001/29/ΕΚ που αναφέρθηκε προηγουμένως ενσωματώθηκε στο εγχώριο δίκαιο με τον Ν. 4481/2017, κατόπιν τροποποίησης του Ν. 2121/93, περί *"Προστασίας των*

πνευματικών δικαιωμάτων και διατάξεων για την παροχή ψηφιακών υπηρεσιών ανακοινώσεων έργων πνευματικής ιδιοκτησίας και παρόμοιων δικαιωμάτων". Ως προς την αστική ευθύνη τόσο του φυσικού παραβάτη όσο και του διαμεσολαβητού-παρόχου στο διαδίκτυο, δίνεται το δικαίωμα λήψης ασφαλιστικών μέτρων και θεσμοθετούνται η υποχρέωση για άρση της προσβολής και παράλειψή της στο μέλλον και η υποχρέωση για αποζημίωση του δημιουργού. Σε σχέση με τις ποινικές κυρώσεις λόγω προσβολής των δικαιωμάτων αυτών, ο νόμος προβλέπει, κατά το άρθρο 66, τις ποινές της φυλάκισης και χρηματικές κυρώσεις, ανάλογα με το βαθμό της παραβίασης και τη σοβαρότητα των πράξεων. Η Οδηγία 2004/48/ΕΚ της Ευρωπαϊκής Ένωσης σχετικά με την προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας δεν ενσωματώθηκε στο εγχώριο δίκαιο.

Επιπλέον, με τον Νόμο 4481/2017, στο άρθρο 52 παρ. 1, θεσπίστηκε η δημιουργία και λειτουργία μιας ειδικής Επιτροπής, για την εξωδικαστική αντιμετώπιση περιπτώσεων διαδικτυακής προσβολής δικαιωμάτων πνευματικής ιδιοκτησίας ή συγγενικών δικαιωμάτων. Στις 3 Σεπτεμβρίου 2018, ξεκίνησε η λειτουργία της Επιτροπής για τη Διαδικτυακή Προσβολή Δικαιωμάτων Πνευματικής Ιδιοκτησίας (ΕΔΠΠΙ), με στόχο την αντιμετώπιση της προσβολής δικαιωμάτων πνευματικής ιδιοκτησίας στο διαδίκτυο.

Η διαδικασία υποβολής αίτησης στην Επιτροπή, η οποία ορίζεται στο ίδιο άρθρο αφορά ένα σύστημα ειδοποίησης και απόσυρσης του περιεχομένου (notice and takedown procedure) που προσβάλλει δικαιώματα πνευματικής ιδιοκτησίας στο διαδίκτυο, το οποίο, σύμφωνα με την αιτιολογική έκθεση του εν λόγω άρθρου, τίθεται για *"τη διευκόλυνση των δικαιούχων και την αποσυμφόρηση των δικαστηρίων, είναι αναλογικό και πρόσφορο και λαμβάνει υπόψη του τα δικαιώματα και τις ελευθερίες όλων των εμπλεκόμενων μερών, ιδίως δε την ελευθερία της έκφρασης αλλά και τις εξαιρέσεις και τους περιορισμούς που προβλέπονται στο δίκαιο της πνευματικής ιδιοκτησίας"*.

Κάθε δικαιούχος, του οποίου τα δικαιώματα πνευματικής ιδιοκτησίας ή συγγενικά δικαιώματα προσβάλλονται στο διαδίκτυο δύναται να προσφύγει στην Επιτροπή με την υποβολή αίτησης αυτοπροσώπως ή ηλεκτρονικά. Εντός δέκα εργάσιμων ημερών από τη λήψη της αίτησης η Επιτροπή αποφασίζει, είτε να θέσει την υπόθεση στο αρχείο, είτε να συνεχίσει τη διαδικασία και εν τέλει να δημοσιεύσει σχετική απόφαση. Σε περίπτωση μη συμμόρφωσης προς το διατακτικό της απόφασης, δύναται να επιβληθεί πρόστιμο ανάλογο των ημερών μη συμμόρφωσης.

5.6.2.2 Στη Γερμανία

Στη Γερμανία, η Οδηγία 2001/29/ΕΚ ενσωματώθηκε με τον *"Νόμο για την Εναρμόνιση του Δικαίου περί Πνευματικής Ιδιοκτησίας με το Δίκαιο της Πληροφορίας και για την Τροποποίηση άλλων Διατάξεων"* (Urheberrechtsgesetz – UrhG). Ο νέος νόμος αντικατέστησε τον προηγούμενο νόμο περί πνευματικής ιδιοκτησίας και ενσωμάτωσε τις απαιτήσεις της Οδηγίας σε θέματα πνευματικής ιδιοκτησίας, ψηφιακής παροχής έργων, χρήσης στο διαδίκτυο και άλλες πτυχές που αφορούν την πνευματική ιδιοκτησία και την διανομή έργων πνευματικής δημιουργίας. Ως προς την αστική ευθύνη του παραβάτη υπάρχει και στην περίπτωση αυτή η υποχρέωση για άρση της προσβολής και παράλειψή της στο μέλλον και η υποχρέωση για αποζημίωση του δημιουργού, ενώ οι ποινικές διατάξεις περί πνευματικής ιδιοκτησίας βρίσκονται στα άρθρα 106 και επόμενα UrhG, κατά τα οποία προβλέπονται ποινές φυλάκισης και χρηματικού προστίμου, ανάλογα με την σοβαρότητα της παραβίασης.

Επίσης, η Γερμανία ενσωμάτωσε και την Οδηγία 2004/48/ΕΚ της ΕΕ σχετικά με την προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας στο εθνικό της δίκαιο. Η Οδηγία ενσωματώθηκε με τον νόμο *"Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums"* (Νόμος για τη βελτίωση της εφαρμογής των δικαιωμάτων της πνευματικής ιδιοκτησίας), γνωστός και ως *"IP Enforcement Act",* που εγκρίθηκε το 2008.

Τέλος, με μεταρρύθμιση της νομοθεσίας περί των περιορισμών των πνευματικών δικαιωμάτων στην Γερμανία, σε μία προσπάθεια προσαρμογής της στις νέες απαιτήσεις της ψηφιακής εποχής, τέθηκε σε ισχύ από την 1η Μαρτίου 2018, ο νόμος για την προσαρμογή των πνευματικών δικαιωμάτων στις τρέχουσες απαιτήσεις της κοινωνίας της γνώσης (Urheberrechts-Wissensgesellschafts-Gesetz - UrhWissG), ο οποίος ρυθμίζει τις επιτρεπόμενες από τον νόμο πράξεις χρήσης πνευματικών δικαιωμάτων στον τομέα της εκπαίδευσης και της επιστήμης, όπου προβλέπεται ότι η χρήση έργων για διδακτικούς σκοπούς σε σχολεία μπορεί να γίνει μόνο με τη συγκατάθεση του δικαιούχου. Συνεπώς, δεν επιτρέπονται αναλογικά ή ψηφιακά αντίγραφα από σχολικά βιβλία χωρίς την άδεια των εκδοτών, ύστερα μάλιστα από αξιολόγηση του εν λόγω νόμου τον Ιανουάριο του 2023. Για να μπορέσουν οι εκπαιδευτικοί να κάνουν ψηφιακά και αναλογικά αντίγραφα, τα Ομοσπονδιακά κρατίδια έχουν συνάψει το "συμβόλαιο φωτοτυπίας" - τη σύμβαση "Διπλότυπα στα σχολεία" - με τις εταιρείες συλλογικής διαχείρισης WORT, Bild-Kunst και Musikedition καθώς και εκδότες εκπαιδευτικών μέσων. Η σύμβαση ισχύει από την 1η

Ιανουαρίου 2023 έως τις 31 Δεκεμβρίου 2027, όπου θα πραγματοποιηθεί εκ νέου αξιολόγηση[135].

