ΔΠΜΣ με τίτλο:

«ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ»

ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΜΑΚΕΔΟΝΙΑΣ

ΚΑΙ ΤΜΗΜΑΤΟΣ ΝΟΜΙΚΗΣ ΔΗΜΟΚΡΙΤΕΙΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΘΡΑΚΗΣ

Διπλωματική Εργασία

με Θέμα:

«ΤΟΠΟΣ ΤΕΛΕΣΗΣ ΤΟΥ ΔΙΑΔΙΚΤΥΑΚΟΥ ΕΓΚΛΗΜΑΤΟΣ»

Μεταπτυχιακή Φοιτήτρια:

Νίκου Α. Κλειώ (Α.Μ.: 21051)

Μέλη Τριμελούς Επιτροπής:

1.Δαλακούρας Θεοχάρης (Επιβλέπων)

2.Σαββίδης Νικόλαος (Συνεπιβλέπων)

3.Δανιήλ Γεώργιος

Θεσσαλονίκη, Ιανουάριος 2024

Σύνοψη

Η ραγδαία ανάπτυξη και χρήση του διαδικτύου συνδέεται με τη διάπραξη παραδοσιακών και νεότερων ποινικών αδικημάτων. Ο διασυνοριακός χαρακτήρας του ηλεκτρονικού εγκλήματος και ο χαρακτήρας του ως εγκλήματος απόστασης αναγείρει το πρόβλημα οι τόποι τέλεσης των οικείων αδικημάτων να τοποθετούνται πολλές φορές σε περισσότερα κράτη. Σκοπός της παρούσας εργασίας είναι να απαντήσει σε μία σειρά ερωτημάτων που ανακύπτουν από τις ιδιαιτερότητες του ηλεκτρονικού εγκλήματος. Ειδικότερα, επιχειρείται να απαντηθεί, πρώτον, το ερώτημα πότε είναι εφαρμοστέοι οι εθνικοί ποινικοί κανόνες του κάθε κράτους, δεύτερον, ποιοι κανόνες ρυθμίζουν και πρέπει να ρυθμίζουν τα ζητήματα αυτά, και, τρίτον, εάν υφίστανται επί του παρόντος ικανοποιητικές λύσεις σε εθνικό ή υπερεθνικό επίπεδο, ώστε οι αρχές επιβολής του νόμου και οι δικαστικές αρχές να είναι σε θέση να ερευνούν και να καταστέλλουν αποτελεσματικά τις περιπτώσεις ηλεκτρονικού εγκλήματος. Στο μέρος Α παρατίθενται ορισμένες εισαγωγικές σκέψεις και τίθεται το ερευνητικό πλαίσιο,. Στο μέρος Β ερευνάται το ζήτημα του τόπου τέλεσης του ηλεκτρονικού εγκλήματος. Ειδικότερα, αρχικά οριοθετούνται οι έννοιες, οι διακρίσεις και τα ιδιαίτερα χαρακτηριστικά γνωρίσματα των εγκλημάτων στον κυβερνοχώρο. Έπειτα, εξετάζονται οι βασικές αρχές του τόπου τέλεσης των εγκλημάτων, δηλαδή η αρχή της εδαφικότητας, η αρχή της ενότητας της πράξης, οι αρχές του υποκειμενικού και αντικειμενικού ενδιαφέροντος και η αρχή της παγκόσμιας δικαιοσύνης. Τέλος, ερευνάται ο τόπος τέλεσης συγκεκριμένα του ηλεκτρονικού εγκλήματος και η εξάρτηση της εύρεσής του αφενός από το είδος της αξιόποινης πράξης, αφετέρου από τη συγκεκριμένη χρήση της τεχνολογίας. Στο μέρος Γ ερευνώνται ειδικότερα ζητήματα που συναρτώνται με τον χώρο του ηλεκτρονικού εγκλήματος. Πιο συγκεκριμένα, αρχικά εξετάζεται η συμμετοχική ευθύνη των ενδιάμεσων παρόχων διαδικτύου στο ηλεκτρονικό έγκλημα, μέσω της παράθεσης των αναγκαίων ορισμών και των προϋποθέσεων κατάφασης της ευθύνης τους. Εν συνεχεία,

ερευνάται ο ρόλος που διαδραματίζουν τα ηλεκτρονικά αποτυπώματα στο ηλεκτρονικό έγκλημα μέσω της εξέτασης των μεθόδων ανώνυμης σύνδεσης στο διαδίκτυο και των ψηφιακών αποτυπωμάτων. Τέλος, ερευνάται η αξία της συνδρομής των ηλεκτρονικών αποδεικτικών στοιχείων (e-evidence) στις ποινικές διαδικασίες και αξιολογούνται τα νέα νομοθετικά μέτρα της ΕΕ για το καθεστώς των ηλεκτρονικών αποδείξεων. Στο μέρος Δ παρατίθενται οι συμπερασματικές σκέψεις και η προσωπική κρίση της γράφουσας.

Α.-ΕΙΣΑΓΩΓΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ

Η ραγδαία ανάπτυξη και χρήση του διαδικτύου συνδέεται με τη διάπραξη παραδοσιακών και νεότερων ποινικών αδικημάτων. Το ηλεκτρονικό έγκλημα καταλαμβάνει τις αξιόποινες πράξεις που τελούνται στο διαδίκτυο είτε πρόκειται για αδικήματα του φυσικού χώρου, είτε για αδικήματα που έχουν αντικείμενο, ή χρησιμοποιούν ως μέσο, πληροφοριακά συστήματα. Το ηλεκτρονικό έγκλημα ενέχει απειλές τόσο σε βάρος φυσικών και νομικών προσώπων, που βασίζονται στις νέες τεχνολογίες, όσο και σε βάρος κρατικών οντοτήτων. Το στοιχείο της παγκοσμιότητας των δεδομένων ανάγει το ηλεκτρονικό έγκλημα σε κίνδυνο διαφορετικής ποιότητας και έκτασης για την ασφάλεια των εννόμων αγαθών και των ελευθεριών των ατόμων. Ταυτόχρονα, η διαδικτυακή παρουσία των ατόμων συνεχώς αυξάνεται ποσοτικά και αναβαθμίζεται ποιοτικά, με συνέπεια να αυξάνονται αντίστοιχα και οι ποινικά κολάσιμες διαδικτυακές συμπεριφορές. Ο διασυνοριακός και ποικιλόμορφος χαρακτήρας του ηλεκτρονικού εγκλήματος δύναται να αντιμετωπιστεί αποτελεσματικά μόνο μέσω της θέσπισης νομοθετικών μέτρων και μέσω της αναβάθμισης του πλαισίου της δικαστικής και αστυνομικής συνεργασίας σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο.

Ειδικότερα, κεντρικό χαρακτηριστικό γνώρισμα του ηλεκτρονικού εγκλήματος είναι ότι αποτελεί αδίκημα απόστασης, καθώς η εκδήλωση της συμπεριφοράς του δράστη απέχει τοπικά από το αξιόποινο αποτέλεσμα. Ο διασυνοριακός χαρακτήρας του ηλεκτρονικού εγκλήματος οφείλεται στη διακίνηση των δεδομένων σε όσους τόπους υπάρχει δυνατότητα διαδικτυακής πρόσβασης, με αποτέλεσμα οι τόποι τέλεσης των οικείων αδικημάτων να τοποθετούνται σε περισσότερα κράτη. Ανακύπτουν έτσι μια σειρά ερωτημάτων. Ειδικότερα, ανακύπτει, πρώτον, το ερώτημα πότε είναι εφαρμοστέοι οι εθνικοί ποινικοί κανόνες του κάθε κράτους, δεύτερον, ποιοι κανόνες ρυθμίζουν και πρέπει να ρυθμίζουν τα ζητήματα αυτά, και, τρίτον, εάν υφίστανται επί του παρόντος ικανοποιητικές λύσεις σε εθνικό ή υπερεθνικό επίπεδο, ώστε οι αρχές επιβολής του

νόμου και οι δικαστικές αρχές να είναι σε θέση να ερευνούν και να καταστέλλουν αποτελεσματικά τις περιπτώσεις ηλεκτρονικού εγκλήματος.

Σκοπός της παρούσας εργασίας είναι να δοθούν απαντήσεις στα ανακύπτοντα ερωτήματα. Στο μέρος Β ερευνάται το ζήτημα του τόπου τέλεσης του ηλεκτρονικού εγκλήματος. Ειδικότερα, αρχικά οριοθετούνται οι έννοιες, οι διακρίσεις και τα ιδιαίτερα χαρακτηριστικά γνωρίσματα των εγκλημάτων στον κυβερνοχώρο. Έπειτα, εξετάζονται οι βασικές αρχές του τόπου τέλεσης των εγκλημάτων, δηλαδή η αρχή της εδαφικότητας, η αρχή της ενότητας της πράξης, οι αρχές του υποκειμενικού και αντικειμενικού ενδιαφέροντος και η αρχή της παγκόσμιας δικαιοσύνης. Τέλος, ερευνάται ο τόπος τέλεσης συγκεκριμένα του ηλεκτρονικού εγκλήματος και η εξάρτηση της εύρεσής του αφενός από το είδος της αξιόποινης πράξης, αφετέρου από τη συγκεκριμένη χρήση της τεχνολογίας. Στο μέρος Γ ερευνώνται ειδικότερα ζητήματα που συναρτώνται με τον χώρο του ηλεκτρονικού εγκλήματος. Πιο συγκεκριμένα, αρχικά εξετάζεται η συμμετοχική ευθύνη των ενδιάμεσων παρόχων διαδικτύου στο ηλεκτρονικό έγκλημα, μέσω της παράθεσης των αναγκαίων ορισμών και των προϋποθέσεων κατάφασης της ευθύνης τους. Εν συνεχεία, ερευνάται ο ρόλος που διαδραματίζουν τα ηλεκτρονικά αποτυπώματα στο ηλεκτρονικό έγκλημα μέσω της εξέτασης των μεθόδων ανώνυμης σύνδεσης στο διαδίκτυο και των ψηφιακών αποτυπωμάτων. Τέλος, ερευνάται η αξία της συνδρομής των ηλεκτρονικών αποδεικτικών στοιχείων (e-evidence) στις ποινικές διαδικασίες και αξιολογούνται τα νέα νομοθετικά μέτρα της ΕΕ για το καθεστώς των ηλεκτρονικών αποδείξεων.

Καταληκτικά, παρατίθενται οι συμπερασματικές σκέψεις και η προσωπική κρίση της γράφουσας, η οποία καταλήγει αφενός πως η οριοθέτηση του τόπου τέλεσης ενός κυβερνοεγκλήματος, ελλείψει ύπαρξης κοινών διεθνών κανόνων, πρέπει να αναζητηθεί στους εθνικούς κανόνες του διεθνούς ποινικού δικαίου. Ωστόσο, η εφαρμογή των εθνικών αυτών κανόνων πρέπει να συμβαδίζει και να είναι προσαρμοσμένη στα ιδιαίτερα χαρακτηριστικά γνωρίσματα του διαδικτύου, με ιδιαίτερη έμφαση στο είδος της αξιόποινης πράξης και στη μορφή της χρησιμοποιούμενης τεχνολογίας. Αφετέρου πως το νέο νομικό πλαίσιο της ΕΕ για τις ηλεκτρονικές αποδείξεις, δοθέντος ότι η δυναμική φύση της τεχνολογίας και το εξελισσόμενο τοπίο του εγκλήματος στον κυβερνοχώρο θέτουν συνεχείς προκλήσεις, κινείται στη σωστή κατεύθυνση, καθώς παρέχει τη δυνατότητα άμεσης επικοινωνίας των δικαστικών και

αστυνομικών αρχών με τους παρόχους, επιτρέποντας την πρόσβαση σε κρίσιμα δεδομένα χρηστών και ενισχύοντας περαιτέρω την ποινική έρευνα του ηλεκτρονικού εγκλήματος.

Β.-Ο ΤΟΠΟΣ ΤΕΛΕΣΗΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Β.1.-Διακρίσεις και χαρακτηριστικά των εγκλημάτων στον Κυβερνοχώρο

Β.1.α.-Οριοθέτηση εννοιών και διακρίσεις

Η Δίωξη Ηλεκτρονικού Εγκλήματος ορίζει ως ηλεκτρονικό έγκλημα τις *«αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία»*.[1] Στην ελληνική έννομη τάξη, πέραν από τον γενικό όρο του ηλεκτρονικού εγκλήματος, χρησιμοποιούνται και δύο ειδικότεροι όροι, του διαδικτυακού εγκλήματος και του εγκλήματος στον κυβερνοχώρο, οι οποίοι όροι ενσωματώνουν το στοιχείο της δικτύωσης.[2]

Με βάση τους όρους αυτούς, τα ηλεκτρονικά εγκλήματα διακρίνονται σε δύο κύριες κατηγορίες:[3] Αφενός στα αδικήματα που τελούνται μέσω της χρήσης ηλεκτρονικών υπολογιστών (computer crime) και αφετέρου στα αδικήματα που τελούνται μέσω του διαδικτύου, τα λεγόμενα κυβερνοεγκλήματα (cyber crime). Τα κυβερνοεγκλήματα μπορούν να διακριθούν περαιτέρω σε γνήσια και σε μη γνήσια εγκλήματα. Γνήσια κυβερνοεγκλήματα συνιστούν εκείνες οι αξιόποινες πράξεις, που τελούνται μέσω δικτύων ηλεκτρονικής επικοινωνίας και συστημάτων πληροφοριών, όπου όμως το στοιχείο αυτό τυποποιείται ειδικά στην αντικειμενική υπόσταση του αδικήματος. Παράδειγμα τέτοιου αδικήματος είναι η διάδοση παιδικού πορνογραφικού υλικού μέσω του κυβερνοχώρου. Μη γνήσια κυβερνοεγκλήματα αποτελούν οι παραδοσιακές μορφές εγκλημάτων, τα οποία διαπράττονται μέσω δικτύων

[1] Ηλεκτρονικά διαθέσιμο σε: www.lawspot.gr/nomikes-plirofories/voithitika-kemena/ilektroniko-egklima
[2] Βλ. *Ε. Μεταξάκη*, Κυβερνοέγκλημα, 2022.
[3] Βλ. Ι. *Αγγελή*, Έγκλημα στον κυβερνοχώρο (Cybercrime - Internet Crime), ΠοινΧρον 2000, σελ. 675 επ.

ηλεκτρονικής επικοινωνίας και συστημάτων πληροφοριών, χωρίς όμως το στοιχείο αυτό να τυποποιείται διακριτά. Παράδειγμα τέτοιου αδικήματος αποτελεί η συκοφαντική δυσφήμιση.

Το ηλεκτρονικό έγκλημα παρουσιάζει τρεις ιδιομορφίες.[4] Αποτελεί μία νέα μορφή εγκλήματος, η τέλεση του οποίου γίνεται μέσω ηλεκτρονικών υπολογιστών, παραλλάσσει ήδη υφιστάμενα αδικήματα που τελούνται μέσω υπολογιστών και εκδηλώνεται ως έγκλημα με την με οποιονδήποτε τρόπο παρεμβολή ηλεκτρονικού υπολογιστή. Με βάση τον τρόπο τέλεσής τους,[5] τα ηλεκτρονικά εγκλήματα διακρίνονται σε αδικήματα που τελούνται σε *«κοινό»* περιβάλλον και στο διαδίκτυο,[6] σε αδικήματα που τελούνται σε περιβάλλον ηλεκτρονικών υπολογιστών χωρίς μεσολάβηση διαδικτύου[7] και σε αδικήματα που τελούνται στον κυβερνοχώρο.[8]

Το κυβερνοέγκλημα έχει ως σημείο αναφοράς τη διασύνδεση του ηλεκτρονικού υπολογιστή και των smartphones σε σύστημα πληροφοριών άλλοτε ως στόχο της επίθεσης, άλλοτε ως βασικό μέσο της επίθεσης και άλλοτε ως βασικό εργαλείο αυτής. Με βάση αυτή την τριμερή διάκριση προκύπτουν τρεις κατηγορίες ποινικών αδικημάτων:[9] Η πρώτη κατηγορία αφορά τα γνήσια πληροφορικά εγκλήματα, τα οποία τελούνται μέσω ηλεκτρονικού υπολογιστή και μέσω συστημάτων πληροφοριών. Η δεύτερη κατηγορία αναφέρεται στα εγκλήματα με ψηφιακό περιεχόμενο, τα οποία σχετίζονται με την διακίνηση παράνομου περιεχομένου μέσω συστημάτων πληροφοριών. Η τελευταία κατηγορία περιλαμβάνει τα εγκλήματα κατά πληροφοριακών συστημάτων, τα οποία διαπράττονται κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριακών συστημάτων και των ψηφιακών δεδομένων, αποτελώντας έτσι υποκατηγορία των κυβερνοεγκλημάτων.

[4] Βλ. *Κ. Βλαχόπουλο*, Ηλεκτρονικό Έγκλημα, Μορφές, Πρόληψη, Αντιμετώπιση, 2007, σελ. 135.
[5] Βλ. *Μ. Καϊάφα- Γκμπάντι*, Ποινικό Δίκαιο και Καταχρήσεις της Πληροφορικής, Αρμ 2007, σελ. 1062.
[6] Βλ. για παράδειγμα άρθρο 363 ΠΚ.
[7] Βλ. για παράδειγμα άρθ.ρο370Γ[1] ΠΚ.
[8] Βλ. για παράδειγμα άρθρο 348Α ΠΚ.
[9] Βλ. *Ι. Αγγελή*, Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, ΠοινΔικ 2001, σελ. 1218.

Β.1.β.-Τα ιδιαίτερα χαρακτηριστικά των εγκλημάτων στον Κυβερνοχώρο

Τα ιδιαίτερα χαρακτηριστικά γνωρίσματα του ηλεκτρονικού εγκλήματος καθιστούν επιτακτική την ανάγκη νομοθέτησης μέσω της προώθησης ειδικών ποινικών νόμων. Ωστόσο, ακριβώς οι ιδιαιτερότητες των χαρακτηριστικών γνωρισμάτων του ηλεκτρονικού εγκλήματος είναι το βασικό σημείο που αποτελεί τροχοπέδη στην επίτευξη αυτού του στόχου.