5.6.3 Το προνόμιο της ιδιωτικής χρήσης

Ένα ζήτημα το οποίο έχει απασχολήσει έντονα τόσο τη θεωρία όσο και τη νομολογία, ιδιαίτερα στην Γερμανία αποτελεί το προνόμιο της χρήσης για ιδιωτικούς σκοπούς.

Στην Ελλάδα, η προστασία των πνευματικών δικαιωμάτων για ιδιωτικούς σκοπούς ρυθμίζεται από το άρθρο 18 του Νόμου 2121/1993. Σύμφωνα με το άρθρο αυτό, επιτρέπεται η αναπαραγωγή έργων για ιδιωτική χρήση και για χρήση μέσα σε οικογενειακό περιβάλλον, ακόμα και αν αυτή γίνεται με την χρήση αναπαραγωγικών μέσων, όπως φωτοαντίγραφα, ηχογραφήσεις κ.λπ. Η χρήση αυτή πρέπει να γίνεται για προσωπική, ιδιωτική, ή οικογενειακή χρήση, χωρίς κερδοσκοπικό σκοπό. Επίσης, η παροχή δυνατότητας αντιγραφής έργων για ιδιωτική χρήση σε φωτοαντίγραφα, σε ηλεκτρονική μορφή και σε μορφή ηχογράφησης επιτρέπεται επίσης σε βιβλιοθήκες, μουσεία, εκπαιδευτικά ιδρύματα και κέντρα ερευνών για επιστημονικούς ή προσωπικούς σκοπούς, υπό συγκεκριμένες προϋποθέσεις.

Στη Γερμανία, η προστασία των πνευματικών δικαιωμάτων για ιδιωτικούς σκοπούς ρυθμίζεται στο άρθρο 53 UrhG. Σύμφωνα με τον γερμανικό νόμο, οι πολίτες έχουν το δικαίωμα να δημιουργούν αντίγραφα έργων για προσωπική χρήση, αλλά υπό πολλές περιοριστικές προϋποθέσεις. Συγκεκριμένα, στο πλαίσιο της προσωπικής χρήσης, επιτρέπεται η αναπαραγωγή πνευματικών έργων σε αντίγραφα για ιδιωτική χρήση, υπό την προϋπόθεση ότι δεν υπάρχει κερδοσκοπικός σκοπός. Αυτό μπορεί να συμπεριλαμβάνει αντίγραφα μουσικής, ταινιών, βιβλίων και άλλων προστατευόμενων έργων. Ωστόσο, οι περιορισμοί είναι αυστηροί και συμπεριλαμβάνουν περιορισμούς σχετικά με τον αριθμό των αντιγράφων που μπορούν να δημιουργηθούν, καθώς και περιορισμούς σε συγκεκριμένα είδη έργων. Επίσης, δεν επιτρέπεται η δημόσια διανομή των αντιγράφων αυτών ή η χρήση τους για εμπορικούς σκοπούς.

Σε κάθε περίπτωση, δεν υπάρχει κανένα προνόμιο εάν η αναπαραγωγή προέρχεται από προφανώς παράνομα παραχθέν πρωτότυπο. Ο προσδιορισμός της έννοιας του

[135] Verband Bildungs Medien (2023), https://bildungsmedien.de/unsere-themen/urheberrecht-und-bildung/kopierregeln-und-urhwissg.

"παρανόμως παραχθέντος" είναι σίγουρα δύσκολος στην ερμηνεία του, όμως, σύμφωνα με το Ευρωπαϊκό Δικαστήριο (ECJ) η έννοια του *"προφανούς"* δεν είναι πλέον σχετική[136].

Στη Γερμανία, ακόμα, υπάρχει ένα νομικό καθορισμένο όριο για την παράνομη λήψη αρχείων (αντιγράφων) για προσωπική χρήση, κάτω από το οποίο η πράξη αυτή δεν διώκεται ποινικά. Αυτό γνωστό ως *"Bagatellgrenze"* ή *"Geringfügigkeitsgrenze"* και αναφέρεται στη λήψη προστατευμένου περιεχομένου για προσωπική χρήση, στο άρθρο 106 StGB. Συγκεκριμένα, η παράγραφος 5 του άρθρου 106 ορίζει το ακριβές όριο όπου η παράνομη αντιγραφή για προσωπική χρήση δεν διώκεται ποινικά: *"Δεν διώκεται ποινικά όποιος προβαίνει σε αντιγραφή, αναπαραγωγή, πολυτύπηση, διάδοση, προβολή, παρουσίαση ή διάθεση στο κοινό προστατευμένου έργου ή άλλης ψηφιακής επίδοσης για προσωπική χρήση, αν από το ενδιαφέρον της πράξης δεν προκύπτει κανένα κίνητρο επικερδούς επαγγελματικής φύσης και τα ψηφιακά αρχεία δεν διατίθενται για επαναλαμβανόμενη χρήση κατά τον τρόπο που συνήθως προβλέπεται για αυτήν τη χρήση."*

Συνεπώς, η παράνομη λήψη αρχείων (όπως μουσική, ταινίες, βιβλία, λογισμικό κλπ.) για προσωπική χρήση δεν διώκεται ποινικά εάν η αξία των αρχείων είναι κάτω από ένα συγκεκριμένο όριο. Αυτό το όριο καθορίζεται νομολογιακά σε 25 ευρώ. Αυτό σημαίνει ότι, εάν η αξία των αρχείων που έχουν ληφθεί παράνομα για προσωπική χρήση είναι κάτω από τα 25 ευρώ, η πράξη αυτή δεν θεωρείται ποινική παράβαση. Παρόλα αυτά, αυτό το όριο αφορά μόνο την ποινική δίωξη. Η πνευματική ιδιοκτησία εξακολουθεί να προστατεύεται, αλλά η προαναφερθείσα διάταξη καθορίζει τα όρια της ποινικής δίωξης για πράξεις μικρής κλίμακας, ενώ οι αστικές αξιώσεις και σε αυτήν την περίπτωση παραμένουν ανεπηρέαστες.

5.6.4 Το streaming ως μέσο αποθήκευσης

Ένας ακόμα προβληματισμός σχετικά με την ποινική αξιολόγηση πράξεων που σχετίζονται με την προβολή προστατευόμενων πνευματικών έργων στο διαδίκτυο είναι η αποσαφήνιση της έννοιας του του streaming ως μέσου αποθήκευσης ή μη. Το streaming (ή στριμάρισμα) αναφέρεται στην αναπαραγωγή πολυμέσων (όπως βίντεο, ήχος, κ.λπ.) απευθείας από το διαδίκτυο, χωρίς την ανάγκη να γίνεται πρώτα λήψη του αρχείου στη συσκευή του χρήστη. Ο όρος *"streaming"* προέρχεται από τη λέξη *"stream"* που σημαίνει ροή, και αναφέρεται στη συνεχή ροή των δεδομένων πολυμέσων από τον διακομιστή προς τη

[136] Απόφαση ΔΕΕ της 10 Απριλίου .2014, στην υπόθεση C-435/12, *ACI Adam BV κ.λπ. κατά Stichting de Thuiskopie και Stichting Onderhandelingen Thuiskopie vergoeding,* https://curia.europa.eu/juris/liste.jsf?language=el&num=C-435/12.

συσκευή του χρήστη ενώ ο χρήστης βλέπει ή ακούει το περιεχόμενο. Οι υπηρεσίες streaming απαιτούν σταθερή σύνδεση στο διαδίκτυο για να λειτουργήσουν ομαλά, αφού τα δεδομένα παραδίδονται σταδιακά κατά τη διάρκεια της προβολής ή αναπαραγωγής, αντί να αποθηκεύονται τοπικά στη συσκευή του χρήστη.

Κατ' αρχήν, στον ευρωπαϊκό νομικό χώρο, το streaming δεν θεωρείται αποθήκευση, αλλά αναπαραγωγή κατά τη διάρκεια της μετάδοσης του περιεχομένου. Κατά τη διάρκεια του streaming, τα δεδομένα λαμβάνονται από το διακομιστή και αναπαράγονται στη συσκευή του χρήστη χωρίς να αποθηκεύονται μόνιμα στη συσκευή. Ωστόσο, υπάρχουν περιπτώσεις που το streaming μπορεί να συνδυάζεται με προσωρινή αποθήκευση στη μνήμη της συσκευής για την ομαλή αναπαραγωγή. Σε αυτές τις περιπτώσεις, θα πρέπει να κρίνεται κατά περίπτωση αν αυτή η προσωρινή αποθήκευση ισχύει ως αποθήκευση που παραβιάζει τα πνευματικά δικαιώματα ή όχι.

Τόσο η ελληνική, όσο και η γερμανική νομοθεσία και νομολογία δεν έχουν καθορίσει σαφώς αν το streaming θεωρείται αποθήκευση ή όχι. Ωστόσο, κατά την κρατούσα στη θεωρία άποψη το streaming θεωρείται αναπαραγωγή κατά τη διάρκεια της μετάδοσης του περιεχομένου και δεν εκλαμβάνεται ως μόνιμη αποθήκευση του περιεχομένου στη συσκευή του χρήστη. Στην Γερμανία, οι ειδικοί συμμερίζονται, πλέον, την τρέχουσα εκτίμηση του Ομοσπονδιακού Υπουργείου Δικαιοσύνης ότι το streaming δεν χρειάζεται νομικά να θεωρείται παράνομο αντίγραφο, το ερώτημα αυτό, ωστόσο, δεν έχει ακόμη διευκρινιστεί από ανώτατο δικαστήριο[137]. Γενικά, η νομολογία και η νομοθεσία προσαρμόζονται στην τεχνολογική εξέλιξη, και η ερμηνεία του streaming ως αποθήκευσης μπορεί να διαφέρει ανάλογα με το κράτος και το ειδικό πλαίσιο νομοθετικής ρύθμισης.

Στο παρελθόν, βέβαια, η γερμανική δικαιοσύνη έχει αναγνωρίσει την παράνομη προβολή μέσω ροής δεδομένων (streaming) ως αποθήκευση μόνιμων αντιγράφων, αν τα δεδομένα που αντιγράφονται παραμένουν προσβάσιμα για μεγάλο χρονικό διάστημα και συγκεκριμένη στην υπόθεση *"Kino.to"*, μια από τις μεγαλύτερες υποθέσεις πειρατικού streaming που έχει διασυνδεθεί με τη Γερμανία. Το Kino.to ήταν μια ιστοσελίδα που προσέφερε πειρατικά περιεχόμενα, όπως ταινίες και τηλεοπτικές σειρές, για δωρεάν προβολή μέσω streaming, παραβιάζοντας πνευματικά δικαιώματα.

[137] Volker Briegleb (2014), https://www.heise.de/news/Regierung-Betrachten-von-Streams-verstoesst-nicht-gegen-Urheberrecht-2077782.html.

Η υπόθεση Kino.to ξεκίνησε το 2011, όταν οι γερμανικές αρχές προχώρησαν σε ευρείες έρευνες και συλλήψεις σε συνεργάτες και υπεύθυνους της ιστοσελίδας. Περίπου 135.000 πειρατικές ταινίες, σειρές και ντοκιμαντέρ ήταν διαθέσιμα μέσω του Kino.to και αποτελούσε τη μεγαλύτερη γερμανόφωνη βάση δεδομένων ροής, ενώ διαφημίσεις που τοποθετούνταν στις τοποθεσίες συχνά οδηγούσαν τους χρήστες σε ιστοτόπους αντιγραφής και παγίδες συνδρομής[138]. Η ιστοσελίδα κατέβηκε, ενώ πολλά άτομα συνελήφθησαν και δικάστηκαν για παραβίαση πνευματικών δικαιωμάτων, οργανωμένο έγκλημα, κέρδος από παραβατικές δραστηριότητες και άλλες κατηγορίες. Ο ιδρυτής και διαχειριστής της παράνομης διαδικτυακής πύλης ταινιών Kino.to καταδικάστηκε σε φυλάκιση τεσσάρων ετών και έξι μηνών από το Περιφερειακό Δικαστήριο της Λειψίας. Εκτός από το Kino.to, ήταν επίσης υπεύθυνος για το λεγόμενο filehoster[139] στο οποίο αποθηκεύονταν οι παράνομα αντεγραμμένες ταινίες. Η υπόθεση Kino.to είχε μεγάλο αντίκτυπο στον τομέα της πειρατικής προβολής περιεχομένου και είχε σαν αποτέλεσμα να ενισχύσει τις προσπάθειες των αρχών για τον έλεγχο τέτοιων παράνομων δραστηριοτήτων στο διαδίκτυο.

Αξίζει, γενικότερα, να σημειωθεί, ότι οι διαδικτυακοί ιστότοποι κοινής χρήσης πολυμέσων είναι κατά βάση παράνομοι, επειδή δεν διαθέτουν συνήθως έγκυρη άδεια από τον κάτοχο των προστατευόμενων πνευματικών δικαιωμάτων. Ως εκ τούτου, όποιος κατεβάζει μουσική από τέτοιες ιστοσελίδες ή φορείς για ιδιωτική χρήση υπόκειται σε ποινική δίωξη. Στην περίπτωση των δικτυακών εφαρμογών, εναπόκειται στην κρίση του φορέα εκμετάλλευσης να καθορίσει τους όρους και τις προϋποθέσεις σχετικά με τις εκάστοτε άδειες ή απαγορεύσεις επεξεργασίας του έργου που αναπαράγεται ή προβάλλεται. Για παράδειγμα, το άρθρο 6Κ των γενικών όρων και προϋποθέσεων του YouTube ορίζει ότι τα έργα-βίντεο μπορούν να μεταδοθούν μόνο σε ροή και ότι η λήψη χωρίς άδεια δεν επιτρέπεται[140].