Οι βασικές ιδιαιτερότητες του ηλεκτρονικού εγκλήματος είναι η εύκολη τέλεσή του σε πολλαπλούς τόπους και με ταχύτατους χρόνους. Τα ειδικότερα χαρακτηριστικά γνωρίσματα αυτού του είδους των εγκλημάτων μπορούν να συνοψιστούν ως εξής:[10]

1) Τελούνται εύκολα από όσους έχουν τις απαιτούμενες γνώσεις.
2) Ανιχνεύονται δύσκολα, καθώς τα ίχνη που αφήνουν είναι ψηφιακά.
3) Για την τέλεσή τους είναι συνήθως απαραίτητες άριστες και εξειδικευμένες γνώσεις.
4) Ο δράστης μπορεί να τελέσει τα αδικήματα αυτά χωρίς να μετακινηθεί, ενεργώντας είτε από το γραφείο, είτε από το σπίτι του, με τη χρήση του ηλεκτρονικού του υπολογιστή.
5) Παρέχεται η δυνατότητα σε συγκεκριμένες κατηγορίες ατόμων, όπως για παράδειγμα οι παιδόφιλοι (περιπτώσεις παιδικής πορνογραφίας - child pornography) να επικοινωνούν γρήγορα μεταξύ τους ή/και σε πραγματικό χρόνο, χωρίς να απαιτηθεί να μετακινούνται, εύκολα και ανέξοδα, καθώς επίσης και να βρίσκονται περισσότεροι μαζί στις ίδιες ομάδες συζητήσεως (news groups), ή μέσα σε chat rooms.
6) Οι *«εγκληματίες του Κυβερνοχώρου»* πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα και αποστέλλουν μηνύματα ηλεκτρονικής αλληλογραφίας με ψευδή στοιχεία.

[10] Βλ. *F. Steven*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, 2006, *Ι. Καρακώστα*, Δίκαιο και internet, 2009.

7) Τελούνται διασυνοριακά και τα αποτελέσματά των αδικημάτων αυτών δύνανται να πραγματοποιούνται ταυτόχρονα σε περισσότερους τόπους.
8) Υπάρχει σοβαρή δυσκολία στον προσδιορισμό του τόπου τέλεσης των αδικημάτων αυτών, στη διερεύνηση και τον εντοπισμό του δράστη. Σύνηθες είναι το φαινόμενο ο δράστης του αδικήματος να εντοπίζεται σε μία χώρα και τα αποδεικτικά στοιχεία να βρίσκονται σε διαφορετική χώρα, ή ακόμα να βρίσκονται ταυτόχρονα σε περισσότερες διαφορετικές και απομακρυσμένες χώρες.
9) Η αποτελεσματική διερεύνηση των εγκλημάτων αυτών απαιτεί κατά κανόνα συνεργασία δύο τουλάχιστον κρατών, αφενός του κράτους όπου έγινε αντιληπτό το αποτέλεσμα της εγκληματικής συμπεριφοράς, αφετέρου του κράτους όπου εντοπίζονται τα αποδεικτικά στοιχεία. Είναι σπάνιες οι περιπτώσεις, όπου τέτοιες εγκληματικές συμπεριφορές εκδηλώνονται στα όρια ενός μόνο κράτους.
10) Η αποτύπωση της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα, διότι ελάχιστες περιπτώσεις τέτοιων αδικημάτων καταγγέλλονται διεθνώς, με συνέπεια το μέγεθος της εγκληματικότητας στο χώρο του Διαδικτύου να εμφανίζεται ακόμα πιο *«σκοτεινό»*, από ότι στον *«κοινό»* εγκληματικό χώρο.

Β.2.-Βασικές αρχές του τόπου τέλεσης του εγκλήματος

Β.2.α.-Η αρχή της εδαφικότητας και η αρχή της ενότητας της πράξης

Η συνεχής εξέλιξη του διαδικτύου και η ανάδειξή του σε κυρίαρχο μέσο επικοινωνίας έχει ως συνέπεια να εμφανίζονται συνεχώς νέες προκλήσεις με την αυξανόμενη εμφάνιση νέων μορφών εγκληματικότητας. Τόσο η ελληνική, όσο και ευρωπαϊκή νομοθεσία αναγκάζονται να προσαρμοστούν σταδιακά σε αυτή τη νέα πραγματικότητα.

Στην ελληνική έννομη τάξη, ο ορισμός των τοπικών ορίων του εγκλήματος πραγματοποιείται στα άρθρα 5 έως 11 του ΠΚ. Ειδικότερα, η αρμοδιότητα των ελληνικών δικαστικών αρχών προσδιορίζεται από τα άρθρα 5, 6, 7 και 8 του ΠΚ, τα οποία ορίζουν τα τοπικά όρια ισχύος των ελληνικών ποινικών νόμων. Στην περίπτωση που η πράξη τελέστηκε συνολικά ή μερικά στην ελληνική επικράτεια, εφαρμόζεται το άρθρο 5 ΠΚ, που ενσωματώνει την αρχή της εδαφικότητας, κατά την οποία το συνδετικό στοιχείο με την ελληνική έννομη τάξη είναι η τέλεση του αδικήματος στο έδαφος της επικρατείας.[11] Η αρχή αυτή αποτελεί έκφανση της σύγχρονης αντίληψης της της θετικής και αρνητικής όψης της κρατικής κυριαρχίας, κατά την οποία αντίληψη η κρατική κυριαρχία, θετικά, εφαρμόζει τους ημεδαπούς ποινικούς νόμους και, αρνητικά, απωθεί την εμπλοκή άλλου κράτους στην εθνική έννομη τάξη της.[12] Αντίθετα, εάν η πράξη τελέστηκε εξ ολοκλήρου στην αλλοδαπή, τότε εφαρμόζονται τα άρθρα 6, 7 και 8 ΠΚ. Καθίσταται έτσι εμφανές ότι η εφαρμογή των διατάξεων αυτών εξαρτάται σε μεγάλο βαθμό από τον καθορισμό του τόπου τέλεσης της εγκληματικής συμπεριφοράς.

---

[11] Βλ. *Χ. Μυλωνόπουλο*, Διεθνές Ποινικό Δίκαιο, Τα τοπικά όρια των ποινικών νόμων, 1993, σελ. 204.

[12] Βλ. *U. Neumann*, Η αρχή της παγκοσμιοποιημένης δικαιοσύνης σε μία παγκοσμιοποιημένη κοινότητα δικαίου, σε: Ι. *Μανδωλεδάκη/C. Prittwitz*, Διεθνοποίηση του ποινικού δικαίου, 2003, σελ. 8.

Για τον καθορισμό του τόπου τέλεσης της πράξης, ο ελληνικός Ποινικός Κώδικας εφαρμόζει την αρχή της ενότητας, θεωρία η οποία αποτυπώνεται στο άρθρο 16 ΠΚ.[13] Σύμφωνα με το άρθρο αυτό, ο τόπος τέλεσης της πράξης είναι τόσο ο τόπος, όπου ο υπαίτιος διέπραξε ολικά ή μερικά την αξιόποινη ενέργεια ή παράλειψη, όσο και ο τόπος όπου επήλθε ή, σε περίπτωση απόπειρας, έπρεπε σύμφωνα με την πρόθεση του υπαιτίου να επέλθει το αξιόποινο αποτέλεσμα.

Νομολογιακά έχει κριθεί πως από την ερμηνεία του άρθρου 16 ΠΚ,[14] προκύπτει ότι τόπος τέλεσης είναι κάθε τόπος, στον οποίο πραγματώθηκε τμήμα της πράξης που ανήκει στην αντικειμενική υπόσταση του εγκλήματος, συμπεριλαμβανόμενου και του τόπου του αποτελέσματος. Έτσι, στην περίπτωση που η πράξη διενεργήθηκε τμηματικά, σε περισσότερους τόπους, τότε τόπος τέλεσης της πράξης είναι ταυτόχρονα και κάθε ένας από τους τόπους αυτούς, διότι κρίσιμο για τον καθορισμό του τόπου τέλεσης ενός εγκλήματος είναι το σύνολο της διαδρομής των γεγονότων, δηλαδή από την αρχή της τέλεσης μέχρι την ολοκλήρωση. Κατά συνέπεια, από τη μία πλευρά τόπος τέλεσης είναι εκείνος ο τόπος, όπου πραγματώθηκε έστω και ένα τμήμα από την αντικειμενική υπόσταση του εγκλήματος, από την άλλη πλευρά, ένα έγκλημα μπορεί να εμφανίζει ταυτόχρονα περισσότερους τόπους τέλεσης.

Στα εγκλήματα απόστασης η ενέργεια του υποκειμένου και το εξ αυτής εγκληματικό αποτέλεσμα απέχουν μεταξύ τους τοπικά και χρονικά. Σύμφωνα με την θεωρία της ενότητας, ο καθορισμός του τόπου τέλεσης των εγκλημάτων αυτών λαμβάνει υπόψη το σύνολο των στοιχείων που συγκροτούν την έννοια της πράξης, δηλαδή τόσο την αξιόποινη ενέργεια ή παράλειψη, όσο και το αξιόποινο αποτέλεσμα. Συνεπώς, τόπος τέλεσης σε αυτήν την κατηγορία αδικημάτων είναι αφενός ο τόπος που εκδηλώθηκε η εγκληματική συμπεριφορά, αφετέρου ο τόπος που πραγματώθηκε το αξιόποινο αποτέλεσμα.[15] Με την αρχή της ενότητας διευρύνεται το πεδίο εφαρμογής των ελληνικών ποινικών νόμων του άρθρου 5[1] ΠΚ, οι οποίοι έτσι επεκτείνονται και καταλαμβάνουν και αδικήματα, τα οποία έχουν εν μέρει τελεστεί στην

[13] Βλ. *Δ. Κιούπη*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, σε *Θ. Δαλακούρα*, Ηλεκτρονικό έγκλημα, ουσιαστικές και δικονομικές όψεις, 2023, σελ. 45 επ.
[14] Βλ. ΑΠ 586/2021, ΤΝΠ ΝΟΜΟΣ.
[15] Βλ. ΠλημμΝαυπλ 78/1991, ΠοινΧρ ΜΒ, σελ. 71.

αλλοδαπή, περιέχοντας ένα στοιχείο εξωεδαφικότητος, χωρίς να απαιτείται η συνδρομή των όρων του άρθρου 6 ΠΚ, όπως για παράδειγμα η συνδρομή του όρου του διπλού αξιοποίνου.[16]

Στο κατ' εξακολούθηση έγκλημα του άρθρου 98 ΠΚ, σύμφωνα με την αρχή της ενότητας, τόπος τέλεσης είναι αυτός που επιχειρήθηκε οποιαδήποτε μερικότερη πράξη, δηλαδή τόσο ο τόπος ολικής ή μερικής εκδήλωσης της συμπεριφοράς, όσο και ο τόπος του αποτελέσματος κάθε επιμέρους πράξης. Συνεπώς, στην περίπτωση που έστω και τμήμα μιας μερικότερης πράξης ενός κατ' εξακολούθηση εγκλήματος τελέστηκε στην ημεδαπή, ή επήλθε στην ημεδαπή το αποτέλεσμα μιας μερικότερης πράξης ενός τέτοιου αδικήματος, τόπος τέλεσης είναι η ημεδαπή, διότι η αρχή της ενότητας αντιμετωπίζει την αξιόποινη πράξη ως ενιαίο και αδιαίρετο σύνολο.[17]

Στην περίπτωση των διαρκών εγκλημάτων, υπό το πρίσμα της αρχής της ενότητας, ως τόπος τέλεσης θεωρείται εκείνος, όπου εξακολουθεί η πραγμάτωση έστω και ενός τμήματος της αντικειμενικής υπόστασης του αδικήματος, ή όπου λαμβάνει χώρα η ουσιαστική αποπεράτωσή του.[18] Συνεπώς, ένα διαρκές έγκλημα που αρχίζει στην ημεδαπή και αποπερατώνεται ουσιαστικά στην αλλοδαπή, θεωρείται ότι τελείται στην Ελλάδα, έστω και αν η επιβαρυντική περίπτωσή του συνέβη στην αλλοδαπή. Αντιστρόφως, τόπος τέλεσης του διαρκούς εγκλήματος είναι η ημεδαπή, όταν στην τελευταία το διαρκές αδίκημα αποπερατώθηκε ουσιαστικά.

Τόσο στο υπαλλακτικά, όσο και στο σωρευτικά μεικτό έγκλημα, ως τόπος τέλεσης θεωρείται κάθε τόπος, όπου πραγματώθηκε έστω και ένας από τους επιμέρους τρόπους τέλεσης του αδικήματος. Συνεπώς, εάν ένας, οποιοσδήποτε, από τους περισσότερους τρόπους τέλεσης του αδικήματος διενεργήθηκε εντός των ορίων της ελληνικής επικράτειας, , τότε το μεικτό έγκλημα θεωρείται ότι τελέστηκε στην ημεδαπή και εφαρμόζονται οι ελληνικοί ποινικοί νόμοι, χωρίς ν' απαιτείται η συνδρομή των όρων του άρθρου 6 ΠΚ.[19]

Αναφορικά με τον τόπο επέλευσης του αποτελέσματος, ως αξιόποινο αποτέλεσμα νοείται αυτό που περιλαμβάνεται στην ειδική υπόσταση του εγκλήματος.[20] Το αποτέλεσμα αυτό υπάρχει σε όλα τα εγκλήματα αποτελέσματος, σε αντίθεση με τα εγκλήματα συμπεριφοράς. Κρίσιμο είναι

[16] Βλ. *Χ. Μυλωνόπουλο*, Διεθνές και Ευρωπαϊκό Ποινικό Δίκαιο, 2021, σελ. 124-125.
[17] Βλ. ΑΠ 286/2019, ΤΝΠ ΝΟΜΟΣ.
[18] Βλ. ΑΠ 905/1981, ΠοινΧρ ΛΒ, σελ. 162.
[19] Βλ. ΑΠ 1500/2006, ΠοινΧρ ΝΖ, σελ. 704.
[20] Βλ. ΑΠ 286/2019, ΤΝΠ ΝΟΜΟΣ.

να εντοπιστεί πότε ένα έγκλημα λειτουργεί ως έγκλημα αποτελέσματος και πότε ως έγκλημα συμπεριφοράς. Ταυτόχρονα, ως αποτέλεσμα δεν θα πρέπει να νοηθεί μόνο η υλική επενέργεια σε ένα υλικό αντικείμενο, όπως για παράδειγμα στο ξένο πράγμα στις περιπτώσεις των αδικημάτων κλοπής, αλλά και η παρέλευση ενός συγκεκριμένου νοήματος σε γνώση αλλού, όπως για παράδειγμα στο έγκλημα της εξύβρισης, το οποίο αποτελεί έγκλημα εξωτερίκευσης.[21]

Ως αξιόποινο αποτέλεσμα νοείται τόσο εκείνο που συνιστά βλάβη του εννόμου αγαθού, δηλαδή τα εγκλήματα βλάβης, όσο και εκείνο που εκδηλώνεται ως συγκεκριμένος κίνδυνος, δηλαδή τα εγκλήματα συγκεκριμένης διακινδύνευσης.[22] Αντίθετα δεν είναι εφικτή η ύπαρξη αξιόποινου αποτελέσματος στα εγκλήματα αφηρημένης διακινδύνευσης,[23] όπου ο κίνδυνος βρίσκεται ποσοτικά και ποιοτικά στην πιο χαλαρή του μορφή. Στις περιπτώσεις αυτές, το αποτέλεσμα της πράξης δεν περιγράφεται στην αντικειμενική υπόσταση του αδικήματος. Ο νομοθέτης ανάγει μια προπαρασκευαστική ενέργεια σε τελειωμένο έγκλημα, αδιαφόρως εάν αυτό έχει επέλθει.

Τα εγκλήματα αφηρημένα συγκεκριμένης ή δυνητικής διακινδύνευσης συνιστούν μία ιδιαίτερη κατηγορία εγκλημάτων, στα οποία ενυπάρχει μία λειτουργική πηγή κινδύνου, ανοιχτή και προσβάσιμη στα έννομα αγαθά, η οποία είναι ικανή δυνητικά να οδηγήσει αυτοδύναμα στη βλάβη τους. Πρόκειται για μία ενδιάμεση κατηγορία, στην οποία απαιτείται η δυνατότητα πρόκλησης κινδύνου, όχι η επέλευσή του, αλλά ούτε και μία γενικώς επικίνδυνη συμπεριφορά.[24] Το ερώτημα εάν η δυνατότητα πρόκλησης κινδύνου μπορεί να αποτελέσει αξιόποινο αποτέλεσμα κατά τις επιταγές του άρθρου 16 ΠΚ και, σε περίπτωση καταφατικής απάντησης, με ποιον τρόπο εντοπίζεται ως τοπικό μέγεθος διαφορετικό από τον τόπο εκδήλωσης της ίδιας της συμπεριφοράς, αποτελεί σημείο αμφισβήτησης.[25]

Ως προς τις ειδικότερες διακρίσεις των αδικημάτων διακινδύνευσης, συνοπτικά, κατά μία πρώτη άποψη,[26] η κατηγορία των εγκλημάτων αφηρημένης διακινδύνευσης απορρίπτεται, διότι δεν

---

[21] Βλ. ΑΠ 2334/2004, ΤΝΠ ΝΟΜΟΣ, αναφορικά με αντίστοιχες σκέψεις ως προς το αδίκημα της υπεξαίρεσης.

[22] Βλ. *Χ. Μυλωνόπουλο*, σε: *Ν. Ανδρουλάκη κ.ά.*, Συστηματική Ερμηνεία Ποινικού Κώδικα, 2005, άρθρο 16, αρ. 4.

[23] Βλ. *Χ. Μυλωνόπουλο*, Ποινικό Δίκαιο - Γενικό Μέρος, Ι, 2007, σελ. 152.

[24] Βλ. *Ι. Γιαννίδη*, σε: *Ν. Ανδρουλάκη κ.ά.*, Συστηματική Ερμηνεία Ποινικού Κώδικα, 2005, άρθρο 14, αρ. 39.

[25] Υπέρ της άποψης ότι υπάρχει αξιόποινο αποτέλεσμα και τόπος τέλεσης σε αυτήν την κατηγορία εγκλημάτων, βλ.. *Χ. Μυλωνόπουλο*, Διεθνές και Ευρωπαϊκό Ποινικό Δίκαιο, 2021, σελ. 137. Αντίθετα, βλ. *Δ. Κιούπη*, Δημοσίευση ιστοσελίδων με αξιόποινο περιεχόμενο, ΠΛογ, 2001, σελ. 402 επ.

[26] Βλ. *Ε. Συμεωνίδου- Καστανίδου*, Η διαβάθμιση του κινδύνου στα εγκλήματα διακινδύνευσης, Τιμ. Τόμος για τον Δ. Σπινέλλη, 2001, σελ. 1064.