5.6.5 Μέτρα αντιμετώπισης

➔ Έρευνα (ανακριτική) για την εξασφάλιση αποδεικτικών στοιχείων

➔ Κατάσχεση φορέων δεδομένων για τη διασφάλιση της αποδεικτικής διαδικασίας, όπως η κατάσχεση συστήματος EDP (Ηλεκτρονική Επεξεργασία Δεδομένων - EDP αφορά ένα σύστημα υλικού, λογισμικού, διαδικασιών και προσωπικού που

[138] Wernert M. (2021), σελ. 204.
[139] Ως filehoster (*"φιλοξενητές"* αρχείων) αναφέρονται οι πάροχοι υπηρεσιών διαδικτύου αναφέρονται, όπου ο χρήστης μπορεί να αποθηκεύσει ή να κατεβάσει αρχεία απευθείας με ή χωρίς προηγούμενη διαδικασία εγγραφής [βλ. LKA Βάδης-Βυρτεμβέργης (2016), https://im.baden-wuerttemberg.de/de/service/publikation/did/cybercrimedigitale-spuren].
[140] Wernert M. (2021), σελ. 203.

συνεργάζονται για την ταξινόμηση και την επεξεργασία δεδομένων έτσι ώστε να μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς) για την εξασφάλιση της διαδικασίας και της επιβολής

- ➔ Αξιολόγηση των πειστηρίων
- ➔ Ταυτοποίηση μαρτύρων (κατά περίπτωση *"πελατών"*)
- ➔ Ανάκριση κατηγορουμένου

6. Επίλογος

Από τα παραπάνω συνάγεται ότι αναφορικά με τα μέτρα προστασίας για τα θύματα του ηλεκτρονικού εγκλήματος, αυτά αφορούν σε μεγάλο βαθμό την πρόληψη και μετέπειτα, σε περίπτωση διενέργειας ενός τέτοιου εγκλήματος, την διευκόλυνση εξιχνίασης του εγκλήματος και την καταπράυνση των συνεπειών του κυρίως σε σχέση με τον παθόντα. Η εξέλιξη της τεχνολογίας οδηγεί στην επέκταση του τοπίου των απειλών για την κυβερνοασφάλεια, γεγονός που δημιουργεί νέες προκλήσεις για τα κράτη-μέλη, ενώ το μέγεθος, η επινοητικότητα, η συχνότητα και ο αντίκτυπος των περιστατικών κυβερνοασφάλειας αυξάνονται και συνιστούν μείζονα απειλή για τη λειτουργία των δικτυακών και πληροφοριακών συστημάτων.

Ο τρόπος και η διατύπωση στον νόμο, τόσο στο ελληνικό όσο και στο γερμανικό δίκαιο, των μέτρων αυτών είναι ιδιαιτέρως αναλυτική, χωρίς, ωστόσο, να είναι συχνά επαρκώς σαφής και ορισμένη. Αυτό συμβαίνει διότι τα ηλεκτρονικά εγκλήματα αποτελούν μια σύγχρονη κατηγορία εγκλημάτων. Ο τρόπος τέλεσής τους και οι πιθανές συνέπειές τους δεν δύνανται πάντοτε να προβλεφθούν, ενώ χαρακτηρίζονται από διαρκή εξέλιξη και αλλαγές, με την συνεχή χρήση νέων τεχνικών μέσων και εργαλείων.

Επομένως, η αντιμετώπισή τους απαιτεί προσαρμοσμένες, συντονισμένες και καινοτόμες αποκρίσεις και καθίσταται σαφής η ανάγκη συμμετοχής ειδικών πληροφορικής και νομικών με εξειδικευμένες γνώσεις πληροφορικής τόσο κατά το στάδιο τής πρόληψης όσο και κατά τη διαδικασία τής δίωξης. Η ταχεία και αποτελεσματική αντιμετώπιση ηλεκτρονικών εγκλημάτων απαιτεί τον συνδυασμό εξειδικευμένων γνώσεων πληροφορικής και νομικής και την άμεση συνεργασία ειδικών επαγγελματιών των δύο αυτών επιστημών, ενώ οι συνδυαστικές σπουδές στους δύο αυτούς τομείς, που κάποτε φάνταζαν παντελώς ασύνδετοι, συναντώνται όλο και πιο συχνά.

Επιπλέον, ένα ισχυρό πλαίσιο προστασίας, μπορεί να οδηγήσει σε ένα αυστηρό πλέγμα, όπου ο ιδιωτικός χώρος του ατόμου περιστέλλεται σε βαθμό που το ίδιο το άτομο δεν μπορεί να ελέγξει. Η στάθμιση των μέτρων προστασίας και κυβερνοασφάλειας και του δικαιώματος στην ιδιωτικότητα σύμφωνα με τις αρχές που διέπουν το ηπειρωτικό δίκαιο και ιδιαιτέρως την αρχή της αναλογικότητας είναι απαραίτητη αλλά συνάμα δύσκολη. Πράγματι, ο κίνδυνος υπέρμετρης συρρίκνωσης θεμελιωδών δικαιωμάτων των χρηστών του διαδικτύου

έχει πολλάκις αποτελέσει αντικείμενο έντονου διαλόγου και φυσικά αποτελεί ένα ζήτημα που δεν πρέπει να προσπερνάται απερίσκεπτα.

Παρόλα αυτά, οι συνθήκες για την παρουσίαση νέων προτάσεων και μέτρων πιο συγκεκριμένων σε σχέση με την αντιμετώπισή τους σε νομικό-δικονομικό πλαίσιο έχουν πλέον ωριμάσει και ο επιστημονικός διάλογος σχετικά με το ζήτημα αυτό φαντάζει πιο έντονος από ποτέ. Για την αποτελεσματικότερη προστασία ο νόμος θα πρέπει να επικεντρώνεται περισσότερο στο θύμα-παθόντα με τον καθορισμό συγκεκριμένων και επικαιροποιημένων μέτρων. Η δυσκολία σε αυτό έγκειται, ωστόσο, στο γεγονός ότι η δυναμική τής τεχνολογίας καθιστά αναγκαία την συνεχή μεταβολή και τροποποίηση των αντίστοιχων διατάξεων, ώστε αυτές να ανταποκρίνονται διαρκώς στις εκάστοτε ανάγκες προστασίας των χρηστών.

Ο νομοθέτης, από την άλλη, φαίνεται να συμβαδίζει με τις ανάγκες της σύγχρονης ψηφιακής κοινωνίας, όπως διαφαίνεται από τις τελευταίες προσθήκες και τροποποιήσεις, τόσο στην Ελλάδα όσο και στη Γερμανία. Το ελληνικό νομικό σύστημα συνεχίζει να συμπορεύεται με το αντίστοιχο γερμανικό στον τομέα τού κυβερνοεγκλήματος, με μικρή χρονική απόκλιση λίγων ετών, λόγω της ταχύτερης τεχνολογικής εξέλιξης της Γερμανίας σε σχέση με την Ελλάδα, και με ορισμένες διαφορές στο περιεχόμενό τους, οι οποίες φαίνεται να οφείλονται κυρίως σε πρακτικούς λόγους, εξαιτίας τής διαφορετικής μορφής των δύο κρατών. Για τον ίδιο λόγο, η ελληνική βιβλιογραφία σχετικά με το θέμα που πραγματεύεται η παρούσα είναι σημαντικά περιορισμενη σε σχέση με την αντίστοιχη γερμανική, αν και τα τελευταία χρόνια παρουσιάζεται σημαντική βελτίωση.