δύναται να νοηθεί άδικο λιγότερο από το άδικο της δυνητικής διακινδύνευσης λόγω έλλειψης, στην περίπτωση αυτήν, του οποιουδήποτε συνδέσμου της πράξης είτε με τον έννομο αγαθό απευθείας, είτε με τον χώρο που περιβάλλει το έννομο αγαθό. Σύμφωνα με την άποψη αυτή, ορισμένες πράξεις εξέρχονται από το ποινικό δίκαιο, διότι λείπει το ουσιαστικό άδικο. Τα υπόλοιπα εγκλήματα αφηρημένης διακινδύνευσης χαρακτηρίζονται κατά περίπτωση είτε ως εγκλήματα συγκεκριμένης διακινδύνευσης, είτε ως εγκλήματα δυνητικής διακινδύνευσης ή ως εγκλήματα βλάβης. Κατά μία δεύτερη άποψη,[27] υποστηρίζεται ως ορθότερη η κατάταξη των εγκλημάτων αφηρημένης, δυνητικής και συγκεκριμένης διακινδύνευσης, σε εγκλήματα θεμελίωσης ή συντήρησης πηγής κινδύνου, απόπειρας πρόκλησης κινδύνου και συγκεκριμένου κινδύνου αντίστοιχα. Τέλος, μία τρίτη άποψη,[28] διακρίνει μεταξύ των εγκλημάτων κινδύνου, στα οποία ο κίνδυνος αποτελεί μια αντικειμενική κατάσταση, και των εγκλημάτων επικινδυνότητας, στα οποία τιμωρείται μια ορισμένη ποιότητα συμπεριφοράς που αξιολογείται ως επικίνδυνη.

Συνεπώς, με βάση τον συνδυασμό της αρχής της εδαφικότητας και της αρχής της ενότητας, που έχει επιλέξει ο Έλληνας νομοθέτης, ως τόπος τέλεσης νοείται τόσο ο τόπος που ενήργησε, ή παρέλειψε να ενεργήσει, ο δράστης, όσο και ο τόπος που επήλθε το αξιόποινο αποτέλεσμα. Στη συμπεριφορά του δράστη, περιλαμβάνονται όλες οι πράξεις από την αρχή εκτέλεσης έως και την περάτωση. Αναφορικά με το αξιόποινο αποτέλεσμα, διακρίνονται τρεις περιπτώσεις ανάλογα με την κατάταξη των εγκλημάτων σε εγκλήματα αποτελέσματος, συγκεκριμένης διακινδύνευσης, αφηρημένης διακινδύνευσης και αφηρημένα συγκεκριμένης ή δυνητικής διακινδύνευσης. Ειδικότερα, στις δύο πρώτες κατηγορίες αδικημάτων υπάρχει το αποτέλεσμα που συνιστά τόπο τέλεσης. Στην τρίτη κατηγορία εγκλημάτων, κατά την κρατούσα άποψη, δεν υπάρχει αποτέλεσμα που συνιστά τόπο τέλεσης του εγκλήματος, ενώ στην τελευταία, προβληματική, κατηγορία αδικημάτων, οι απόψεις διίστανται.[29]

[27] Βλ. *Μ. Καϊάφα- Γκμπάντι*, Κοινώς επικίνδυνα εγκλήματα, 2005, σελ. 84.
[28] Βλ. *Ν. Ανδρουλάκη*, Ποινικό δίκαιο, Γενικό Μέρος, 2006, σελ. 174 επ.
[29] Βλ. *Δ. Κιούπη*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, σε *Θ. Δαλακούρα*, Ηλεκτρονικό έγκλημα, ουσιαστικές και δικονομικές όψεις, 2023, σελ. 47-48.

Β.2.β.-Οι αρχές του υποκειμενικού και αντικειμενικού ενδιαφέροντος και η αρχή της παγκόσμιας δικαιοσύνης

Εκτός από την αρχή της εδαφικότητας, η οποία κατέχει κυρίαρχο ρόλο στον καθορισμό των τοπικών ορίων ισχύος των ημεδαπών ποινικών νόμων, το ελληνικό ποινικό δίκαιο, στα άρθρα 6-8 ΠΚ, έχει υιοθετήσει από τον χώρο του διεθνούς δικαίου τις αρχές του υποκειμενικού και αντικειμενικού ενδιαφέροντος και την αρχή της παγκόσμιας δικαιοσύνης.

Ειδικότερα, σύμφωνα με τη διάταξη του άρθρου 6 ΠΚ, οι ελληνικοί ποινικοί νόμοι εφαρμόζονται στις περιπτώσεις, όπου κάποιο έγκλημα τελέστηκε στην αλλοδαπή, εφόσον δράστης ήταν ημεδαπός. Παράλληλα, θα πρέπει η πράξη να θεωρείται αξιόποινη και κατά τους νόμους του αλλοδαπού τόπου τέλεσης. Για τη δίωξη των εγκλημάτων που τελέστηκαν από ημεδαπό στην αλλοδαπή, απαιτείται πάντοτε, ακόμη και στα αυτεπαγγέλτως διωκόμενα εγκλήματα, έγκληση του παθόντος ή αίτηση της Κυβέρνησης της χώρας όπου τελέστηκε η πράξη. Η διάταξη αυτή τέθηκε χάριν της αλληλεγγύης μεταξύ των κρατών και κατατείνει στην τιμωρία του υπαιτίου και την αποφυγή της ανεπίτρεπτης ατιμωρησίας, με άμεσο στόχο την ομαλή κοινωνική συμβίωση.[30]

Η διάταξη του άρθ. 6 ΠΚ συνιστά εφαρμογή της αρχής του υποκειμενικού ενδιαφέροντος,[31] σύμφωνα με την οποία απαραίτητο στοιχείο για την άσκηση δικαιοδοσίας των ελληνικών ποινικών δικαστηρίων είναι η ιθαγένεια του δράστη, ο οποίος πρέπει είτε να ήταν Έλληνας πολίτης κατά την τέλεση της πράξης, είτε να απέκτησε την ελληνική ιθαγένεια εκ των υστέρων.

[30] Βλ. ΠλημμΑθ 3087/2022, ΤΝΠ ΝΟΜΟΣ.
[31] Βλ. *Μ. Μαργαρίτη/Α. Μαργαρίτη*, Ποινικός Κώδικας Ερμηνεία – Εφαρμογή, έκδοση 4η, 2020.

Με τη διάταξη του άρθρου 6 ΠΚ προβλέπεται η εφαρμογή του ελληνικού ποινικού νόμου κατά την εκδίκαση τελεσθέντος στην αλλοδαπή από ημεδαπό ποινικού αδικήματος, υπό τον όρο ότι το χαρακτηριζόμενο ως κακούργημα ή πλημμέλημα είναι αξιόποινο και κατά τους νόμους της αλλοδαπής χώρας, στο έδαφος της οποίας τελέστηκε το αδίκημα. Η πρόβλεψη αυτή συνιστά εξωτερικό όρο του αξιοποίνου, δεδομένου ότι βρίσκεται εκτός της αντικειμενικής υπόστασης του προβλεπόμενου από τον ελληνικό ποινικό νόμο αδικήματος και δεν περιλαμβάνεται στον άδικο χαρακτήρα της πράξης, αλλά ούτε και στον καταλογισμό.

Ο όρος του διττού αξιοποίνου εντάσσεται στην έννοια των θετικών προϋποθέσεων του εγκλήματος και ανάγεται στην ενοχή του κατηγορουμένου. Δεν ασκεί επιρροή το γεγονός ότι ο όρος αυτός εμπεριέχεται σε άλλη διάταξη, η οποία αφορά γενική ρύθμιση, που σχετίζεται με τα τοπικά όρια της ισχύος των ποινικών νόμων στην ημεδαπή και στην αλλοδαπή, ούτε και το γεγονός ότι δεν αναγράφεται ο όρος αυτός ως τμήμα της σχετικής διάταξης, με την οποία προσδιορίζονται τα επιμέρους στοιχεία του συγκεκριμένου αδικήματος.

Σε περίπτωση κατά την οποία η εγκληματική πράξη χαρακτηρίζεται στο ελληνικό ποινικό δίκαιο ως κακούργημα, για να διεξαχθεί η ποινική δίωξη κατά ημεδαπού για την πράξη που τελέστηκε στην αλλοδαπή, αρκεί η τελευταία να χαρακτηρίζεται απλώς ως αξιόποινη από τον αλλοδαπό ποινικό νόμο. Στην περίπτωση αυτήν, δεν είναι κρίσιμος ο χαρακτηρισμός της πράξης από τον αλλοδαπό ποινικό νόμο ως κακουργήματος ή πλημμελήματος, ούτε η ποινή που απειλείται για το αδίκημα, δοθέντος ότι η ποινική διαδικασία διεξάγεται με βάση το ελληνικό ποινικό δίκαιο.[32]

Η διάταξη του άρθρου 7 ΠΚ ορίζει τις προϋποθέσεις υπό τις οποίες οι ελληνικοί ποινικοί νόμοι εφαρμόζονται όταν το έγκλημα τελείται στην αλλοδαπή από ημεδαπό. Με τη διάταξη αυτήν, ο Έλληνας νομοθέτης εφαρμόζει την αρχή του αντικειμενικού ενδιαφέροντος.[33]

Σύμφωνα με τη διάταξη του άρθρου 7 ΠΚ, οι ελληνικοί ποινικοί νόμοι εφαρμόζονται και κατά αλλοδαπού, για πράξη που τελέστηκε στον αλλοδαπή και που χαρακτηρίζεται από το ελληνικό ποινικό δίκαιο ως κακούργημα ή πλημμέλημα, αν η πράξη αυτή στρέφεται σε βάρος Έλληνα πολίτη και αν είναι αξιόποινη και κατά του νόμους της χώρας όπου τελέστηκε, ή αν διαπράχθηκε

[32] Βλ. ΠλημμΑθ. 3087/2022, ΤΝΠ ΝΟΜΟΣ.
[33] Βλ. Αιτιολογική Έκθεση του νέου ΠΚ, σελ. 9, άρθρο 7.

σε πολιτειακά ασύντακτη Χώρα. Για την εφαρμογή του άρθρου 7 ΠΚ ο δράστης πρέπει να είναι αλλοδαπός, το θύμα ημεδαπός και το αδίκημα πρέπει να είναι αξιόποινο σύμφωνα και με το δίκαιο του τόπου, όπου τελέστηκε. Υπό το πρίσμα των εξαιρέσεων που τάσσουν τα άρθρα 5[2] και 8 Π.Κ., η προϋπόθεση αυτή αποτελεί εξωτερικό όρο του αξιοποίνου και η έλλειψη της καθιστά την πράξη μη αξιόποινη.[34] Στην περίπτωση αυτή, το δικαστήριο κηρύσσει αθώο τον κατηγορούμενο και το δικαστικό συμβούλιο αποφαίνεται να μη γίνει κατηγορία.[35]

Κατά το άρθρο 9 ΠΚ, η ποινική δίωξη για πράξη που τελέστηκε στην αλλοδαπή αποκλείεται σε τρεις περιπτώσεις: Πρώτον, στην περίπτωση που ο υπαίτιος δικάστηκε για την πράξη αυτή στην αλλοδαπή και αθωώθηκε, ή αν σε περίπτωση που καταδικάστηκε έχει εκτίσει ολόκληρη την ποινή του. Δεύτερον, στην περίπτωση που σύμφωνα με τον αλλοδαπό νόμο η πράξη έχει παραγραφεί ή η ποινή που επιβλήθηκε έχει παραγραφεί ή χαριστεί και, τρίτον, στην περίπτωση που σύμφωνα με τον αλλοδαπό νόμο χρειάζεται έγκληση για την δίωξη και τέτοια έγκληση είτε δεν υποβλήθηκε, είτε ανακλήθηκε.[36] Οι πιο πάνω διατάξεις δεν εφαρμόζονται για τα εγκλήματα που προβλέπει το άρθρο 8, ούτε και στις περιπτώσεις που προβλέπει το άρθρο 5[2] ΠΚ.

Το άρθρο 9 καθιερώνει την αρχή της διευθετήσεως και απαριθμεί τις περιπτώσεις, στις οποίες αποκλείεται η ποινική δίωξη για πράξεις που τελέστηκαν στην αλλοδαπή από ημεδαπό ή αλλοδαπό και για τις οποίες υπάρχει ποινική εξουσία με βάση τα άρθρα 6 και 7 Π.Κ.[37] Με το άρθρο αυτό εισάγεται δικονομικό κώλυμα προκειμένου να αποφευχθεί η διπλή τιμώρηση του υπαιτίου (ne bis in idem ή double jeopardy). Σε περίπτωση συνδρομής του δικονομικού αυτού κωλύματος η δίωξη κηρύσσεται απαράδεκτη. Σε περίπτωση καταδίκης, το άρθρο 9 εφαρμόζεται μόνο αν ο υπαίτιος εξέτισε ολόκληρη την ποινή του.[38] Αν η ποινή εκτίθηκε μερικά και όχι ολόκληρη, εφαρμόζεται το άρθρο 10 ΠΚ, το οποίο εισάγει την αρχή του συνυπολογισμού ή συμψηφισμού των ποινών. Η ποινή δεν θεωρείται ότι εκτίθηκε ολόκληρη, αν ο καταδικασθείς απολύθηκε με όρο, ή αν του χορηγήθηκε αναστολή εκτέλεσης.[39]

[34] Βλ. ΑΠ 136/2004, ΤΝΠ ΝΟΜΟΣ.
[35] Βλ. ΑΠ 318/2019, ΑΠ 1613/2000, ΤΝΠ ΝΟΜΟΣ.
[36] Βλ. ΠλημμΑθ 1794/2008, ΤΝΠ ΝΟΜΟΣ.
[37] Βλ. Ολομ ΑΠ 7/2002, ΠοινΧρ ΝΒ, σελ. 704.
[38] Βλ. ΠλημμΑθ 3169/1975, ΠοινΧρ Λ, σελ. 85.
[39] Βλ. ΕφΑΘ 226/1982, ΠοινΧρ ΛΒ, σελ. 434, ΑΠ 761/1975, ΠοινΧρ ΚΣΤ, σελ. 150.

Τέλος, στο άρθρο 8 ΠΚ ο νομοθέτης εφαρμόζει την αρχή της παγκόσμιας δικαιοσύνης μέσα από έναν κατάλογο συγκεκριμένων εγκλημάτων, στα οποία εφαρμόζονται οι ελληνικοί ποινικοί νόμοι και τα ελληνικά ποινικά δικαστήρια μπορούν να ασκήσουν τη δικαιοδοσία τους, ανεξαρτήτως αν τα αδικήματα αυτά τελέστηκαν από ημεδαπό ή αλλοδαπό. Ωστόσο, τα εν λόγω εγκλήματα θα πρέπει να έχουν τελεστεί εξ ολοκλήρου στην αλλοδαπή, διότι αν τελέστηκαν, έστω και μερικώς στην Ελλάδα, τότε εφαρμόζεται το άρθρο 5 ΠΚ.

Η βασικότερη διαφορά του άρθρου 8 ΠΚ από τα προηγούμενα άρθρα είναι το γεγονός ότι στις περιπτώσεις του άρθρου 8 δεν απαιτείται η ύπαρξη της προϋπόθεσης του διπλού αξιοποίνου, δηλαδή είναι αδιάφορο αν οι συγκεκριμένες πράξεις που αναφέρονται στο άρθρο 8 θεωρούνται αξιόποινες και διώκονται και κατά τον ποινικό νόμο του τόπου τέλεσης. Νομολογιακά πάντως γίνεται δεκτό ότι η άσκηση του δικαιώματος ποινικής δίωξης με βάση την αρχή του άρθρου 8 πρέπει να έχει επικουρικό χαρακτήρα και να ασκείται με φειδώ, ώστε να αποκλείεται η αυθαίρετη επέκταση των ημεδαπών ποινικών νόμων σε πράξεις που άπτονται περισσότερο των ποινικών δικαιοδοσιών ξένων κρατών.[40]

Εν κατακλείδι, για να προσδιοριστεί αν ένα έγκλημα έχει τελεστεί στην ημεδαπή ή στην αλλοδαπή και, κατ᾽ επέκταση, για τον καθορισμό της ισχύος των ελληνικών ποινικών νόμων, σημασία έχει, εκτός των άλλων, ο καθορισμός του τόπου ή των τόπων τέλεσης της πράξης. Έτσι, για ένα έγκλημα που έχει τελεστεί στην αλλοδαπή από ημεδαπό, κατά το άρθρο 6 ΠΚ, οι ελληνικοί ποινικοί νόμοι εφαρμόζονται, υπό τις προϋποθέσεις ότι πρόκειται, κατά τον ελληνικό ποινικό νόμο, για κακούργημα ή πλημμέλημα, η πράξη είναι αξιόποινη και κατά τους νόμους της χώρας που τελέστηκε ή διαπράχθηκε σε πολιτειακά ασύντακτη χώρα και, στην περίπτωση που πρόκειται για πλημμέλημα κατά τον ελληνικό ποινικό νόμο, να έχει υποβληθεί έγκληση του παθόντος ή αίτηση της κυβέρνησης της χώρας του τόπου τέλεσης.

Κατά το άρθρο 8 ΠΚ, οι ελληνικοί ποινικοί νόμοι εφαρμόζονται και για ορισμένες πράξεις που τελέστηκαν στην αλλοδαπή και στρέφονται εναντίον ορισμένων ανθρώπινων συμφερόντων, χωρίς να έχει σημασία η υπηκοότητα του δράστη ή του θύματος και χωρίς να παίζει ρόλο αν είναι ή όχι αξιόποινες κατά τους νόμους της χώρας, στην οποία τελέστηκαν. Αν, όμως, ένα έγκλημα

[40] Βλ. ΑΠ 752/2017, ΤΝΠ ΝΟΜΟΣ.

έχει τελεστεί και στην ημεδαπή και στην αλλοδαπή, είτε γιατί η εγκληματική δραστηριότητα αναπτύχθηκε στην αλλοδαπή, το αποτέλεσμά της όμως πραγματώθηκε στην Ελλάδα ή και αντίστροφα, είτε γιατί η εγκληματική δραστηριότητα πραγματώθηκε σταδιακά σε περισσότερους τόπους στην αλλοδαπή και την ημεδαπή, τότε το έγκλημα αυτό, που, ασφαλώς, ενδιαφέρει την ημεδαπή έννομη τάξη, υπάγεται στους ελληνικούς ποινικούς νόμους και δεν είναι αναγκαία η συνδρομή των προϋποθέσεων του άρθρου 6 ή του άρθρου 8 ΠΚ.[41]

Β.3.-Ο τόπος τέλεσης του ηλεκτρονικού εγκλήματος

Το διαδικτυακό έγκλημα, αποτελεί τις περισσότερες φορές έγκλημα απόστασης, καθώς ο δράστης δεν έρχεται σε προσωπική επαφή με το θύμα. Το στοιχείο της απόστασης, που χαρακτηρίζει τα διαδικτυακά εγκλήματα, γεννά προβληματισμούς, στις περιπτώσεις όπου τα εγκλήματα αυτά εκτείνονται έξω από τα όρια της εθνικής έννομης τάξης και δυσχεραίνει τον προσδιορισμό του τόπου τέλεσής τους. Ο προσδιορισμός του τόπου τέλεσης του διαδικτυακού εγκλήματος είναι καθοριστικός, καθώς από αυτόν εξαρτάται ο προσδιορισμός του εφαρμοστέου δικαίου και η δικαιοδοσία των αρμόδιων ποινικών δικαστηρίων.[42]

Για να αντιμετωπιστούν τα προβλήματα που ανέκυψαν από την άνθιση του διαδικτυακού εγκλήματος, ο Έλληνας νομοθέτης εισήγαγε ειδική νομοθεσία. Συγκεκριμένα, με το ν. 1805/1988 προστέθηκε εμβόλιμα στον ελληνικό Ποινικό Κώδικα δεύτερο εδάφιο στο άρθρο 13[γ], καθώς επίσης προστέθηκε και το άρθρο 370Β, το άρθρο 370Γ και το άρθρο 386Α. Με τον τρόπο αυτόν έγινε ένα σημαντικό βήμα προς την καταπολέμηση ορισμένων εγκλημάτων που συνδέονται με την πληροφορική και τη χρήση ηλεκτρονικών υπολογιστών.[43]

Σημαντικό ρόλο στην αντιμετώπιση του κυβερνοεγκλήματος διαδραμάτισε αφενός η Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα,[44] αφετέρου Οδηγίες της ΕΕ, οι οποίες

[41] Βλ. ΑΠ 1177/2019, ΤΝΠ ΝΟΜΟΣ.

[42] Βλ. *Δ. Κιούπη*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, σε *Θ. Δαλακούρα*, Ηλεκτρονικό έγκλημα, ουσιαστικές και δικονομικές όψεις, 2023, σελ. 48.

[43] Βλ. *Ι. Ιγγλεζάκη*, Δίκαιο Πληροφορικής, 4η εκδ., 2021, σ. 403-405.

[44] Αναλυτικά επί της Σύμβασης, βλ. *Θ. Δαλακούρα*, Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν 4411/2016) , σε *Θ. Δαλακούρα*, Ηλεκτρονικό έγκλημα, ουσιαστικές και δικονομικές όψεις, 2023, σελ. 1 επ.

ενσωματώθηκαν στην ελληνική έννομη τάξη, όπως η Οδηγία της ΕΕ 2016/1148 *«σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση»*, η οποία τέθηκε σε ισχύ τον Αύγουστο του 2016 και ενσωματώθηκε στο ελληνικό δίκαιο με τον Ν. 4577/2018. Επίσης, ο Έλληνας νομοθέτης προχώρησε σε μία πρωτοτυπία με τη θέσπιση του Ν. 4267/2014, η οποία όπως αποδείχθηκε, δεν αποτέλεσε ικανοποιητική λύση για τον προσδιορισμό του τόπου τέλεσης του διαδικτυακού εγκλήματος.

Ειδικότερα, με το Ν. 4267/2014 προστέθηκε τρίτη παράγραφος στο άρθρο 5 ΠΚ, η οποία θέσπιζε τα κριτήρια για τον προσδιορισμό του τόπου τέλεσης του διαδικτυακού εγκλήματος. Σύμφωνα με την προϊσχύουσα μορφή του άρθρου 5[3] ΠΚ, *«όταν η πράξη τελείται μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, τόπος τέλεσης θεωρείται και η ελληνική επικράτεια, εφόσον στο έδαφος της παρέχεται πρόσβαση στα συγκεκριμένα μέσα, ανεξάρτητα από τον τόπο εγκατάστασής τους».* Με την διάταξη αυτήν, ο Έλληνας νομοθέτης καθιέρωσε όχι αποκλειστική διεθνή δικαιοδοσία για τα ελληνικά δικαστήρια για όσες αξιόποινες πράξεις τελούνται μέσω διαδικτύου από αλλοδαπούς, αλλά συντρέχουσα δικαιοδοσία των ελληνικών δικαστηρίων, ενόψει του ότι θεωρήθηκε ως τόπος τέλεσης τέτοιων αδικημάτων και η ελληνική επικράτεια.[45]

Με βάση το προϊσχύον άρθρο 5[3] ΠΚ, η ημεδαπή θεωρείται τόπος τέλεσης για όλα τα εγκλήματα που τελούνται στο διαδίκτυο και στα οποία παρέχεται από την Ελλάδα πρόσβαση σε μέσα, όπως είναι οι ιστοσελίδες, οι λογαριασμοί σε υπηρεσίες κοινωνικής δικτύωσης, κλπ. Ωστόσο, μία τέτοια διάταξη όχι μόνο διευρύνει τα όρια της *«ημεδαπής»*, αλλά παράλληλα δημιουργεί και σύγκρουση δικαιοδοσιών, καθώς η υιοθέτηση της λύσης αυτής και από άλλες έννομες τάξεις θα άγει στην τιμώρηση του διαδικτυακού εγκλήματος παντού, με εμφανή τον κίνδυνο καταστρατήγησης βασικών συνταγματικών αρχών.[46]

Για τους λόγους που προεκτέθηκαν, καθώς και για άλλες αντιρρήσεις που εκφράστηκαν στη θεωρία σχετικά με την αδικαιολόγητη επέκταση της αρχής της εδαφικότητας,[47] με το ν. 4619/2019 επήλθε η κατάργηση της τρίτης παραγράφου του άρθρου 5 ΠΚ. Έτσι, επανήλθε η

[45] Βλ. ΑΠ 2080/2017, ΤΝΠ ΝΟΜΟΣ.

[46] Βλ. *Δ. Κιούπη*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος και η απροσδόκητη διεύρυνση της έννοιας της «ημεδαπής» (άρθρο 5 παρ. 3 ΠΚ), ΠοινΧρ, 2014, σελ 561 επ., Γ. Ζέκο, Διαδίκτυο και τεχνητή νοημοσύνη στο ελληνικό δίκαιο, 2022, σελ. 395.

[47] Βλ. Αιτιολογική Έκθεση νέου ΠΚ, σελ. 4.

εφαρμογή του άρθρου 16 ΠΚ και της αρχής της ενότητας, όπου ως τόπος τέλεσης της πράξης θεωρείται τόσο ο τόπος, όπου ο υπαίτιος διέπραξε ολικά ή μερικά την αξιόποινη ενέργεια ή παράλειψη, όσο και ο τόπος όπου επήλθε ή, σε περίπτωση απόπειρας, έπρεπε σύμφωνα με την πρόθεση του υπαιτίου να επέλθει, το αξιόποινο αποτέλεσμα.

Στο οικείο μας δικαιικό σύστημα, μέχρι πρότινος, το ζήτημα αντιμετωπιζόταν με τα άρθρα 5 έως 11 ΠΚ, εξαιρουμένων των αδικημάτων που περιλαμβάνονται στο άρθρο 8 ΠΚ περί παγκόσμιας δικαιοσύνης.[48] Ωστόσο, για να μπορέσει να εξαχθεί ένας ασφαλές συμπέρασμα σχετικά με τον τόπο τέλεσης του εγκλήματος, είναι σημαντικό να ληφθεί υπόψη η διάκριση των εγκλημάτων σε εγκλήματα συμπεριφοράς και αποτελέσματος, βλάβης και διακινδύνευσης, καθώς και η συγκεκριμένη κάθε φορά τεχνολογία που χρησιμοποιείται από το δράστη. Η διαδικασία προσδιορισμού του τόπου τέλεσης των διαδικτυακών εγκλημάτων διευκολύνθηκε περαιτέρω από τον συνδυασμό της αρχής της εδαφικότητας και της αρχής της ενότητας της πράξης. Ειδικότερα, όλα τα διαδικτυακά εγκλήματα που περιέχουν αξιόποινο αποτέλεσμα, είτε με τη μορφή της βλάβης, είτε με τη μορφή του κινδύνου, το οποίο αποτέλεσμα επέρχεται στην ημεδαπή, έχουν ως τόπο τέλεσης, δηλαδή τελούνται, στην ημεδαπή.

[48] Βλ. *Χ. Μυλωνόπουλο*, Διεθνές Ποινικό Δίκαιο, Τα τοπικά όρια των ποινικών νόμων, 1993, σελ. 203 επ. και 284 επ.

Β.3.α.-Η εξάρτηση του τόπου τέλεσης από το είδος της αξιόποινης πράξης

Η απόσταση που χαρακτηρίζει το διαδικτυακό έγκλημα, λόγω της χρήσης της τεχνολογίας, δημιουργεί την ανάγκη εύρεσης ικανοποιητικών λύσεων, στις περιπτώσεις που η απόσταση αυτή ξεπερνά τα εθνικά σύνορα και οδηγεί σε επέκταση του τόπου τέλεσης μιας πράξης σε διαφορετικές έννομες τάξεις.[49] Για την εύρεση του τόπου τέλεσης μιας πράξης, που τελείται μέσω του διαδικτύου, είναι αναγκαίο να εξειδικεύσουμε την συγκεκριμένη κάθε φορά αξιόποινη πράξη ad hoc και να την εντάξουμε σε μία από τις κατηγορίες εγκλημάτων, που αναφέρθηκαν ανωτέρω. Έτσι, διαφορετικός είναι ο τόπος τέλεσης ενός διαδικτυακού εγκλήματος αποτελέσματος και διαφορετικός ο τόπος τέλεσης ενός διαδικτυακού εγκλήματος αφηρημένης διακινδύνευσης.[50] Ειδικότερα, αναφορικά με τα εγκλήματα αποτελέσματος, ως τόπος συμπεριφοράς του δράστη νοείται τόσο ο φυσικός χώρος, οπού αυτός ενήργησε, δηλαδή ο χώρος όπου ο δράστης χρησιμοποίησε τον υπολογιστή του, όσο και ο χώρος, οπού ο δράστης ολοκλήρωσε την συμπεριφορά του με την δημοσίευση των δεδομένων του, δηλαδή ο χώρος όπου φιλοξενούνται τα δεδομένα από τους διακομιστές.[51]

---

[49] Βλ. *Δ. Κιούπη*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, σε *Θ. Δαλακούρα*, Ηλεκτρονικό έγκλημα, ουσιαστικές και δικονομικές όψεις, 2023, σελ. 48.

[50] *Βλ. Δ. Κιούπη*, Ποινικό δίκαιο και internet, 1999, σελ. 88 επ.

[51] βλ. *Δ. Κιούπη*, Δημοσίευση ιστοσελίδων με αξιόποινο περιεχόμενο, ΠΛογ, 2001, σελ. 407.

Πράγματι, σε αρκετές ειδικές υποστάσεις αδικημάτων, η συμπεριφορά του δράστη ολοκληρώνεται και αποκτά περιεχόμενο με την ανάρτηση των δεδομένων, δηλαδή με τη δημοσιοποίησή τους. Περαιτέρω, όταν γίνεται αναφορά σε διαδικτυακή συμπεριφορά, αυτή θα πρέπει να νοείται με τις αντίστοιχες παραμέτρους και όχι με τις παραμέτρους της φυσικής παρουσίας του παραδοσιακού εγκλήματος. Ο δράστης που δημοσιεύει δεδομένα μέσω διαδίκτυού πράττει σε δύο τόπους. Στον τόπο, όπου είναι σωματικά παρών, αλλά και στον τόπο όπου αποθηκεύει τα δεδομένα, καθώς ο τελευταίος είναι ο μόνος τόπος από τον οποίο μπορούν να αποκτούν πρόσβαση οι χρήστες. Ο δράστης μπορεί να μην είναι σωματικά παρών, αλλά διαθέτει όλους τους τρόπους να αποκτά πρόσβαση αμέσως στα δεδομένα του. Το διαδικτυακό έγκλημα συνιστά τελικώς μια πράξη, την οποία ο υπαίτιος διαπράττει εν μέρει στον χώρο της φυσικής του παρουσίας και εν μέρει στον χώρο, οπού βρίσκονται οι διακομιστές.[52]

Καθίσταται αντιληπτό ότι η διαδικτυακή συμπεριφορά του δράστη δεν εξαντλείται στον τόπο της φυσικής του παρουσίας, αλλά εκτείνεται και στον τόπο που ο ίδιος, με χρήση λογισμικού, αποθηκεύει τα ψηφιακά δεδομένα, καθιστώντας έτσι το περιεχόμενό τους προσιτό στους άλλους. Έτσι όμως διευρύνεται υπερβολικά ο αξιόποινος χαρακτήρας της πράξης, αφού ο δράστης καλείται να αντιμετωπίσει έννομες τάξεις που δεν γνώριζε, ή δεν μπορούσε να προβλέψει ότι θα αντιμετώπιζε και με τον τρόπο αυτόν θίγεται η έννοια του ηθελημένου αποτελέσματος. Υπό το πρίσμα αυτό, θα πρέπει να αποτραπεί μια υπερβολική επέκταση των τοπικών ορίων ισχύος των εθνικών νομών και να ενταχθούν στην ποινική δικαιοδοσία, όχι όλες οι πράξεις του διαδίκτυού, αλλά μόνον όσες παρουσιάζουν έναν άμεσο και ουσιαστικό δεσμό με την ημεδαπή. Αυτό σημαίνει ότι, οι οποίες λύσεις δίνονται σε εθνικό επίπεδο, δεν μπορούν να παραβλέπουν τις συνέπειες που συνεπάγονται στο πεδίο του διεθνούς δίκαιου.[53]

Στην περίπτωση ενός εγκλήματος που τελείται μέσω διαδικτύου, μετά την κατάργηση της τρίτης παραγράφου του άρθρου 5 του προϊσχύσαντος ΠΚ, όταν πρόκειται για εγκλήματα βλάβης ή συγκεκριμένης διακινδύνευσης, αυτά διώκονται κατά το άρθρο 5 ΠΚ, εφόσον η βλάβη ή ο συγκεκριμένος κίνδυνος βλάβης έλαβε χώρα στην ημεδαπή, ενώ όταν πρόκειται για εγκλήματα

[52] Βλ. *Δ. Κιούπη*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, σε Θ. *Δαλακούρα*, Ηλεκτρονικό έγκλημα, ουσιαστικές και δικονομικές όψεις, 2023, σελ. 51-52.

[53] Βλ. *Δ. Κιούπη*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, σε *Θ. Δαλακούρα*, Ηλεκτρονικό έγκλημα, ουσιαστικές και δικονομικές όψεις, 2023, σελ. 53-54.

που τελούνται με ενέργεια, αυτά διώκονται κατά το άρθρο 5 ΠΚ, εφόσον η αξιόποινη ενέργεια έλαβε χώρα στο σύνολό της ή μερικώς στην Ελλάδα.[54] Όσον αφορά τα αδικήματα αφηρημένης και δυνητικής διακινδύνευσης, δεδομένου ότι ο νομοθέτης δεν απαιτεί την επέλευση ενός συγκεκριμένου κίνδυνου, ούτε αρκείται στην απλή περιγραφή μιας συμπεριφοράς την οποία θεωρεί επικίνδυνη, θα αποτελούσε υπερβολική διεύρυνση του αξιοποίνου η νομιμοποίηση ως τοπικά αρμόδιου κάθε κράτους, στο οποίο θα μπορούσε να επέλθει ο δυνητικός κίνδυνος.

Β.3.β.-Η εξάρτηση του τόπου τέλεσης από τη συγκεκριμένη χρήση της τεχνολογίας

Ένας επιπρόσθετος λόγος για τον οποίο θα πρέπει κάθε φορά να εξατομικεύεται και να συγκεκριμενοποιείται έκαστο διαδικτυακό έγκλημα ad hopc είναι η διαφοροποίηση στην τεχνολογία που χρησιμοποιείται. Διαφορετική είναι η αντιμετώπιση μιας διμερούς συνομιλίας μέσω διαδικτύου, όπως για παράδειγμα μέσω ηλεκτρονικού ταχυδρομείου, από την αντιμετώπιση μίας ανάρτησης σε μία ιστοσελίδα, στην οποία έχει πρόσβαση ένας αόριστος αριθμός προσώπων. Στις περιπτώσεις αυτές, η διαφοροποίηση έγκειται στη συγκεκριμένη χρήση της εκάστοτε τεχνολογίας και όχι στο είδος της πράξης.[55]

Η εξέταση της συγκεκριμένης κάθε φορά τεχνολογίας που χρησιμοποιείται από τον δράστη έχει κυρίαρχη θέση στον ορισμό του τόπου τέλεσης του διαδικτυακού εγκλήματος. Η επικοινωνία μέσω διαδικτύου μπορεί να λάβει πολλές και διαφορετικές μορφές. Για παράδειγμα, ένα πρόσωπο στέλνει μήνυμα ηλεκτρονικού ταχυδρομείου με υβριστικό περιεχόμενο σε ένα άλλο πρόσωπο. Στην περίπτωση αυτήν, τόπος τέλεσης αποτελεί τόσο ο τόπος που ενεργεί το πρώτο πρόσωπο το οποίο στέλνει το υβριστικό μήνυμα, όσο και ο τόπος στον οποίο βρίσκεται το πρόσωπο που δέχεται το μήνυμα, καθώς εκεί εκδηλώνεται το αποτέλεσμα της πράξης.

[54] Βλ. ΑΠ 586/2021, ΤΝΠ ΝΟΜΟΣ.
[55] Βλ. Δ. *Κιούπη*, Ποινικό δίκαιο και internet, 1999, σελ. 92 επ.

Διαφορετική είναι η περίπτωση όπου η χρήση της τεχνολογίας δεν χρησιμοποιείται για την επικοινωνία συγκεκριμένων προσώπων, αλλά για ακαθόριστο πλήθος ατόμων. Τέτοιες είναι οι περιπτώσεις ιστολογίων και ιστοσελίδων, όπου η συμπεριφορά του δράστη έχει το χαρακτήρα προσφοράς προς ακαθόριστο αριθμό τέτοιων ατόμων.[56]

Η νέα πραγματικότητα που διαμορφώνεται με τη χρήση ενός υπολογιστή συνδεδεμένου στον παγκόσμιο ιστό, αποτελεί εναρκτήριο έναυσμα για μία νέα διαδικασία προσδιορισμού του τόπου τέλεσης, διότι δεν είναι σαφή τα όρια εκδήλωσης συμπεριφοράς ή της επέλευσης του αποτελέσματος. Θεωρείται σχεδόν αυτονόητη η κατάληξη των πληροφοριών που αποστέλλονται μέσω του διαδικτύου στον προορισμό που έχει καθοριστεί. Στην πραγματικότητα όμως η διαδικασία αποστολής των πληροφοριών είναι εξαιρετικά σύνθετη.