Εν κατακλείδι, για να είναι η κοινωνία και η οικονομία έτοιμη για την ψηφιακή εποχή και την αύξηση των κυβερνοεπιθέσεων στο μέλλον, απαιτείται ένας ασφαλής ψηφιακός χώρος για τους πολίτες και τις επιχειρήσεις, ο οποίος θα είναι συμπεριληπτικός και προσβάσιμος για όλους και συγχρόνως κατάλληλα, ρεαλιστικά και αποτελεσματικά μέτρα προστασίας των χρηστών. Η γνώση του τι επιφυλάσσει το μέλλον μπορεί να βοηθήσει στην καλύτερη προετοιμασία για επερχόμενα γεγονότα. Στον χώρο του κυβερνοεγκλήματος, όμως, αυτό δεν είναι δυνατό λόγω της ιδίας της φύσης του. Μοναδικό σταθερό παράγοντα αποτελούν η πολυπλοκότητα τής σύγχρονης κυβερνοασφάλειας και η ανάγκη συνεργασίας διαφορετικών ομάδων και υπηρεσιών σε διακρατικό επίπεδο για την καταπολέμηση των κυβερνοεπιθέσεων στις οποίες εκτίθενται όχι μόνο ιδιώτες, αλλά ακόμη και ολόκληρα κράτη.

Βιβλιογραφία

Βιβλία

- Δαλακούρας Θ. / Κωνσταντινίδης Α. (2014), *Εμβάθυνση στο Ποινικό Δικονομικό Δίκαιο*, Αθήνα-Θεσσαλονίκη: Νομική Βιβλιοθήκη.
- Δαλακούρας Θ. (2023), *Ηλεκτρονικό Έγκλημα*, 2η έκδοση, Αθήνα-Θεσσαλονίκη: Νομική Βιβλιοθήκη.
- Δαλακούρας Θ. (2020), *Ο Νέος Κώδικας Ποινικής Δικονομίας, Συνοπτική Ερμηνεία κατ' άρθρο του Ν. 4620/2019*, Αθήνα-Θεσσαλονίκη: Νομική Βιβλιοθήκη.
- Δαλακούρας Θ. (2003), *Ποινική Δικονομία. Βασικές έννοιες και θεσμοί της ποινικής δίκης*, β' τόμος, Αθήνα- Κομοτηνή: Σάκκουλας.
- Ζέκος Γ. (2022), *Διαδίκτυο και Τεχνητή Νοημοσύνη στο ελληνικό δίκαιο*, Αθήνα-Θεσσαλονίκη:: Σάκκουλας.
- Θεμελή Ό. (2014), *Τα παιδία καταθέτει. Η δικανική εξέταση ανηλίκων μαρτύρων, θυμάτων σεξουαλικής κακοποίηση,* Αθήνα: Τόπος.
- Ιγγλεζάκης Ι. (2021), *Δίκαιο πληροφορικής*, 4η έκδοση, Αθήνα-Θεσσαλονίκη: Σάκκουλας.
- Ιγγλεζάκης Ι. (2022), *Το δίκαιο της ψηφιακής οικονομίας*, Αθήνα-Θεσσαλονίκη: Σάκκουλας.
- Ιντζεσίλογλου Ν. (2009), Κοινωνικοποίηση των νέων και παραβατικότητα. *Παραβατικότητα και σχολείο*, Θεσσαλονίκη: Αφοί Κυριακίδη ΕΚΔΟΣΕΙΣ Α.Ε..
- Κιούπης Δ. (2007), στο Ιωαννίδου Α. (2007), *Η παιδική πορνογραφία στο διαδίκτυο*, Αθήνα-Θεσσαλονίκη: Νομική Βιβλιοθήκη.
- Κουράκης Ν.Ε. (2012), Η πορνογραφία ανηλίκων στο διαδίκτυο (άρθρο 348 Α ΠΚ). *Εγκληματολογία*, τεύχος 1.
- Κωνσταντινίδης Α. (2012), *Η απόδειξη στην ποινική δίκη*, 2η έκδοση, Αθήνα-Θεσσαλονίκη: Σάκκουλας.
- Μαργαρίτης Λ. (2020), *Ο νέος Κώδικας Ποινικής Δικονομίας ερμηνεία κατ' άρθρο,* τόμος α', Αθήνα-Θεσσαλονίκη: Νομική Βιβλιοθήκη.
- Ορφανός Σ. (2022), *Σεξουαλικά εγκλήματα*, Αθήνα-Θεσσαλονίκη: Νομική Βιβλιοθήκη.
- Παπαδαμάκης Α. (2021), *Ποινική Δικονομία*, 10η έκδοση, Αθήνα-Θεσσαλονίκη: Σάκκουλας.

- Παρασκευόπουλος Ν./ Φυτράκης Ε. (2021), *Αξιόποινες σεξουαλικές πράξεις*, 2η έκδοση, Αθήνα-Θεσσαλονίκη: Σάκκουλας.
- Παύλου Σ. / Σάμιος Θ. (2014), *Ειδικοί Ποινικοί Νόμοι - Ερμηνεία κατ' άρθρον*, τόμος β', Αθήνα: Π.Ν. Σάκκουλα, σελ 7.
- Συκιώτη Α./ Παπαγεωργίου-Γονατάς, Στ. (2021), Ο νέος Ποινικός Κώδικας - Ερμηνεία κατ' άρθρο του Ν 4619/2019. Τόμος Β', Αθήνα-Θεσσαλονίκη: Νομική Βιβλιοθήκη.
- Συμεωνίδου-Καστανίδου Ε. (2020), *Εγκλήματα κατά προσωπικών αγαθών*, 4η έκδοση, Αθήνα-Θεσσαλονίκη: Νομική Βιβλιοθήκη.
- Τριανταφύλλου Α. (2014), *Ζητήματα Μαρτυρικής Απόδειξης στην Ποινική Δίκη*, Αθήνα: Π.Ν. Σάκκουλας.
- Χατζηνικολάου Ν. (2009), *Η ποινική καταστολή της παράνομης μετανάστευσης και της εμπορίας ανθρώπων στην ελληνική έννομη τάξη: αναζητώντας την αξιολογική συνοχή της μεταξύ τιμωρητικής όξυνσης και θυματολογικής προσέγγισης,* Αθήνα-Θεσσαλονίκη: Νομική Βιβλιοθήκη.
- Borges G./ Schwenk J./ Stuckenberg C.F./ Wegener C. (2011), *Identitätsdiebstahl und Identitätsmissbrauch im Internet – Rechtliche und technische Aspekte*, Βερολίνο: Springer.
- Dölling D./ Jehle J.M., επιμ. (2013) *Täter-Taten-Opfer, Grundlagenfragen und aktuelle Probleme der Kriminalität und ihrer Kontrolle*, τόμος 114, Mönchengladbach: Kriminologische Gesellschaft e.V.
- Eckstein K. (2001), *Besitz als Straftat*, Βερολίνο: Duncker & Humblot.
- Freeman – Longo R. E. (1989), *The sexual victimization of Males: Victim to Victimizer: Clinical Observations and Case Studies*, Washington, DC: Hemisphere.
- Gercke M., Understanding cybercrime: phenomena, challenges and legal response. *ITU,* https://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html, 09.08.2023.
- Kleile M. (2016), *Handbuch Internetrecherche*, Στουτγκάρδη: Boorberg.
- Mag. phil. Michael Weber (2014), *„Happy-Slapping" – Eine sozialpädagogische Studie über den Zusammenhang von Gewalt, Medien und Schule.* Διδακτορική διατριβή, Γκρατς: Πανεπιστήμιο Karl-Franzens
- Mischkewitz A.(2014), *Das staatliche Zeugenschutzprogramm in Deutschland – Übersicht, Analyse der Rechtslage und Problemfelder des polizeilichen Zeugenschutzes,*Μπόχουμ: Felix.
- Siegismund C. (2009), *Der Schutz gefährdeter Zeugen in der Bundesrepublik unter besonderer Berücksichtigung des Gesetzes zur Harmonisierung des Schutzes*