Ειδικότερα, όταν αποστέλλονται πληροφορίες μέσω του διαδικτύου, το πρωτόκολλο T.C.P. (Transmission Control Protocol)[57] αρχικά τις *«σπάει»* σε πακέτα. Ο υπολογιστής στέλνει τα εν λόγω πακέτα στο τοπικό δίκτυο ή στον πάροχο υπηρεσιών διαδικτύου ή στην online συνδεδεμένη υπηρεσία. Από εκεί τα πακέτα ταξιδεύουν περνώντας από πολλαπλά επίπεδα δικτύων, υπολογιστών και τηλεπικοινωνιακών γραμμών πριν φτάσουν στον τελικό τους προορισμό, ο οποίος μπορεί να είναι στην ίδια πόλη ή σε οποιοδήποτε μέρος του κόσμου. Ένας αξιοσημείωτος αριθμός hardware προϊόντων επεξεργάζεται αυτά τα πακέτα και τα κατευθύνει προς τις σωστές κατευθύνσεις. Τα εν λόγω προϊόντα hardware έχουν σχεδιαστεί για να μεταφέρουν δεδομένα μεταξύ δικτύων και λειτουργούν ως συνδετικοί κρίκοι στο διαδίκτυο. Επομένως, τόπος τέλεσης της πράξης μπορεί να αποτελέσει κάθε τόπος από τον οποίο αποκτήθηκε πρόσβαση είτε στην ενέργεια, είτε στο αποτέλεσμα του εγκλήματος, κάθε τόπος στον οποίο αποθηκεύτηκε έστω και προσωρινά η πληροφορία, καθώς και κάθε τόπος στον οποίο διακινήθηκε η πληροφορία, έστω και ως δίαυλος.

Παράδειγμα αποτελεί η αποστολή παρανόμως ληφθέντος πορνογραφικού υλικού μέσω συνομιλίας Messenger. Στην περίπτωση αυτήν, διακρίνουμε από τη μία την αποστολή του παράνομου υλικού και από την άλλη την αποθήκευσή του στην πλατφόρμα. Αρχικά, θα πρέπει

[56] Βλ. *J. Morinigiello/W. Reynolds*, The new territorialism in the not-so-new frontier of cyberspace, Cornell Law Review, 2014, σελ. 1415 επ.

[57] Βλ. αναλυτικά *W. Buchanan*, Transmission Control Protocol (TCP) and Internet Protocol (IP), σε: *W. Buchanan*, Applied Data Communications and Networks, 1996, σελ. 87 επ.

να γίνει αξιολόγηση της παράνομης ενέργειας και να γίνει σύνδεση με κάποιον κυρωτικό κανόνα δικαίου. Έπειτα, βάσει του κυρωτικού αυτού κανόνα και του εάν τιμωρεί την κατοχή, τη διάθεση, την παραγωγή ή την αποθήκευση, θα αναζητηθεί αντίστοιχα και ο τόπος τέλεσης της πράξης. Επομένως, στην περίπτωση που ως αξιόποινη πράξη θεωρείται η διάθεση, τότε τόπος τέλεσης είναι μόνο ο τόπος του δράστη, ενώ στην περίπτωση που ως αξιόποινη πράξη θεωρείται η δημοσίευση, τότε τόπος τέλεσης είναι μόνο ο τόπος στον οποίο αποθηκεύονται τα δεδομένα.

Στην περίπτωση των ιστοσελίδων, τα δεδομένα αποθηκεύονται στους υπολογιστές των δημιουργών τους, στους διακομιστές του παρόχου πρόσβασης υπηρεσιών στο διαδίκτυο και εν γένει στον κυβερνοχώρο. Στις περιπτώσεις αυτές, ως τόπος τέλεσης δεν μπορεί να θεωρηθεί μόνο ένας τόπος, με αποτέλεσμα να είναι δύσκολη η εύρεση του δικαίου που θα εφαρμοστεί. Ως εκ τούτου, ως τόπος τέλεσης ενός διαδικτυακού εγκλήματος μπορεί να θεωρηθεί ο τόπος από τον οποίο δημοσιεύτηκαν τα δεδομένα, ο τόπος αποθήκευσης αυτών, ο τόπος του παρόχου φιλοξενίας και, φυσικά, ο τόπος λήψης των δεδομένων.[58]

Νομολογιακά[59] έχει κριθεί ότι «*στα διαδικτυακά εγκλήματα που τελούνται με την χρήση συνδέσμων παραπομπής ή με δίκτυα ομότιμων κόμβων η επίδικη συμπεριφορά του δράστη δεν εξαντλείται στον τόπο της φυσικής του παρουσίας, αλλά εκτείνεται και στον τόπο όπου αυτός μόνος ή με την αναγκαία συνεργασία και άλλων συμμετόχων του, αποθηκεύει, μεταφορτώνει, καταφορτώνει, ή άλλως επεξεργάζεται ψηφιακά δεδομένα, έστω και με προεγκατεστημένες από αυτόν σε άλλο τόπο αυτοματοποιημένες διαδικασίες, έτσι ώστε να καθιστά με τρόπο παράνομο τα δεδομένα αυτά προσιτά σε άλλους, οπότε μόνο τότε και εκεί η συμπεριφορά του αποκτά το αρνητικό κοινωνικό νόημα που αταξιολογεί ο ποινικός νομοθέτης».*

Τόσο ο Ευρωπαίος, όσο και ο Έλληνας νομοθέτης, προκειμένου να εξεύρουν μία λύση στα ανωτέρω προβλήματα, αποσύνδεσαν την εφαρμογή ορισμένων ποινικών διατάξεων από τον

[58] Βλ. *J. Goldsmith/T. Wu*, Who controls the Internet, 2006, σελ. 147 επ., αναφορικά με το ζήτημα της προσβολής ημεδαπών εννόμων αγαθών μέσω της ανάρτησης σε ιστοσελίδα δεδομένων από δράστες τρίτης χώρας, όπου η πράξη αυτή δεν τιμωρείται ποινικά.
[59] Βλ. ΕφΑθ 6613/2016, ΤΝΠ ΝΟΜΟΣ.

τόπο τέλεσης, εντάσσοντας ορισμένες κατηγορίες σοβαρών εγκλημάτων στην κατηγορία των εγκλημάτων που διώκονται με βάση την αρχή της παγκόσμιας δικαιοσύνης.[60]

Επιπλέον, μέσω της ευρωπαϊκής νομοθεσίας και των διεθνών συμβάσεων, δημιουργήθηκε ένα ενιαίο πλαίσιο για αρκετά εγκλήματα τελούμενα μέσω διαδικτύου, με συνέπεια την εξασφάλιση του διπλού αξιοποίνου, όταν η πράξη θεωρείται ότι τελέστηκε στην αλλοδαπή, διευκολύνοντας έτσι την εφαρμογή των άρθρων 6 και 7 ΠΚ. Ακόμη, σημαντικό ρόλο έπαιξε η αρχή της εδαφικότητας σε συνδυασμό με την αρχή της ενότητας, καθώς όλα τα διαδικτυακά εγκλήματα που περιέχουν αξιόποινο αποτέλεσμα (βλάβη ή κίνδυνο), το οποίο επέρχεται στην ημεδαπή, τελούνται στην ημεδαπή. Τέλος, αναφορικά με τον τόπο συμπεριφοράς του δράστη, όπως αναφέρθηκε και ανωτέρω, αυτός καλύπτει τόσο τον φυσικό χώρο, οπού ενήργησε ο δράστης, δηλαδή τον χώρο που έκανε χρήση του υπολογιστή του, όσο και τον χώρο, οπού ο δράστης ολοκλήρωσε την συμπεριφορά διά της δημοσίευσης των δεδομένων του, δηλαδή τον χώρο, όπου φιλοξενούνται τα δεδομένα από τους διακομιστές.[61]

Η λύση αυτή εμφανίζεται ως η ορθότερη, καθώς αφενός σε αρκετές ειδικές υποστάσεις εγκλημάτων τυποποιείται η έννοια της δημοσιοποίησης, με συνέπεια η ολοκλήρωση της συμπεριφοράς του δράστη να επιτυγχάνεται με την ανάρτηση των δεδομένων. Αφετέρου καθίσταται αντιληπτό ότι η συχνά διασυνοριακή φύση του διαδικτυακού εγκλήματος επιτρέπει την ύπαρξη ενός εγκλήματος, που τελείται εν μέρει στον τόπο, όπου βρίσκεται ο δράστης και εν μέρει στο χώρο, όπου βρίσκονται οι διακομιστές (servers), εξαιτίας της σύμβασης φιλοξενίας (hosting), που έχει συναφθεί μεταξύ του δράστη και του παρόχου. Ο δράστης διαθέτει προσωπικούς κωδικούς με τους οποίους ελέγχει, επενεργεί και διαθέτει στον αντίστοιχο διακομιστή που φιλοξενεί τα δεδομένα του.[62]

Στον αντίποδα της άποψης αυτής, εκφράστηκαν και άλλες απόψεις με σημαντικότερες τις ακόλουθες δύο: Σύμφωνα με την πρώτη άποψη, με αυτόν τον τρόπο χάνεται από τον τόπο συμπεριφοράς το ουσιαστικό στοιχείο της φυσικής παρουσίας του δράστη. Η άποψη αυτή δεν

---

[60] Βλ. *U. Neumann*, Η αρχή της παγκοσμιοποιημένης δικαιοσύνης σε μία παγκοσμιοποιημένη κοινότητα δικαίου, σε: *Ι. Μανδωλεδάκη/C. Prittwitz*, Διεθνοποίηση του ποινικού δικαίου, 2003, σελ. 1 επ..

[61] βλ. *Δ. Κιούπη*, Δημοσίευση ιστοσελίδων με αξιόποινο περιεχόμενο, ΠΛογ, 2001, σελ. 407.

[62] Βλ. *Δ. Κιούπη*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, σε *Θ. Δαλακούρα*, Ηλεκτρονικό έγκλημα, ουσιαστικές και δικονομικές όψεις, 2023, σελ. 50-52.

εμφανίζεται ορθή, δεδομένου ότι ο τόπος από τον οποίο ενεργεί ο δράστης δεν εγκαταλείπεται, αλλά απλώς εκτείνεται και στον τόπο όπου ο δράστης με τη χρήση λογισμικού αποθηκεύει τα ψηφιακά δεδομένα, καθιστώντας έτσι το περιεχόμενό τους προσιτό σε τρίτα πρόσωπα.

Σύμφωνα με τη δεύτερη άποψη, έχει εκφραστεί η αρκετά σημαντική αντίρρηση πως στην περίπτωση που θεωρηθεί ως τόπος συμπεριφοράς του δράστη ο τόπος αποθήκευσης των δεδομένων, ο τόπος θα εξαρτάται από τυχαίους παράγοντες με συνέπεια την υπερβολική και απρόβλεπτη επέκταση του αξιοποίνου. Ειδικότερα, ο τόπος που αποθηκεύονται τα δεδομένα εξαρτάται από τον τόπο εγκατάστασης των διακομιστών, ο οποίος διαφοροποιείται από τυχαίους παράγοντες, όπως για παράδειγμα οικονομικές συμφωνίες των παρόχων. Στην περίπτωση αυτήν, ο τόπος τέλεσης είναι αδύνατον να προβλεφθεί από τον δράστη.

Η αντίρρηση αυτή βασίζεται στο γεγονός ότι ο τόπος τέλεσης αποτελεί εξωτερικό όρο του αξιοποίνου και όχι συστατικό στοιχείο της πράξης. Ωστόσο, η άποψη αυτή δεν είναι ορθή. Στα παραδοσιακά εγκλήματα η επέλευση του αξιόποινου αποτελέσματος σε τόπο άγνωστο και απρόβλεπτο για τον δράστη καταστρατηγεί την αρχή της ενοχής. Το αποτέλεσμα της πράξης του δράστη από κάποιο τυχαίο και απρόβλεπτο γεγονός μπορεί να επέλθει σε άγνωστο γι' αυτόν τόπο, όπου η πράξη αυτή θεωρείται αξιόποινη, σε αντίθεση με τον τόπο όπου βρίσκεται ο δράστης. Έτσι, ο δράστης κινδυνεύει να βρεθεί αντιμέτωπος με μία έννομη τάξη που τον θεωρεί εγκληματία. Ορθότερο είναι ο τόπος συμπεριφοράς του δράστη να καλύπτεται από τον δόλο του. Είναι δηλαδή απαραίτητο να γνωρίζει ο δράστης και να αποδέχεται τον τόπο, στον οποίο αποθηκεύονται τα δεδομένα του, καθώς σε διαφορετική περίπτωση υφίσταται πραγματική πλάνη του. Πράγματι, μία μη προβλέψιμη για τον δράστη τοπική απόκλιση δεν μπορεί να άγει για πρώτη φορά σε θεμελίωση αξιοποίνου στη βάση συμπτωματικών λόγων, ανίκανων να στοιχειοθετήσουν ενοχή του δράστη. Ως εκ τούτου, ποινική ευθύνη του χρήστη δεν υφίσταται, όταν τα δεδομένα του αποθηκεύονται σε μία τυχαία τρίτη χώρα.[63]

[63] Σχετικά, βλ. *Χ. Μυλωνόπουλο*, Διεθνές Ποινικό Δίκαιο, Τα τοπικά όρια των ποινικών νόμων, 1993, σελ. 182 επ.

Γ.-ΕΙΔΙΚΑ ΖΗΤΗΜΑΤΑ ΣΤΟΝ ΧΩΡΟ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Γ.1.-Η συμμετοχική ευθύνη των ενδιάμεσων παρόχων διαδικτύου στο ηλεκτρονικό έγκλημα

Γ.1.α.-Ορισμοί

Η χρήση της τεχνολογίας και του διαδικτύου άνοιξε το δρόμο για τη δημιουργία νέων εγκλημάτων, η πολυπλοκότητα των οποίων πολλές φορές έγκειται όχι μόνο στην εύρεση του τόπου τέλεσης τους, αλλά και στην εύρεση των ίδιων των δραστών, καθώς τα δεδομένα ταξιδεύουν στο διαδίκτυο περνώντας από διαφορετικούς τόπους, αλλά και από διαφορετικούς ανθρώπους. Βασικό ρόλο στο *«ταξίδι»* των δεδομένων αυτών διαδραματίζει ο πάροχος του διαδικτύου, δηλαδή αυτός που παρέχει στους συνδρομητές και χρήστες του υπηρεσίες σχετικές με το διαδίκτυο. Στην Οδηγία 2000/31/ΕΚ *«για το ηλεκτρονικό εμπόριο»* (ΟΔΗΛΕ), που ενσωματώθηκε στην ελληνική έννομη τάξη με το π.δ. 131/2003, οι ενδιάμεσοι πάροχοι διαδικτύου διακρίνονται σε τρεις κατηγορίες: Στην πρώτη κατηγορία ανήκουν οι πάροχοι της

απλής μετάδοσης δεδομένων, στη δεύτερη κατηγορία οι πάροχοι αποθήκευσης σε κρυφή μνήμη και στην τρίτη κατηγορία ανήκουν οι παροχή φιλοξενίας.[64]

Ειδικότερα, οι πάροχοι *«πρόσβασης»* (access providers) έχουν το ρόλο του *«αγωγού»* μετάδοσης πληροφοριών με ή χωρίς αντίτιμο, χωρίς να ελέγχουν τις πληροφορίες που μεταβιβάζουν. Επιπλέον, δεν έχουν τη δυνατότητα πρόσβασης στις πληροφορίες αυτές, ούτε τη δυνατότητα παρέμβασης.[65] Οι πάροχοι πρόσβασης μεταφέρουν πληροφορίες προσώπων σε μορφή τηλεπικοινωνιακών σημάτων στους χρήστες των υπηρεσιών της πληροφορίας. Συνεπώς, πάροχοι *«πρόσβασης»* αποτελούν τόσο οι εταιρίες τηλεπικοινωνίας που είναι εξοπλισμένες με τα απαραίτητα μηχανήματα (διακομιστές – servers και δρομολογητές – routers)[66] και εξασφαλίζουν την πρόσβαση στο διαδίκτυο στους χρήστες τους, έναντι συνδρομής, όσο και τα καταστήματα που είναι ευρύτερα γνωστά ως *«Internet café»*, τα οποία λειτουργούν με χρονοχρέωση, αλλά και δημόσιοι οργανισμοί, όπως πανεπιστήμια και σχολεία, τα οποία παρέχουν ελεύθερη διαδικτυακή πρόσβαση στα μέλη τους. [67]

Στη δεύτερη κατηγορία συναντάμε τους παρόχους *«κρυφής μνήμης»* (cache providers), οι οποίοι έχουν το ρόλο μεσολαβητή μεταξύ των παρόχων που διατηρούν διακομιστές (servers) με πρωτότυπες πληροφορίες και των προσώπων εκεινών που κάνουν χρήση των υπηρεσιών των πρώτων. Συγκεκριμένα, όταν ο χρήστης του διαδίκτυού αιτείται μεσώ του φυλλομετρητή (browser) να παραλάβει τις παραπάνω πρωτότυπες πληροφορίες, αυτές τροφοδοτούνται από τον αρχικό διακομιστή, που τις περισσότερες φορές βρίσκεται σε κάποια απομακρυσμένη τοποθεσία, ίσως και σε κάποια άλλη ήπειρο. Με τον τρόπο αυτό, είναι φανερό ότι θα επηρεαζόταν η λειτουργιά του υπολογιστή – διακομιστή του αρχικού προέχου, αλλά και του δικτυού που τον υποστηρίζει. Η ροή των δεδομένων θα ήταν αρκετά χρονοβόρα, λόγω του τεράστιου όγκου πληροφοριών που θα έπρεπε να διακινήσει στους χρήστες του σε ούλη την

[64] Βλ. *Κ. Κακαβούλη*, Η συμμετοχική ευθύνη των ενδιάμεσων παρόχων Internet στα διαδικτυακά εγκλήματα, ΠοινΧρ 2015, σελ. 326.

[65] Βλ. *Γ. Γιαννόπουλο*, Ροή πληροφοριών στο διαδίκτυο, τεχνολογία και νομικές ρυθμίσεις, 2002, σελ. 39.

[66] Διακρίνονται από τους *«carriers»*, οι οποίοι διαθέτουν τον κατάλληλο εξοπλισμό και την υποδομή για την παροχή υπηρεσιών σχετικών με την τηλεφωνική επικοινωνία των πελατών τους. Οι υπηρεσίες τους συνιστούν υπηρεσία της τηλεπικοινωνίας και όχι της κοινωνίας της πληροφορίας, βλ. *Ε. Διαμαντή*, Ευθύνη των μεσαζόντων παροχής υπηρεσιών στο διαδικτυο κατά το ΠΔ 131/2003 - Ενσωμάτωση της Οδηγίας 2000/31 για το ηλεκτρονικό εμπόριο στο εθνικό δικαιο, Δίκαιο Επιχειρήσεων & Εταιριών 10/2004, σελ. 986 επ.