gefährdeter Zeugen (Zeugenschutz-Harmonisierungsgesetz ZSHG), Osnabrück: Univ.-Diss.

- Stewen M. (2008), *Die Herausforderung Internet – dargestellt an den Deliktsbereichen Kinderpornografie und sexueller Missbrauch von Kindern*, Βερολίνο: der kriminalist 5/2008.

- Wernert M. (2021), *Internetkriminalität: Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen*, 4η έκδοση, Στουτγκάρδη: Boorberg.

Άρθρα

- Μιαούρας Κ. (2018), *Οι ειδικές διατάξεις προστασίας και βοήθειας των θυμάτων του ηλεκτρονικού εγκλήματος στην εγχώρια και διεθνή έννομη τάξη*, διπλωματική εργασία, Θεσσαλονίκη: ΠαΜακ και ΔΠΘ.

- Μίχα Ε. (2016), Ζητήματα αποκατάστασης για τα θύματα της εμπορίας ανθρώπων: Το Διεθνές Νομικό Πλαίσιο και οι υποχρεώσεις εφαρμογής της Ελλάδας. *Κυβερνοέγκλημα και Κρίση*, Τιμητικός Τόμος Κουράκη, http://crime-in-crisis.com/%CE%B6%CE%B7%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1-%CE%B1%CF%80%CE%BF%CE%BA%CE%B1%CF%84%CE%AC%CF%83%CF%84%CE%B1%CF%83%CE%B7%CF%82-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B1-%CE%B8%CF%8D%CE%BC%CE%B1%CF%84%CE%B1/, 20.07.2023.

- Μπούρμπας Γ. (2016), Προσπάθειες εννοιολογικού προσδιορισμού της κατοχής ηλεκτρονικών δεδομένων με χαρακτήρα παιδικής πορνογραφίας Υπό το πρίσμα των νεώτερων νομοθετικών εξελίξεων και των αρχών του Κράτους Δικαίου. *Κυβερνοέγκλημα και Κρίση*, Τιμητικός Τόμος Κουράκη, http://crime-in-crisis.com/category/%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1-%CE%BA%CE%B1%CE%B9-%CE%BA%CF%81%CE%AF%CF%83%CE%B7/, 20.07.2023.

- Νάϊντος Χ. (2017), Ειδικές ανακριτικές πράξεις: επίκαιρα ζητήματα, *Ποινικά Χρονικά*, Αύγουστος- Σεπτέμβριος 2017.

- Συμεωνίδης Δ. (2004), Ο υποχρεωτικός διορισμός συνηγόρου σύμφωνα με τον Κ.Π.Δ. υπό το πρίσμα του ν.3226/2004, *Ποινικός Λόγος.*

- Τριανταφύλλου Α. (2017), Δικαίωμα υπερασπίσεως σε διαδικασίες ειδικών χαρακτηριστικών, *Εισήγηση στο 7ο Συνέδριο της Ένωσης Ελλήνων Ποινικολόγων με θέμα : "ΤΟ ΔΙΚΑΙΩΜΑ ΥΠΕΡΑΣΠΙΣΕΩΣ ΣΤΗΝ ΠΟΙΝΙΚΗ ΔΙΚΗ - Όψεις και Όρια" (Πάτρα 15 & 16/4/2016),* Αθήνα: Νομική Βιβλιοθήκη.

- Χειδάρης Β. (2016), Η ΥΠΕΡΑΣΠΙΣΗ ΤΩΝ ΟΙΚΟΝΟΜΙΚΩΣ ΑΔΥΝΑΤΩΝ ΣΤΗ ΝΟΜΟΛΟΓΙΑ ΤΟΥ ΕΔΔΑ, *Εισήγηση στο 7ο Συνέδριο της Ένωσης Ελλήνων Ποινικολόγων με θέμα : "ΤΟ ΔΙΚΑΙΩΜΑ ΥΠΕΡΑΣΠΙΣΕΩΣ ΣΤΗΝ ΠΟΙΝΙΚΗ ΔΙΚΗ - Όψεις και Όρια" (Πάτρα 15 & 16/4/2016),* https://lawtakpap.blogspot.com/2016/04/h.html, 03.09.2023.
- Bär W. (2013), Rechtliche Herausforderungen bei der Bekämpfung von Cybercrime. *BKA-Herbsttagung „Cybercrime – Bedrohung, Intervention, Abwehr“, CybercrimeBKAhttps://www.bka.de › Herbsttagungen › 2013 › he…*, 07.07.2023.
- Bock S. (2013), Das europäische Opferrechtspaket: zwischen substantiellem Fortschritt und blindem Aktionismus ZIS 2013, S. 201–211. *Zeitschrift für Internationale Strafrechtsdogmatik,* https://www.zis-online.com/dat/artikel/2013_4_747.pdf, 15.09.2023.
- Brodowski D. (2021), *Strafrechtsrelevante Entwicklungen in der Europäischen Union – ein Überblick*, διπλωματική εργασία, Σάαρμπρυκεν: Universität des Saarlande, https://www.zis-online.com/dat/artikel/2021_6_1444.pdf, 28.07.2023.
- Burhoff D. (2016), *Neuregelungen in der StPO durch das 3. Opferrechtsreformgesetz*, ZAP-Heft 3/2016, F. 22, S. 861 ff., https://www.burhoff.de/veroeff/aufsatz/zap_F22_861ff.htm#I, 15.09.2023.
- Florian Gathmann, Philipp Wittrock (2014), *Kinderpornografie-Ermittlungen: Der Fall Edathy wird zur Regierungsaffäre.* Spiegel Online, https://www.spiegel.de/politik/deutschland/kinderporno-ermittlungen-fall-edathy-bringt-friedrich-und-spd-in-not-a-953314.html, 20.05.2023.
- Ford M., Boucadair M., Durand A., Levis P., Roberts P. (2011), Issues with IP Address Sharing, INFORMATIONAL, Internet Engineering Task Force (IETF), https://www.rfc-editor.org/rfc/rfc6269.html, 14.09.2023.
- Hase D. (2012), Beratungshilfe: kostenlose Rechtshilfe mit dem Beratungshilfeschein, *akademie.de,* https://www.akademie.de/de/wissen/beratungshilfeschein-kostenlose-rechtshilfe, 02.09.2023.
- Henrichs A./ Wilhelm J. (2010), Global vernetzen – lokal ermitteln. *Polizeiliche Herausforderungen durch soziale Netzwerke*, Ντύσσελντορφ: Gewerkschaft der Polizei, τεύχος 10/2010.
- Mikkelson B. (2021), *Snuff Films Snuff films — are they for real?*, https://www.snopes.com/fact-check/a-pinch-of-snuff/, 02.08.2023.
- Satoh, A.; Fukuda, Y.; Kitagata, G.; Nakamura (2021), Y. A Word-Level Analytical Approach for Identifying Malicious Domain Names Caused by Dictionary-Based

DGA Malware. *Electronics*, https://doi.org/10.3390/electronics10091039, 16.09.2023.