[67] Βλ. *Γ. Γιαννόπουλο,* Η ευθύνη των παρόχων υπηρεσιών στο Internet, 2013, σελ. 8 επ.

υφήλιο. Τη λύση στο ζήτημα αυτό φέρουν οι υπηρεσίες των παρόχων *«κρυφής μνήμης»*, οι οποίοι αποθηκεύουν προσωρινά αντίγραφα των πρωτοτύπων πληροφοριών σε δικούς τους διακομιστές (caching servers), που βρίσκονται διάσπαρτοι ανά τον κόσμο, εξυπηρετώντας τους αρχικούς παρόχους και στους χρήστες, μεταδίδοντας τα αντίγραφα αυτά από τον κοντινότερο στον χρήστη διακομιστή τους, με αποτέλεσμα τη γρηγορότερη διακίνηση δεδομένων.[68]

Οι πάροχοι *«φιλοξενίας»* (host providers) αποθηκεύουν πληροφορίες, οι οποίες βρίσκονται σε ιστοσελίδες τρίτων, ώστε να πραγματοποιείται η πρόσβαση σε αυτές από τους χρήστες του διαδίκτυού. Η εν λόγω διαδικτυακή υπηρεσία επιτυγχάνεται είτε με τη χορήγηση μέρους, ή και ολοκλήρου, του διακομιστή του προέχου (dedicated servers) στον κάτοχο του ισότοπου (shared hosting), είτε με την μεταπώληση χώρου και λοιπών εργαλείων διαχείρισης ιστοσελίδων από παροχή που βρίσκεται σε συμβατική σχέση με κάποιον κάτοχο διακομιστή (reseller hosting). Μεσώ της *«φιλοξενίας»*, τόσο οι εταιρίες, όσο και οι ιδιώτες, εξασφαλίζουν στους χρήστες την αδιάκοπη πρόσβαση σε ιστοσελίδες, χωρίς την ανάγκη δαπανηρού υλικοτεχνικού εξοπλισμού.[69]

Η σημασία των ενδιαμέσων παροχών είναι τεράστια, αφού, μεσώ των υπηρεσιών που προσφέρουν, εκμηδενίζουν τις τεράστιες χιλιομετρικές αποστάσεις δραστηριοποίησης του διαδίκτυού και καθιστούν προσιτά τα διακινούμενα δεδομένα σε όλους τους χρήστες του παγκοσμίως. Αυτό υλοποιείται μεσώ υπολογιστών – διακομιστών (servers) μεγάλης ισχύος, που είναι συνδεδεμένοι με τις κεντρικές αρτηρίες δεδομένων και εγκατεστημένοι ανά την υφήλιο, εξυπηρετώντας την αναζήτηση δεδομένων από προσωπικούς υπολογιστές χρηστών.

Σε αντίθεση με τους ενδιάμεσους παρόχους όπου η δραστηριότητά τους συνίσταται στη διακίνηση πληροφοριών άλλων προσώπων, υπάρχουν και οι πάροχοι *«περιεχομένου»* (content providers), για τους οποίους δεν γίνεται καμία αναφορά στις διατάξεις της ΟΔΗΛΕ και, κατ' επέκταση, του π.δ. 131/2003. Οι πάροχοι αυτοί δημιουργούν το περιεχόμενο που τίθεται σε κυκλοφορία στο διαδίκτυο μέσω αναρτήσεων είτε ιστοσελίδων στον παγκόσμιο ιστό, είτε

[68] Βλ. *G. Huston*, Web caching, The Internet Protocol Journal 2-3, 1999, ηλεκτρονικά διαθέσιμο σε: https://www.potaroo.net/papers/ipj/2-3-caching.pdf

[69] Βλ. *G. Sartor*, Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?, International Data Privacy Law 3-1, 2013, ηλεκτρονικά διαθέσιμο σε: https://academic.oup.com/idpl/article/3/1/3/643990

προσωπικών πληροφοριών σε ιστοτόπους κοινωνικής δικτύωσης (όπως Facebook, κ.λπ.), είτε μηνυμάτων στο ηλεκτρονικό ταχυδρομείο (e-mail), είτε σχολίων σε ιστολόγια (blogs).[70]

Γ.1.β.- Οι προϋποθέσεις της ΟΔΗΛΕ για την κατάφαση ευθύνης των ενδιάμεσων παρόχων

Στις διατάξεις των άρθρων 12 έως 14 της ΟΔΗΛΕ βρίσκονται οι προϋποθέσεις, υπό τις οποίες ο φορέας παροχής υπηρεσιών της κοινωνίας της πληροφορίας απαλλάσσεται από την ευθύνη.[71]

Ειδικότερα, στο άρθρο 12 της ΟΔΗΛΕ ρυθμίζεται η περίπτωση της απλής μετάδοσης. Στην εν λόγω περίπτωση, ο ενδιάμεσος πάροχος, του οποίου η δραστηριότητα έγκειται απλά στη μετάδοση πληροφοριών δεν υφίσταται ευθύνη στην περίπτωση που δεν αποτελεί την αφετηρία της μετάδοσης των πληροφοριών, στην περίπτωση που δεν επιλέγει τον αποδέκτη της μετάδοσης και στην περίπτωση που δεν επιλέγει και δεν τροποποιεί τις μεταδιδόμενες πληροφορίες. Έτσι, δεν υφίσταται ευθύνη των ενδιάμεσων παρόχων που έχουν απλώς βοηθητικό ρόλο και δεν επηρεάζουν τη δημιουργία και το περιεχόμενο της πληροφορίας. Σε

[70] Βλ. *Ι. Καράκωστα*, Δίκαιο και Internet, 2009, σελ. 102 επ.
[71] Βλ. *Γ. Γιαννόπουλο*, Η ευθύνη των παρόχων υπηρεσιών στο Internet, 2013, σελ. 117.

αντίθεση με τις άλλες δύο κατηγορίες παρόχων, δηλαδή τους παρόχους αποθήκευσης σε κρυφή μνήμη και στους παρόχους φιλοξενίας, είναι αδιάφορο αν ο πάροχος απλής μετάδοσης γνώριζε τον παράνομο χαρακτήρα των πληροφοριών που μεταδίδονται.[72]

Η απαλλαγή της ευθύνης των παρόχων κρυφής μνήμης, δηλαδή των παρόχων η δραστηριότητα των οποίων συνίσταται *«στην αυτόματη, ενδιάμεση και προσωρινή αποθήκευση των πληροφοριών η οποία γίνεται με αποκλειστικό σκοπό να καταστεί αποτελεσματικότερη η μεταγενέστερη μετάδοση των πληροφοριών, μετά από αίτηση άλλων αποδεκτών της υπηρεσίας»*, ρυθμίζεται στις διατάξεις του άρθρου 13 της ΟΔΗΛΕ. Ο πάροχος κρυφής μνήμης απαλλάσσεται της ευθύνης, όταν συντρέχουν σωρευτικά οι ακόλουθες προϋποθέσεις: Πρώτον, δεν τροποποιεί τις πληροφορίες. Δεύτερον, τηρεί τους όρους πρόσβασης στις πληροφορίες. Τρίτον, τηρεί τους κανόνες που αφορούν την ενημέρωση των πληροφοριών, οι οποίοι καθορίζονται κατά ευρέως αναγνωρισμένο τρόπο και χρησιμοποιούνται από τον κλάδο. Τέταρτον, δεν παρεμποδίζει τη νόμιμη χρήση της τεχνολογίας, η οποία αναγνωρίζεται ευρέως και χρησιμοποιείται από τον κλάδο, προκειμένου να αποκτήσει δεδομένα σχετικά με τη χρησιμοποίηση των πληροφοριών. Τέλος, ενεργεί άμεσα προκειμένου να αποσύρει τις πληροφορίες που αποθήκευσε ή να καταστήσει την πρόσβαση σε αυτές αδύνατη, μόλις αντιληφθεί ότι οι πληροφορίες έχουν αποσυρθεί από το σημείο του δικτύου, όπου βρίσκονταν αρχικά, ή η πρόσβαση στις πληροφορίες κατέστη αδύνατη, ή μια δικαστική ή διοικητική αρχή διέταξε την απόσυρση των πληροφοριών, ή απαγόρευσε την πρόσβαση σε αυτές.

Τέλος, οι προϋποθέσεις απαλλαγής της ευθύνης των παρόχων φιλοξενίας, δηλαδή των παρόχων που οι υπηρεσίες τους συνίστανται στην αποθήκευση - φιλοξενία στους διακομιστές τους πληροφοριών παρεχομένων από έναν αποδέκτη υπηρεσίας, αναφέρονται στις διατάξεις του άρθρου 14 της ΟΔΗΛΕ. Στη διάταξη αυτή, εντάσσονται κατά αναλογία δικαίου και οι σε καθημερινή βάση χρησιμοποιούμενες υπηρεσίες κοινωνικής δικτύωσης (social media). Προκειμένου να επέλθει απαλλαγή της ευθύνης του ως άνω παρόχου θα πρέπει, είτε ο φορέας παροχής της υπηρεσίας να μην γνωρίζει πραγματικά ότι πρόκειται για παράνομη δραστηριότητα ή πληροφορία και ότι, σε ό,τι αφορά αξιώσεις αποζημίωσης, να μην γνωρίζει τα γεγονότα ή τις

[72] Βλ. *Ε. Αλεξανδρίδου*, Το δικαιο του ηλεκτρονικού εμπορίου, 2010, *Ι. Ιγγλεζάκη*, Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου, 2003.

περιστάσεις από τις οποίες προκύπτει η παράνομη δραστηριότητα ή πληροφορία, είτε ο φορέας παροχής της υπηρεσίας, μόλις αντιληφθεί τα προαναφερθέντα, να αποσύρει ταχέως τις πληροφορίες ή να καθιστά την πρόσβαση σε αυτές αδύνατη. Σ

Ως προς την πρώτη προϋπόθεση, βασικό ρόλο διαδραματίζει η *«πραγματική και συγκεκριμένη γνώση»* ή *«απλή γνώση»*, όταν ασκούνται αξιώσεις αποζημίωσης.[73] Η προϋπόθεση αυτή πληρείται, όταν ο ενδιάμεσος πάροχος λάβει αποδεδειγμένα την κατάλληλη πληροφόρηση, τόσο για την ύπαρξη του περιεχομένου, όσο και για τον παράνομο χαρακτήρα αυτού, από τον προσβαλλόμενο ή από οποιονδήποτε τρίτο ή από τις αρμόδιες δικαστικές ή διοικητικές αρχές, ακόμα και από δημοσιεύματα, ή και από οποιαδήποτε άλλη πηγή πληροφόρησης.

Γ.2.-Ο ρόλος των ηλεκτρονικών αποτυπωμάτων στο ηλεκτρονικό έγκλημα

Στη σύγχρονη ψηφιακή εποχή, οι έξυπνες συσκευές όπως τα κινητά τηλέφωνα, τα έξυπνα ρολόγια κλπ., δύνανται να δώσουν πληροφορίες για την καθημερινότητά μας, όπως για παράδειγμα για τις μετακινήσεις μας και τις ζωτικές μας λειτουργίες, προσδίδοντας έτσι, ακόμη και στην εγκληματικότητα, τεχνολογικά χαρακτηριστικά. Τα ηλεκτρονικά *«αποτυπώματα»*, όπως αυτά αποκαλούνται, αφηγούνται με λεπτομέρειες τις κινήσεις μας στον κυβερνοχώρο, από τις αναζητήσεις μας μέχρι τις ηλεκτρονικές μας συνομιλίες, αποτελώντας σύγχρονα εργαλεία στα χέρια των αρχών επιβολής του νόμου, βοηθώντας στην αποτροπή και την εξιχνίαση εγκλημάτων. Η αποκωδικοποίηση, η εξέταση και η ανάλυση του περιεχομένου των ψηφιακών μέσων - πειστηρίων, είτε προέρχονται από ένα κινητό τηλέφωνο, είτε από το υπολογιστικό νέφος *«cloud»*, οδηγούν πολλές φορές στη εξιχνίαση εγκλημάτων.

[73] Βλ. *Γ. Γιαννόπουλο*, Η ευθύνη των παρόχων υπηρεσιών στο Internet, 2013, σελ. 127 επ.

Όταν πρόκειται για τέλεση κυβερνοεγκλήματος,[74] η IP διεύθυνση του επιτιθέμενου και, γενικά, τα ίχνη του στο διαδίκτυο, μπορεί να οδηγήσουν στον τόπο τέλεσης του εγκλήματος και συνεπώς στον χρήστη - δράστη.[75] Ωστόσο, δυσχέρεια στην εύρεση του τόπου τέλεσης, παρατηρείται στις περιπτώσεις που ο χρήστης - δράστης χρησιμοποιεί VPN, Proxy Server[76] ή Δίκτυο Tor.

Ένας άλλος τρόπος εύρεσης της τοποθεσίας του δράστη ενός διαδικτυακού εγκλήματος είναι η διερεύνηση του παρόχου υπηρεσιών διαδικτύου. Συγκεκριμένα, ο πάροχος υπηρεσιών διαδικτύου (Internet Service Provider - ISP) της συσκευής που χρησιμοποιήθηκε για τη διάπραξη του εγκλήματος μπορεί να χρειασθεί να παράσχει πληροφορίες σχετικά με τη θέση της συσκευής. Επιπλέον, η τοποθεσία του δράστη δύναται να εξευρεθεί και από την ανάλυση του ψηφιακού αποτυπώματος, ήτοι το ψηφιακό αποτύπωμα που άφησε πίσω του ο εγκληματίας, όπως η διαδικτυακή του δραστηριότητα και τα πρότυπα επικοινωνίας, μπορεί να αναλυθεί για τον προσδιορισμό της θέσης του. Τέλος, η χρήση δεδομένων γεωγραφικού εντοπισμού μπορεί να αποκαλύψει την τοποθεσία του δράστη, καθώς οποιαδήποτε δεδομένα γεωγραφικού εντοπισμού που σχετίζονται με το έγκλημα, όπως η θέση της συσκευής κατά τη διάπραξη του εγκλήματος, μπορούν να χρησιμοποιηθούν για τον προσδιορισμό της θέσης του δράστη.

[74] Ηλεκτρονικά διαθέσιμο σε: www.homodigitalis.gr/posts/12340#1668768932080-1b371be6-509c

[75] Βλ. *D.Y. Kao /W. Shiuh-Jeng*, The IP address and time in cyber-crime investigation, Policing: an international Journal of Police strategies & Management 32/2, 2009, σελ. 194 επ.

[76] Βλ. *G.O. Boussia/ H. Gupta/S. A. Hossain*, Financial Crime: A Conceptual Framework Implementation for Prevention of Malicious Request from a VPN or Proxy Server, Scope 13, 2023, σελ. 375 επ.

Γ.2.α.- Μέθοδοι ανώνυμης σύνδεσης στο διαδίκτυο

Τα εικονικά ιδιωτικά δίκτυα (VPN), οι διακομιστές μεσολάβησης (Proxy Servers) και ο δρομολογητής Onion (TOR) είναι τρεις ευρέως χρησιμοποιούμενες τεχνολογίες που διαδραματίζουν κρίσιμο ρόλο στη βελτίωση του απορρήτου στο διαδίκτυο, της ανωνυμίας και της ασφάλειας.[77] Παρέχουν στα άτομα τη δυνατότητα να προστατεύουν τις δραστηριότητές τους στο διαδίκτυο, να προστατεύουν ευαίσθητα δεδομένα και να παρακάμπτουν τους περιορισμούς που επιβάλλονται από κυβερνήσεις ή οργανισμούς. Ενώ τα VPN, οι διακομιστές μεσολάβησης και οι TOR μοιράζονται τον κοινό στόχο της παροχής ανωνυμίας, χρησιμοποιούν διαφορετικούς μηχανισμούς και προσφέρουν διαφορετικά επίπεδα προστασίας.

[77] Βλ. Ι. Μαυρίδη, Ασφάλεια Πληροφοριών στο Διαδίκτυο, 2015.

Ένα εικονικό ιδιωτικό δίκτυο (VPN)[78] δημιουργεί μια ασφαλή και κρυπτογραφημένη σύνδεση μεταξύ της συσκευής ενός χρήστη και του διαδικτύου. Όταν ένας χρήστης συνδέεται σε ένα VPN,[79] η διαδικτυακή του κίνηση δρομολογείται μέσω ενός απομακρυσμένου διακομιστή που βρίσκεται σε διαφορετική γεωγραφική περιοχή. Αυτός ο διακομιστής λειτουργεί ως ενδιάμεσος, προωθώντας τα αιτήματα του χρήστη και λαμβάνοντας απαντήσεις εκ μέρους του. Τα δεδομένα που μεταδίδονται μεταξύ της συσκευής του χρήστη και του διακομιστή VPN είναι κρυπτογραφημένα, παραμένοντας εμπιστευτικά και απρόσιτα σε πιθανές υποκλοπές.

Οι δυνατότητες κρυπτογράφησης και σήραγγας των VPN[80] προστατεύουν αποτελεσματικά τις διαδικτυακές δραστηριότητες από αδιάκριτα βλέμματα, όπως χάκερ, παρόχους υπηρεσιών Διαδικτύου (ISP) ή κρατικούς φορείς παρακολούθησης. Με την απόκρυψη της διεύθυνσης IP του χρήστη, τα VPN δυσκολεύουν τους ιστότοπους ή τις διαδικτυακές υπηρεσίες να παρακολουθήσουν τη φυσική τους τοποθεσία ή να αναγνωρίσουν την ταυτότητά τους. Τα VPN είναι ιδιαίτερα χρήσιμα κατά την πρόσβαση σε δημόσια δίκτυα Wi-Fi, καθώς παρέχουν ένα επιπλέον επίπεδο ασφάλειας έναντι πιθανών απειλών.[81]

Εκτός από τα οφέλη απορρήτου και ασφάλειας, τα VPN επιτρέπουν επίσης στους χρήστες να παρακάμπτουν τους γεωγραφικούς περιορισμούς.[82] Με τη σύνδεση σε διακομιστή VPN σε διαφορετική χώρα, οι χρήστες μπορούν ουσιαστικά να τον κάνουν να φαίνεται σαν να περιηγούνται στο Διαδίκτυο από αυτήν την τοποθεσία. Αυτό τους επιτρέπει να έχουν πρόσβαση σε περιεχόμενο περιορισμένης περιοχής, να ξεπεράσουν τη λογοκρισία ή να αποφύγουν τον αποκλεισμό περιεχομένου που εφαρμόζεται από οργανισμούς ή κυβερνήσεις.[83]

---

[78] Ηλεκτρονικά διαθέσιμο σε: https://diadiktiokaiasfalia.com/τι-είναι-το-vpn/

[79] Βλ. *P. Ferguson/G. Huston*, What is a VPN?, 1998, ηλεκτρονικά διαθέσιμο σε: https://courses.e-ce.uth.gr/CE370/vpn.pdf

[80] *Z. Zhang κ.ά.*, An overview of virtual private network (VPN): IP VPN and optical VPN, Photonic network communications 7, 2004, σελ. 213 επ.

[81] Βλ. *Γ. Πάγκαλο/Ι. Μαυρίδη*, Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων, 2002.

[82] Βλ. *A. Krunoslav/I. Varjačić/M. Jelenski*, Combating Cyber Crime, Academic and Applied Research in Military and Public Management Science 17/3, 2018, σελ. 19 επ.

[83] Ηλεκτρονικά διαθέσιμο σε: https://el.wizcase.com/blog/ένας-πλήρης-οδηγός-για-αρχαρίους-στα-vpn/?gclid=Cj0KCQjwzdOlBhCNARIsAPMwjbyKG4mdqwXpU19gHA1osM6c5VyPYOZLV-8rgv4GaLg9PHDM6VF2nPwaAvPkEALw_wcB

Οι διακομιστές μεσολάβησης (γνωστοί ως Proxy Servers), από την άλλη πλευρά, λειτουργούν ως μεσάζοντες μεταξύ της συσκευής ενός χρήστη και του Διαδικτύου.[84] Όταν ένας χρήστης στέλνει ένα αίτημα για πρόσβαση σε έναν ιστότοπο ή έναν πόρο, πρώτα πηγαίνει στον διακομιστή μεσολάβησης. Στη συνέχεια, ο διακομιστής μεσολάβησης προωθεί το αίτημα στον ιστότοπο προορισμού, ανακτά την απάντηση και την στέλνει πίσω στη συσκευή του χρήστη. Αυτή η διαδικασία καλύπτει αποτελεσματικά τη διεύθυνση IP του χρήστη και προστατεύει την ταυτότητά του από τον ιστότοπο ή την ηλεκτρονική υπηρεσία.

Οι διακομιστές μεσολάβησης προσφέρουν διάφορα πλεονεκτήματα, όπως η ανωνυμία και οι δυνατότητες αποθήκευσης στην κρυφή μνήμη. Χρησιμοποιώντας έναν διακομιστή μεσολάβησης, οι χρήστες μπορούν να αποκρύψουν τη διεύθυνση IP τους και να την κάνουν να φαίνεται σαν τα αιτήματά τους να προέρχονται από τον ίδιο τον διακομιστή. Αυτό παρέχει ένα επιπλέον επίπεδο ανωνυμίας και προστατεύει την πραγματική ταυτότητα και τοποθεσία του χρήστη. Επιπρόσθετα, οι διακομιστές μεσολάβησης μπορούν να αποθηκεύσουν προσωρινά περιεχόμενο ιστού, αποθηκεύοντας αντίγραφα ιστοσελίδων και πόρων τοπικά. Η λειτουργία αυτή επιτρέπει σε επόμενα αιτήματα για το ίδιο περιεχόμενο να προβάλλονται απευθείας από τη μνήμη *«cache»* του διακομιστή μεσολάβησης, μειώνοντας με αυτόν τον τρόπο τη χρήση εύρους ζώνης και βελτιώνοντας τη συνολική απόδοση περιήγησης.

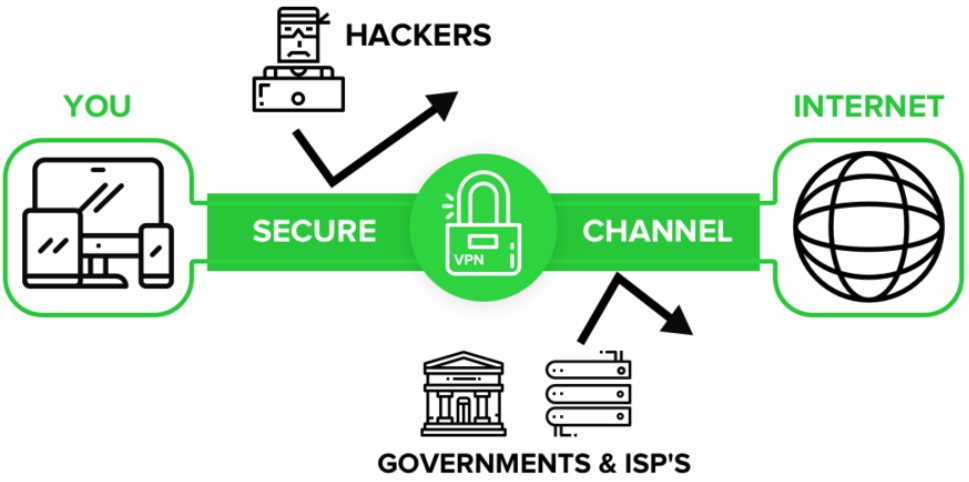
Υπάρχουν διάφοροι τύποι διακομιστών μεσολάβησης, που καλύπτουν συγκεκριμένες ανάγκες και απαιτήσεις. Οι διακομιστής μεσολάβησης HTTP χρησιμοποιούνται συνήθως για περιήγηση στον ιστό, ενώ οι διακομιστές μεσολάβησης HTTPS προσφέρουν κρυπτογραφημένες συνδέσεις για βελτιωμένη ασφάλεια. Οι διακομιστές μεσολάβησης SOCKS λειτουργούν σε χαμηλότερο επίπεδο της στοίβας δικτύου και μπορούν να χειριστούν διάφορους τύπους κίνησης.[85] Διαφανείς διακομιστές μεσολάβησης χρησιμοποιούνται από οργανισμούς ή παρόχους

[84] Βλ. *A. Luotonen*, Web proxy servers, 1998.

[85] Βλ. *N. Ianelli/A. Hackworth*, Botnets as a vehicle for online crime, CERT Coordination Center 1/1, 2005, ηλεκτρονικά διαθέσιμο σε: https://insights.sei.cmu.edu/documents/273/2005_019_001_51249.pdf

υπηρεσιών Διαδικτύου για την παρακολούθηση της κυκλοφορίας των χρηστών. Κάθε τύπος διακομιστή μεσολάβησης λειτουργεί διαφορετικά και παρέχει ξεχωριστές δυνατότητες.

Το Onion Router (TOR) είναι ένα αποκεντρωμένο δίκτυο διακομιστών που λειτουργούν με την βοήθεια εθελοντών σχεδιασμένο να διευκολύνει την ανώνυμη περιήγηση στο Διαδίκτυο.[86] Όταν χρησιμοποιείται το TOR, η κίνηση στο Διαδίκτυο ενός χρήστη δρομολογείται μέσω μιας



σειράς κόμβων TOR ή ηλεκτρονόμων. Κάθε ρελέ στην αλυσίδα γνωρίζει μόνο τη διεύθυνση IP του προηγούμενου και του επόμενου ρελέ, δημιουργώντας πολλαπλά επίπεδα κρυπτογράφησης, που μοιάζουν με τα στρώματα ενός *«κρεμμυδιού»* (onion). Αυτή η διαδικασία δρομολόγησης και κρυπτογράφησης πολλαπλών βημάτων αυξάνει σημαντικά τη δυσκολία εντοπισμού της προέλευσης ενός αιτήματος και αναγνώρισης του χρήστη.[87]

Με την κρυπτογράφηση και την ανακατεύθυνση της κυκλοφορίας στο Διαδίκτυο μέσω μιας σειράς αναμετάδοσης, το TOR προσφέρει ισχυρή ανωνυμία.[88] Οι ιστότοποι και οι υποκλοπές δικτύων θεωρούν εξαιρετικά δύσκολο να προσδιορίσουν την πραγματική προέλευση των αιτημάτων που υποβάλλονται μέσω του TOR. Το TOR υποστηρίζει επίσης *«κρυφές*

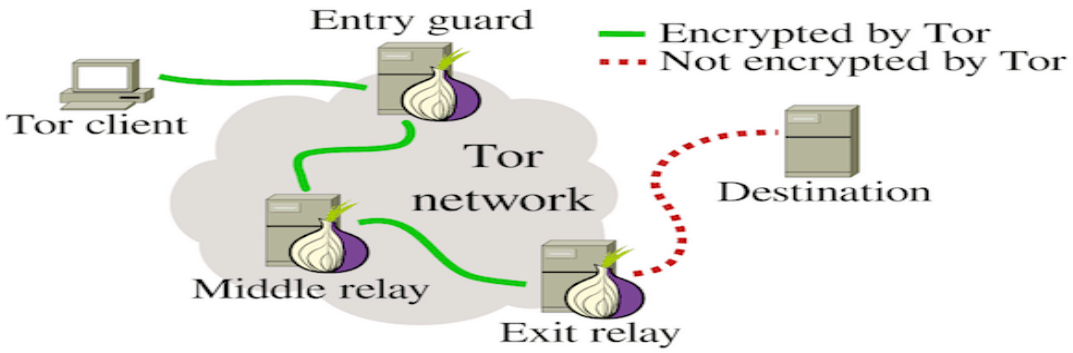
[86] Βλ. *R. Dingledine/N. Mathewson/P.F. Syverson*, Tor: The second-generation onion router, USENIX security symposium 4, 2004, ηλεκτρονικά διαθέσιμο σε: https://www.usenix.org/legacy/publications/library/proceedings/sec04/tech/full_papers/dingledine/dingledine.pdf

[87] Βλ. *A.T. Zulkamine κ.ά.* Surfacing collaborated networks in dark web to find illicit and criminal content, 2016 IEEE Conference on Intelligence and Security Informatics (ISI), 2016, σελ. 109 επ.

[88] Βλ. *R. Snader/N. Borisov,* A Tune-up for Tor: Improving Security and Performance in the Tor Network, 15th Network and Distributed System Security Symposium (NDSS) 8, 2008, ηλεκτρονικά διαθέσιμο σε: https://www.freehaven.net/anonbib/cache/snader08.pdf

υπηρεσίες»,[89] οι οποίες είναι ιστότοποι όπου είναι δυνατή η πρόσβαση μόνο μέσω του δικτύου TOR. Αυτές οι κρυφές υπηρεσίες έχουν τους δικούς τους τομείς *«onion»* και παρέχουν ένα επιπλέον επίπεδο απορρήτου τόσο για τους χειριστές του ιστότοπου όσο και για τους χρήστες.

Ωστόσο, είναι σημαντικό να σημειωθεί ότι η χρήση του TOR μπορεί να έχει ως αποτέλεσμα χαμηλότερες ταχύτητες περιήγησης λόγω της δρομολόγησης πολλαπλών βημάτων και της κρυπτογράφησης. Επιπλέον, ορισμένοι ιστότοποι ενδέχεται να αποκλείσουν ή να περιορίσουν την πρόσβαση από τους κόμβους εξόδου TOR, καθώς ανησυχούν για κατάχρηση ή κακόβουλες δραστηριότητες που προέρχονται από το δίκτυο TOR.



Συμπερασματικά, τα εικονικά ιδιωτικά δίκτυα (VPN), οι διακομιστές μεσολάβησης και ο δρομολογητής Onion (TOR) είναι ανεκτίμητα εργαλεία για άτομα που αναζητούν βελτιωμένο απόρρητο, ανωνυμία και ασφάλεια κατά την περιήγησή τους στο Διαδίκτυο. Τα VPN δημιουργούν ασφαλή σύνδεση κρυπτογραφημένων δεδομένων και δρομολόγηση τους μέσω απομακρυσμένων διακομιστών, ενώ οι διακομιστές μεσολάβησης λειτουργούν ως μεσάζοντες

[89] Βλ. *E. Jardine*, The Dark Web dilemma: Tor, anonymity and online policing, Global Commission on Internet Governance Paper Series 21, 2015, ηλεκτρονικά διαθέσιμο σε: https://www.cigionline.org/sites/default/files/no.21.pdf

μεταξύ των χρηστών και του Διαδικτύου. Η TOR χρησιμοποιεί ένα αποκεντρωμένο δίκτυο ηλεκτρονόμων για να παρέχει ισχυρή ανωνυμία. Κάθε τεχνολογία έχει τα δικά της δυνατά σημεία και περιπτώσεις χρήσης, ανάλογα με το επίπεδο απορρήτου, ασφάλειας και λειτουργικότητας που επιθυμεί ο χρήστης. Αξιοποιώντας αυτές τις τεχνολογίες, τα άτομα μπορούν να ανακτήσουν τον έλεγχο των διαδικτυακών τους δραστηριοτήτων, να προστατεύσουν τα δεδομένα τους και να περιηγηθούν στο Διαδίκτυο με αυξημένη ελευθερία.

Ωστόσο, από τα εργαλεία αυτά ασφαλούς σύνδεσης στο διαδίκτυο μπορούν να επωφεληθούν και οι δράστες των κυβερνοεγκλημάτων. Στην ελληνική έννομη τάξη, οι αρχές επιβολής του νόμου έχουν πρόσβαση σε διάφορα εργαλεία και πόρους που μπορούν να χρησιμοποιηθούν για τον εντοπισμό του εγκληματία και τον προσδιορισμό της θέσης του. Ανάμεσα σε αυτά τα εργαλεία είναι και το μέτρο της άρσης του απορρήτου των επικοινωνιών, το οποίο ρυθμίζεται από τις διατάξεις του Ν. 5002/2022, με τον οποίον καταργήθηκαν τα άρθρα 3 έως και 5 του προγενέστερου ν. 2225/1994.[90] Ο ν. 5002/2022 ορίζει τη διαδικασία άρσης του απορρήτου για την διακρίβωση τέλεσης σοβαρών αδικημάτων,[91] περιγράφει το περιεχόμενο που απαιτείται να έχει το βούλευμα ή η διάταξη για την επιβολή ή απόρριψη του μέτρου[92] και θεσπίζει τη διαδικασία γνωστοποίησης της επιβολής του μέτρου στο θιγόμενο πρόσωπο.[93]

Ταυτόχρονα, ορίζεται η διαδικασία και ο τρόπος διαχείρισης από τις αρμόδιες αρχές των κατασχεμένων ή συλλεχθέντων στοιχείων και του υλικού που συγκέντρωσαν ή αποτύπωσαν οι αρχές, στη βάση του περιεχομένου του βουλεύματος ή της διάταξης, με την οποία επιβάλλεται το μέτρο της άρσης για τη διακρίβωση τέλεσης ενός ή περισσότερων εγκλημάτων.[94] Στα αξιομνημόνευτα του νέου νόμου είναι πως πλέον ορίζεται ρητά στα άρθ. 6(4)(ζ') ότι αντικείμενο του μέτρου αποτελούν, και τα λεγόμενα *«εξωτερικά στοιχεία της επικοινωνίας»*, δηλαδή τα δεδομένα κίνησης, τα δεδομένα θέσης και τα μεταδεδομένα.[95]

[90] Βλ. Ν. 5002/2022, άρθ. 50[1].
[91] Βλ. Ν. 5002/2022, άρθ. 6[3].
[92] Βλ. Ν. 5002/2022, άρθ. 6[4]-[5].
[93] Βλ. Ν. 5002/2022, άρθ. 6[8].
[94] Βλ. Ν. 5002/2022, άρθ. 7, καθώς και Αιτιολογική Έκθεση Ν. 5002/2022, σελ. 48.
[95] Βλ. επίσης Ν. 5002/2022, άρθ. 4(4)(δ).

Ωστόσο, παρά τις ορισμένες βελτιώσεις που έχει επιφέρει ο νομοθέτης κατά τη θέσπιση των τελικών διατάξεων του ν. 5002/2022, εντούτοις ο τελευταίος έχει δεχθεί κριτική διότι δεν έχει λάβει αρκούντως υπόψη τις ραγδαίες τεχνολογικές και ευρωπαϊκές νομοθετικές εξελίξεις, με συνέπεια η γενική εικόνα που παρουσιάζει ο νέος νόμος να μην αντικατοπτρίζει το εξαγγελμένο σύγχρονο νομοθετικό πλαίσιο, που θα αντικαθιστούσε το παλαιότερο. Το παρόν νομικό πλαίσιο που διέπει την άρση του απορρήτου των επικοινωνιών τοποθετείται σε όμοιο σημείο με το προηγούμενο νομοθετικό καθεστώς.[96]

Γ. 2.β.-Ψηφιακά αποτυπώματα

Στον τομέα του εγκλήματος στον κυβερνοχώρο, τα ψηφιακά ίχνη χρησιμεύουν ως ανεκτίμητες ενδείξεις για τους ερευνητές που προσπαθούν να εντοπίσουν και να συλλάβουν τα άτομα που είναι υπεύθυνα για παράνομες δραστηριότητες. Αυτά τα ψηφιακά αποτυπώματα, που αποτελούνται από διευθύνσεις IP, διευθύνσεις MAC, δεδομένα γεωγραφικής τοποθεσίας και

[96] Βλ. *Ε. Συμεωνίδου – Καστανίδου*, Νέοι Νόμοι - Ο νόμος 5002/2022 σχετικά με την άρση του απορρήτου των επικοινωνιών (ΦΕΚ Α΄ 228/9-12-2022): κρίσιμες για τις θεμελιώδεις ελευθερίες «αστοχίες», ΠοινΔικ, 2023, σελ. 108 επ., *Γ. Τσόλια*, Το νομικό πλαίσιο άρσης του απορρήτου των ηλεκτρονικών επικοινωνιών για τη διακρίβωση εγκλημάτων σύμφωνα με τις διατάξεις του Ν 5002/2022και η απολεσθείσα ευκαιρία εκσυγχρονισμού του, ΠοινΔικ, 2023, σελ. 242 επ.

πληροφορίες που παρέχονται από Παρόχους Υπηρεσιών Διαδικτύου (ISP), προσφέρουν κρίσιμες πληροφορίες που βοηθούν τις υπηρεσίες επιβολής του νόμου να ξεδιαλύνουν τον περίπλοκο ιστό των κυβερνοεγκληματικών επιχειρήσεων. Αναλύοντας σχολαστικά και συσχετίζοντας αυτά τα ψηφιακά ίχνη, οι ερευνητές μπορούν να δημιουργήσουν μια περιεκτική διαδρομή που οδηγεί στους δράστες, διευκολύνοντας τελικά την επιδίωξη της δικαιοσύνης και προστατεύοντας την ψηφιακή σφαίρα από κακόβουλες δραστηριότητες.