- Spiegel online (2014), *Edathy-Auftritt in Berlin "Es war falsch, die Filme zu bestellen, aber es war legal"*, https://www.spiegel.de/politik/deutschland/sebastian-edathy-filmbestellung-war-falsch-aber-legal-a-1009190.html, 20.05.2023.
- Verband Bildungs Medien (2023), *Kopierregeln und UrhWissG*, https://bildungsmedien.de/unsere-themen/urheberrecht-und-bildung/kopierregeln-und-urhwissg, 06.08.2023.
- Volker B. (2014), Regierung: Betrachten von Streams verstößt nicht gegen Urheberrecht. *heise online,* https://www.heise.de/news/Regierung-Betrachten-von-Streams-verstoesst-nicht-gegen-Urheberrecht-2077782.html, 06.07.2023.
- Writers S. (2022), *Ransomware protection has become a critical channel upsell,* crn.com, https://www.crn.com.au/feature/ransomware-protection-has-become-a-critical-channel-upsell-583756, 12.07.2023.
- Zeitner, I. (2013), *Internetkriminalität - eine polizeiliche Herausforderung*. PSP 1/2013.

Νομοθεσία και άλλα νομικά κείμενα

- Απόφαση 113/2015 του Συμβουλίου της Επικρατείας Κρήτης.
- Απόφαση ΔΕΕ της 10ης Απριλίου 2014, στην υπόθεση C-435/12, *ACI Adam BV κ.λπ. κατά Stichting de Thuiskopie και Stichting Onderhandelingen Thuiskopie vergoeding*, https://curia.europa.eu/juris/liste.jsf?language=el&num=C-435/12, 06.07.2023.
- Απόφαση ΔΕΕ της 5ης Ιουνίου 2008, στην υπόθεση C-164/0, *James Wood v Fonds de garantie des victimes des actes de terrorisme et d'autres infractions,* https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62007CJ0164, 25.07.2023.
- ΑΠ 681/2023, α' δημοσ. ΤΝΠ NOMOS.
- ΑΠ 43/2023, α' δημοσ. ΤΝΠ NOMOS.
- ΑΠ 681/2023, α' δημοσ. ΤΝΠ NOMOS.
- ΑΠ 279/2020, α' δημοσ. ΤΝΠ NOMOS.
- ΑΠ 1332/2019, α' δημοσ. ΤΝΠ NOMOS.

- ΑΠ 1572/2017, α' δημοσ. ΤΝΠ NOMOS.
- ΑΠ 985/2015, α' δημοσ. ΤΝΠ NOMOS.
- ΑΠ 169/2015, α' δημοσ. ΤΝΠ NOMOS.
- ΑΠ 931/2012, α' δημοσ. areiospagos.gr, https://www.areiospagos.gr/nomologia/apofaseis_DISPLAY.asp?cd=FKS3IS4EWVCQE9LSSJU8CLVTQ7X73S&apof=931_2012&info=%D0%CF%C9%CD%C9%CA%C5%D3%20-%20%20%D3%D4, 05.09.2023.
- ΑΠ 944/2005, α' δημοσ. Δ/ΝΗ 2005/1577, δημοσ. ΠΟΙΝΧΡ 2006/53, δημοσ. ΤΝΠ ΝΟΜΟΣ.
- BSG, Judgment of November 30, 2006 – Ref.: B 9a VG 4/05 R, https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BSG&Datum=30.11.2006&Aktenzeichen=B%209a%20VG%204/05%20R, 28.07.2023.
- COM(2022) 209 final, 2022/0155(COD), Πρόταση - Κανονισμός Του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση κανόνων με σκοπό την πρόληψη και την καταπολέμηση της σεξουαλικής κακοποίησης παιδιών, https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52022PC0209, 19.09.2023.
- Convention on Cybercrime, Budapest, 23.11.2001 (CETS No. 185), https://rm.coe.int/1680081561, 22.04.2023.
- Deutscher Bundestag (2011), *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Petra Pau, Jan Korte, Dr. Petra Sitte, weiterer Abgeordneter und der Fraktion DIE LINKE – Drucksache 17/5674 –*, https://dserver.bundestag.de/btd/17/058/1705835.pdf, 08.09.2023.
- Deutscher Bundestag (1998), *Beschlussempfehlung des Ausschusses nach Artikel 77 des Grundgesetzes (Vermittlungsausschuß),* https://dserver.bundestag.de/btd/13/100/1310001.pdf, 15.09.2023.
- LG Mainz, Beschluss vom 26. Juni 1995 – 302 Js 21307/94 jug. 3 A Kls, NJW 1996.

Ιστότοποι

- Αρχή Προστασίας Δεδομένων, *Συμβουλές για προστασία από SPAM*, https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/proothisiproiontwn/hlektronika_mesa_proothisi/sumvoules_spam, 07.07.2023.
- Ελληνική Αστυνομία (2022), *Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος*, https://www.astynomia.gr/elliniki-astynomia/eidikes-ypiresies/diefthynsi-dioxis-ilektronikou-egklimatos/, 14.09.2023.

- Ελληνική Δημοκρατία η Κυρβέρνηση (2022), *Μέσω gov.gr οι καταγγελίες στη Δίωξη Ηλεκτρονικού Εγκλήματος,* https://www.government.gov.gr/meso-gov-gr-katangelies-sti-dioxi-ilektronikou-egklimatos/, 28.08.2023.
- Ευρωπαϊκή Επιτροπή (2014), *«Ευρωπαϊκό Κέντρο για Εγκλήματα στον Κυβερνοχώρο – ένας χρόνος μετά»,* https://ec.europa.eu/commission/presscorner/detail/el/IP_14_129, 14.09.2023.
- Υπουργείο Εσωτερικών Β. Ρηνανίας-Βεστφαλίας, ετήσια έρευνα 2020, *Revision der kriminalpolizeilichen Bearbeitung von sexuellem Missbrauch an Kindern und Kinderpornografie,* https://www.im.nrw/system/files/media/document/file/abschlussberichtkipost.pdf, 22.02.2023.
- BKA, *Das Programm "Polizei 20/20",* https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/ElektronischeFahndungsInformationssysteme/Polizei2020/Polizei2020_node.html, 13.09.2023.
- Bloomberg J. (2017), *Using Bitcoin Or Other Cryptocurrency To Commit Crimes? Law Enforcement Is Onto You*, https://www.forbes.com/sites/jasonbloomberg/2017/12/28/using-bitcoin-or-other-cryptocurrency-to-commit-crimes-law-enforcement-is-onto-you/, 09.008.2023.
- BMAS (2021), *Opferentschädigungsrecht,* https://www.bmas.de/DE/Soziales/Soziale-Entschaedigung/Opferentschaedigungsrecht/opferentschaedigungsrecht-art.html, 28.07.2023.
- BMAS (2021), *Anspruch auf Entschädigung bei Gewalttaten im europäischen Ausland,* https://www.bmas.de/DE/Soziales/Soziale-Entschaedigung/Opferentschaedigungsrecht/anspruch-auf-entschaedigung-bei-gewalttaten.html, 28.07.2023.
- BSI (2022), *Ransomware: Bedrohungslage, Prävention & Reaktion*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html, 12.07.2023.
- BSI (2020), *Digitaler Verbraucherschutz*, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html, 07.07.02023.
- BSI (2015), *Die Lage der IT-Sicherheit in Deutschland*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf%3F__blob%3DpublicationFile, 06.07.2023.
- BSI, *DoS- und DDoS-Attacken Denial-of-Service (DoS) und Distributed Denial-of-Service (DDoS)*,

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/DoS-Denial-of-Service/dos-denial-of-service_node.html, 22.08.2023.

- BSI, *Sicherheit von Webanwendungen - Maßnahmenkatalog*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/WebSec/WebSec.pdf?__blob=publicationFile&v=1, 22.08.2023.
- BSI, *Woran erkennt man Spam-Inhalte?*, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Spam/Woran-erkennt-man-Spam/woran-erkennt-man-spam.html, 07.07.2023.
- Bundeskriminalamt, BKA, *Wo kann ich Anzeige erstatten?,* https://www.bka.de/SharedDocs/FAQs/DE/Anzeige/anzeigeFrage01.html, 28.08.2023.
- Bundeslagebild, BKA (2015), *Cybercrime*, εκδ. Bundeskriminalamt, https://www.bka.de/DE/Home/home_node.html, 06.07.2023.
- Bundeslagebild, BKA (2010), *IuK-Kriminalität*, εκδ. Bundeskriminalamt, https://www.bka.de/DE/Home/home_node.html, 06.07.2023.
- Edri20 (2023), *Internal market MEPs wrestle with how to fix Commission's CSAR proposal,* https://edri.org/our-work/internal-markets-meps-wrestle-with-how-to-fix-commissions-csar-proposal/, 18.09.2023.
- Eurojust, *SIRIUS*, https://www.eurojust.europa.eu/sirius, 13.09.2023.
- Europäische Kommission, *Zusammenarbeit der SIRENE-Büros,* https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/sirene-cooperation_de, 08.09.2023.
- Frankfurter Allgemeine Sonntagszeitung (2020), *„Ihr seid so krass – Wie Jugendliche sich in „Happy Slapping"-Videos mit Straftaten brüsten und andere dazu ermutigen,* https://abo.faz.net/frankfurter-allgemeine-sonntagszeitung/fas.html?dwvar_fas_medium=FAP_DGT&dwvar_fas_referencePeriodicityGroup=SOABO&dwvar_fas_subscriptionType=REG_SX_PO&affiliate=IP23015&pac=IP23015&pacmedium=FAP_DGT&campID=SEA_BG-BM_PERF_PAY_FAS-FAP_DGT_ABO_SO_REG_UN_PO_standard_IP23015&campaign=_BG-BM_&campID=SEA_BG-BM&s_kwcid=AL!9053!3!463549399339!b!!g!!frankfurter%20allgemeine%20sonntagszeitung%20online&gclid=Cj0KCQjwl8anBhCFARIsAKbbpyR_-PfOxgqyv7SDsPKeAq1HubULjC5x4ZicR-8MtIQ6Zp-_mK5eHREaArtUEALw_wcB, 16.09.2021.
- Gercke M. (2023), Understanding cybercrime: phenomena, challenges and legal response. *ITU,* www.itu.int/ITU-D/cyb/cybersecurity/legislation.html, 09.08.2023.

- gov.gr, *Ελληνική Αστυνομία,* https://www.gov.gr/org/astynomia/kataggelies, 28.08.2023.
- Greek Cybercrime Center, *Το Ελληνικό Κέντρο για το Κυβερνοέγκλημα*, https://www.cybercc.gr/el/poioi-eimaste/, 13.09.2013.
- Interpol (2014), *INTERPOL-coordinated operation strikes back at 'sextortion' networks,* https://www.interpol.int/News-and-Events/News/2014/INTERPOL-coordinated-operation-strikes-back-at-sextortion-networks, 14.09.2023.
- IT-SERVICE.NETWORK, *Drive-by-Download / Drive-by-Exploit – Definition,* https://it-service.network/it-lexikon/drive-by-exploit, 22.08.2023.
- Jura Forum (2022), *Antragsdelikt / Strafantrag nach StGB - Absolute & relative Antragsdelikte inkl. Auflistung*, https://www.juraforum.de/lexikon/antragsdelikte, 22.08.2023.
- LKA Βάδης-Βυρτεμβέργης (2016), ετήσια έρευνα 2015, *Cyberkriminalität. Digitale Spuren*, https://im.baden-wuerttemberg.de/de/service/publikation/did/cybercrimedigitale-spuren, 06.06.2023.
- LKA Βάδης-Βυρτεμβέργης (2015), ετήσια έρευνα 2015, *Warnmeldung für Firmen*, https://www.bw.ihk.de/_Resources/Persistent/007c94cdbec8d10dc845679526f3002e538b296b/M%C3%A4rz-Warnmeldung%20ZAC_sch%C3%A4dliche-E-Mail-Anh%C3%A4nge.pdf, 12.07.2023.
- Microsoft Support, Προστασία του υπολογιστή σας από το ransomware, https://support.microsoft.com/el-gr/windows/%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1-%CF%84%CE%BF%CF%85-%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE-%CF%83%CE%B1%CF%82-%CE%B1%CF%80%CF%8C-%CF%84%CE%BF-ransomware-08ed68a7-939f-726c-7e84-a72ba92c01c3, 08.07.2023.
- h-h.de (2019), *E-Mail-Header lesen und verstehen*, https://th-h.de/net/usenet/faqs/headerfaq/, 08.07.2023.
- Lawspot (2019), *Κυβερνοέγκλημα: Ποιες υποθέσεις πρέπει να παραπέμπονται στη Δίωξη Ηλεκτρονικού Εγκλήματος (Εγκύκλιος ΕισΑΠ)*, https://www.lawspot.gr/nomika-nea/kyvernoegklima-poies-ypotheseis-prepei-na-parapempontai-sti-dioxi-ilektronikoy-egklimatos, 03.09.2023.
- Polizei Nordrhein-Westfallen, *Ich möchte eine Anzeige erstatten*, https://internetwache.polizei.nrw/ich-moechte-eine-anzeige-erstatten, 28.08.2023.

➢ Polizei Nordrhein-Westfallen, *Onlineanzeige der Polizei NRW*, https://formulare.polizei.nrw/ams/anzeige/wizardng/FFE7CD?v=1694083797072, 28.08.2023.

➢ Staatsanwaltschaften Hessen, *GStA Generalstaatsanwaltschaft Frankfurt am Main*, https://gsta-frankfurt-justiz.hessen.de, 03.09.2023.