Οι διευθύνσεις IP διαδραματίζουν κεντρικό ρόλο στις έρευνες για το έγκλημα στον κυβερνοχώρο. Μια διεύθυνση IP (Πρωτόκολλο Διαδικτύου) είναι ένα μοναδικό αριθμητικό αναγνωριστικό που εκχωρείται σε κάθε συσκευή που είναι συνδεδεμένη σε ένα δίκτυο, επιτρέποντας την απρόσκοπτη επικοινωνία μεταξύ συσκευών σε όλη την τεράστια έκταση του Διαδικτύου. Κατά την καταδίωξη των εγκληματιών του κυβερνοχώρου, οι διευθύνσεις IP χρησιμεύουν ως θεμελιώδες εργαλείο για τον εντοπισμό και την παρακολούθηση υπόπτων. Κάθε φορά που ένας εγκληματίας του κυβερνοχώρου εμπλέκεται σε παράνομες δραστηριότητες, η διεύθυνση IP του συχνά καταγράφεται σε αρχεία καταγραφής ή καταγράφεται από διάφορα συστήματα και υπηρεσίες με τις οποίες αλληλεπιδρούν. Αυτό το ψηφιακό αποτύπωμα λειτουργεί ως ψηφιακός δείκτης, επιτρέποντας στις υπηρεσίες επιβολής του νόμου να συνδέσουν συγκεκριμένες δραστηριότητες σε μια συγκεκριμένη διεύθυνση IP και ενδεχομένως να αποκαλύψουν την ταυτότητα του δράστη.

Επιπλέον, οι διευθύνσεις IP προσφέρουν πολύτιμες πληροφορίες για τη γενική γεωγραφική θέση ενός υπόπτου. Χρησιμοποιώντας βάσεις δεδομένων γεωγραφικής τοποθεσίας, ή συνεργαζόμενοι με παρόχους υπηρεσιών διαδικτύου, οι ερευνητές μπορούν να προσεγγίσουν τη φυσική τοποθεσία του υπόπτου. Αυτές οι πληροφορίες καθίστανται κρίσιμες για τον περιορισμό της περιοχής αναζήτησης και την εστίαση των ερευνητικών προσπαθειών σε συγκεκριμένες περιοχές ή δικαιοδοσίες. Επιπλέον, η συνεργασία με τους ISP επιτρέπει στις υπηρεσίες επιβολής του νόμου να εντοπίσουν μια διεύθυνση IP σε έναν συγκεκριμένο συνδρομητή και να αποκτήσουν πρόσθετες λεπτομέρειες, όπως αρχεία συνδρομητών, πληροφορίες χρέωσης ή αρχεία καταγραφής συνδρομητών. Αυτές οι συλλογικές προσπάθειες παρέχουν στις αρχές επιβολής του νόμου ζωτικής σημασίας στοιχεία που διευκολύνουν τον εντοπισμό και τη σύλληψη των εγκληματιών του κυβερνοχώρου.

Ωστόσο, είναι σημαντικό να αναγνωρίσουμε ότι οι διευθύνσεις IP δεν είναι αλάνθαστα αναγνωριστικά στη σφαίρα του εγκλήματος στον κυβερνοχώρο. Καθώς η τεχνολογία προχωρά, οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν διάφορες τεχνικές για να συσκοτίσουν την ταυτότητά τους και να αποφύγουν τον εντοπισμό. Για παράδειγμα, μπορούν να χρησιμοποιούν διακομιστές μεσολάβησης ή εικονικά ιδιωτικά δίκτυα (VPN)[97] για να κρύψουν τις διευθύνσεις IP τους, ανωνυμοποιώντας αποτελεσματικά τις διαδικτυακές τους δραστηριότητες. Αυτά τα μέτρα ενίσχυσης της ιδιωτικής ζωής μπορούν να περιπλέξουν σημαντικά τις έρευνες, καθιστώντας κατ' επέκταση αναγκαία την ανάπτυξη εξελιγμένων τεχνικών εγκληματολογίας και τη συνεργασία με τους παρόχους υπηρεσιών διαδικτύου για την αντιμετώπιση αυτών των προκλήσεων.

Εκτός από τις διευθύνσεις IP, οι διευθύνσεις MAC (Media Access Control) χρησιμεύουν ως μοναδικά αναγνωριστικά που εκχωρούνται στις διεπαφές δικτύου των συσκευών.[98] Σε αντίθεση με τις διευθύνσεις IP, οι οποίες εκχωρούνται από το δίκτυο ή τον ISP, οι διευθύνσεις MAC εκχωρούνται από τους κατασκευαστές συσκευών και προορίζονται να είναι μοναδικές παγκοσμίως. Παρόλο που οι διευθύνσεις MAC διαδραματίζουν μικρότερο ρόλο στις έρευνες εγκλήματος στον κυβερνοχώρο σε σύγκριση με τις διευθύνσεις IP, μπορεί να είναι πολύτιμες στην εγκληματολογία τοπικών δικτύων ή στον εντοπισμό συσκευών σε μια συγκεκριμένη περιοχή. Ωστόσο, οι διευθύνσεις MAC χρησιμοποιούνται κυρίως για σκοπούς διαχείρισης δικτύου και δεν είναι εύκολα ανιχνεύσιμες ή δημόσια ορατές εκτός τοπικών δικτύων.[99]

Τα δεδομένα γεωεντοπισμού αναδεικνύονται ως ένα άλλο κρίσιμο ψηφιακό ίχνος στις έρευνες για το έγκλημα στον κυβερνοχώρο. Τα δεδομένα γεωεντοπισμού περιλαμβάνουν πληροφορίες που καθορίζουν τη φυσική τοποθεσία μιας συσκευής ή ενός ατόμου, οι οποίες μπορούν να προέρχονται από διάφορες πηγές, όπως συντεταγμένες GPS,[100] σήματα Wi-Fi, τριγωνοποίηση πύργων κυψέλης ή βάσεις δεδομένων γεωεντοπισμού IP. Στο πλαίσιο του εγκλήματος στον κυβερνοχώρο, τα δεδομένα γεωεντοπισμού βοηθούν τις αρχές επιβολής του νόμου να εντοπίσουν την κατά προσέγγιση τοποθεσία από την οποία δραστηριοποιείται ένας ύποπτος. Χαρτογραφώντας διευθύνσεις IP σε φυσικές τοποθεσίες μέσω δεδομένων γεωγραφικής

[97] Βλ. S. *Kaur/S. Randhawa,* Dark web: A web of crimes, Wireless Personal Communications 112, 2020, σελ. 2131 επ.
[98] Βλ. *S. Burnett/S. Paine*, RSA Security's Official Guide to Cryptography, 2001.
[99] Βλ. *B. A. Forouzan*, Introduction to cryptography and network security, 2008.
[100] Βλ. *P. Kedia*, Crime mapping and analysis using GIS, International Institute of Information Technology 1-1, 2016, σελ. 1 επ.

τοποθεσίας, οι ερευνητές μπορούν να βελτιώσουν την αναζήτησή τους και να δημιουργήσουν ένα πιο ακριβές χρονοδιάγραμμα των δραστηριοτήτων του υπόπτου.

Επιπλέον, τα δεδομένα γεωγραφικού εντοπισμού μπορούν να διασταυρωθούν με άλλα ψηφιακά ίχνη,[101] όπως χρονικές σημάνσεις, για να καθοριστούν συσχετισμοί και μοτίβα στη συμπεριφορά του υπόπτου. Κατανοώντας πότε και πού συμβαίνουν ορισμένες δραστηριότητες, οι αρχές μπορούν να αποκαλύψουν κρίσιμες πληροφορίες που μπορεί να βοηθήσουν στον εντοπισμό υπόπτων ή στην ανασυγκρότηση του τρόπου λειτουργίας ενός εγκληματία στον κυβερνοχώρο. Ωστόσο, τα δεδομένα γεωγραφικής θέσης δεν είναι χωρίς περιορισμούς. Παράγοντες όπως η μεταβλητότητα του σήματος, οι τεχνικές ανακρίβειες ή ο σκόπιμος χειρισμός μπορεί να επηρεάσουν την ακρίβεια και την αξιοπιστία των πληροφοριών γεωγραφικής θέσης, απαιτώντας προσοχή και περαιτέρω διερεύνηση.

Τα δεδομένα που παρέχονται από τους ISP αναδεικνύονται ως βασικός πόρος για την καταδίωξη των εγκληματιών του κυβερνοχώρου. Οι ISP, διαθέτουν πλήθος δεδομένων που σχετίζονται με τις δραστηριότητες των χρηστών και τις λεπτομέρειες σύνδεσης. Αυτά τα δεδομένα περιλαμβάνουν πληροφορίες συνδρομητών, εκχωρήσεις διευθύνσεων IP, χρονικές σημάνσεις περιόδων σύνδεσης και αρχεία επικοινωνίας μεταξύ της συσκευής του χρήστη και του δικτύου του ISP.[102] Η συνεργασία με τους ISP επιτρέπει στις υπηρεσίες επιβολής του νόμου να ζητούν και να λαμβάνουν δεδομένα που σχετίζονται με συγκεκριμένες διευθύνσεις IP ή λογαριασμούς συνδρομητών, ρίχνοντας έτσι φως στις διαδικτυακές δραστηριότητες του υπόπτου.

Η διαθεσιμότητα και η διατήρηση δεδομένων από τους παρόχους υπηρεσιών Διαδικτύου μπορεί να διαφέρει ανάλογα με τη δικαιοδοσία και το νομικό πλαίσιο.[103] Ορισμένες δικαιοδοσίες μπορεί να έχουν νόμους διατήρησης δεδομένων που υποχρεώνουν τους παρόχους υπηρεσιών διαδικτύου να αποθηκεύουν δεδομένα χρήστη για μια συγκεκριμένη περίοδο, ενώ άλλες μπορεί να μην έχουν τέτοιους κανονισμούς. Επιπλέον, η έκταση των δεδομένων που διατηρούνται από τους ISP μπορεί να διαφέρει, ανάλογα με τις εσωτερικές

[101] Βλ. *O. Hutt, κ.ά.,* Data and evidence challenges facing place-based policing, Policing: An International Journal 41/3, 2018, σελ. 339 επ.
[102] Βλ. *D. Dorr/S. Janich*, The Criminal Responsibility of Internet Service Providers in Germany, Mississippi Law Journal 80, 2010, σελ. 1247 επ.
[103] Βλ. *J. Petersilia/S. Turner*, Intensive probation and parole, Crime and justice 17, 1993, σελ. 281 επ.

πολιτικές και τις δυνατότητες υποδομής τους. Η πλοήγηση στις νομικές απαιτήσεις και η διασφάλιση αποτελεσματικής συνεργασίας με τους παρόχους υπηρεσιών διαδικτύου είναι κρίσιμες πτυχές των ερευνών για τα εγκλήματα στον κυβερνοχώρο,[104] καθώς η έγκαιρη πρόσβαση σε σχετικά δεδομένα μπορεί να επηρεάσει σημαντικά την επιτυχία μιας έρευνας.

Συμπερασματικά, τα ψηφιακά ίχνη, συμπεριλαμβανομένων των διευθύνσεων IP, των διευθύνσεων MAC, των δεδομένων γεωγραφικής θέσης και των πληροφοριών που παρέχονται από τους ISP, αποτελούν το θεμέλιο των ερευνών για το έγκλημα στον κυβερνοχώρο. Αυτά τα ψηφιακά αποτυπώματα προσφέρουν πολύτιμες πληροφορίες που βοηθούν τους ερευνητές να εντοπίσουν υπόπτους, να παρακολουθήσουν τις δραστηριότητές τους και να δημιουργήσουν διασυνδέσεις με εγκληματικές πράξεις. Ενώ οι διευθύνσεις IP παρέχουν βασικά αναγνωριστικά και γεωγραφικές πληροφορίες, οι διευθύνσεις MAC και τα δεδομένα γεωγραφικής τοποθεσίας προσφέρουν πρόσθετες λεπτομέρειες σχετικά με τα συμφραζόμενα. Η συνεργασία με τους ISP επιτρέπει την πρόσβαση σε κρίσιμα δεδομένα χρηστών, ενισχύοντας περαιτέρω τη διαδικασία έρευνας. Ωστόσο, η δυναμική φύση της τεχνολογίας και το εξελισσόμενο τοπίο του εγκλήματος στον κυβερνοχώρο θέτουν συνεχείς προκλήσεις, απαιτώντας από τις αρχές επιβολής να παραμείνουν σε επαγρύπνηση, να προσαρμοστούν στα αναδυόμενα μέτρα ενίσχυσης της ιδιωτικής ζωής και να αξιοποιήσουν την ιατροδικαστική εμπειρογνωμοσύνη για να χρησιμοποιήσουν αποτελεσματικά τα ψηφιακά ίχνη στην καταδίωξη των κυβερνοεγκλημάτων.

Γ.3.-Ηλεκτρονικά αποδεικτικά στοιχεία (E-Evidence)

Γ.3.α.-Η αξία των ηλεκτρονικών αποδεικτικών στοιχείων στις ποινικές διαδικασίες

Το δικαίωμα στην απόδειξη έχει την έννοια ότι ακόμη και αμφισβητούμενα αποδεικτικά μέσα δεν μπορούν να αποκλειστούν και δεν πρέπει να υπάρχουν περιορισμοί όσον αφορά το αποδεικτικό υλικό. Προς αυτή την κατεύθυνση, αν και η αποδοχή τους είναι ενίοτε

[104] Βλ. *S. Turner/J. Petersilia/E.P. Deschenes*, Evaluating intensive supervision probation/parole (ISP) for drug offenders, Crime & Delinquency 38/4, 1992, σελ. 539 επ.

αμφιλεγόμενη, τα ηλεκτρονικά αποδεικτικά στοιχεία, είναι ο πιο αποτελεσματικός τρόπος ταυτοποίησης των ψηφιακών αποτυπωμάτων του εγκλήματος στον κυβερνοχώρο.[105]

Η θέσπιση νομοθετικών μέτρων που επιτρέπουν την ηλεκτρονική απόδειξη διευκολύνει τον εντοπισμό, τη διερεύνηση και τη δίωξη των εγκλημάτων στον κυβερνοχώρο.[106] Οι τύποι των αποδεικτικών στοιχείων που μπορούν να χρειαστούν σε έννομες διαδικασίες διακρίνονται σε τρεις κατηγορίες: Η πρώτη κατηγορία αφορά αποδεικτικά στοιχεία από δημόσια διαθέσιμες ιστοσελίδες, όπως αναρτήσεις σε ιστολόγια και εικόνες που αναρτώνται σε ιστοσελίδες κοινωνικής δικτύωσης. Η δεύτερη κατηγορία αφορά τις ουσιαστικές αποδείξεις, δηλαδή το ηλεκτρονικό ταχυδρομείο ή τα έγγραφα σε ψηφιακή μορφή που δεν διατίθενται στο κοινό και τα οποία φυλάσσονται σε διακομιστή. Η τρίτη και τελευταία κατηγορία αφορά την υποτιθέμενη ταυτότητα του χρήστη και τα δεδομένα κίνησης (μεταδεδομένα), που χρησιμοποιούνται για να βοηθήσουν στην ταυτοποίηση ενός ατόμου στην εξεύρεση της πηγής της επικοινωνίας, αλλά όχι του περιεχομένου.[107] Τα ηλεκτρονικά αποδεικτικά στοιχεία, που αναφέρονται επίσης ως ψηφιακά αποδεικτικά στοιχεία, μπορεί να έχουν τη μορφή κειμένου, βίντεο, φωτογραφιών ή ήχων. Στην υπόθεση *Eparhos Lemesou*,[108] το Ποινικό Εφετείο της Κύπρου εξέτασε το παραδεκτό αποδείξεων που καταγράφηκαν με μηχανικά μέσα. Το Δικαστήριο αποφάσισε ότι ήταν ορθό να εισαχθεί στη δίκη η μαγνητοφώνηση ως παραδεκτό αποδεικτικό στοιχείο, διότι δεν υπάρχει καμία διαφορά μεταξύ μιας φωτογραφίας και μιας μαγνητοφώνησης.

Τα δεδομένα μπορεί να προέρχονται από φορείς ή μεθόδους πρόσβασης, όπως κινητά τηλέφωνα, ιστοσελίδες, υπολογιστές ή συσκευές καταγραφής γεωεντοπισμού, συμπεριλαμβανομένων των δεδομένων που είναι αποθηκευμένα σε αποθηκευτικό χώρο εκτός του ελέγχου του ίδιου του ατόμου. Το ηλεκτρονικό μήνυμα (ηλεκτρονικό ταχυδρομείο) αποτελεί τυπικό παράδειγμα ηλεκτρονικού αποδεικτικού στοιχείου, καθώς πρόκειται για αποδεικτικό στοιχείο που προέρχεται από ηλεκτρονική συσκευή (υπολογιστή ή συσκευή που μοιάζει με

---

[105] Βλ. *C. Michailidou*, Cybercrime and electronic evidence – a way of identifying its digital prints. Europe at a glance, 2018, ηλεκτρονικά διαθέσιμο σε: https://theartofcrime.gr/cybercrime-and-electronic-evidence-a-way-of-identifying-its-digital-prints-europe-at-a-glance/#_ftnref3

[106] Βλ. *S. Mason*, International Electronic Evidence, 2008, Introduction, σελ. Xxxv.

[107] Βλ. *S. Mason*, Council of Europe, European Committee on legal co-operation (CDCJ), The use of electronic evidence in civil and administrative law proceedings and its effect on the rules of evidence and modes of proof, A comparative study and analysis, CDCJ (2015) 14 final, 2016.

[108] Βλ. *Eparhos Lemesou v Giorgalla* [2003] 2 CLR 298.

υπολογιστή) και περιλαμβάνει μεταδεδομένα. Τα μεταδεδομένα είναι δεδομένα που αφορούν άλλα δεδομένα και μπορούν να χαρακτηριστούν ως το ψηφιακό αποτύπωμα των ηλεκτρονικών αποδεικτικών στοιχείων. Μπορούν να περιλαμβάνουν αποδεικτικά δεδομένα, όπως την ημερομηνία και την ώρα δημιουργίας ή τροποποίησης ενός αρχείου ή εγγράφου ή τον συντάκτη τέτοιων αρχείων και την ημερομηνία και την ώρα αποστολής των δεδομένων. Τα ηλεκτρονικά αποδεικτικά στοιχεία δεν θα πρέπει να υφίστανται διακρίσεις ούτε προνόμια έναντι άλλων τύπων αποδεικτικών στοιχείων και τα δικαστήρια θα πρέπει να υιοθετούν μια τεχνολογικά ουδέτερη προσέγγιση, δηλαδή θα πρέπει να λαμβάνονται υπόψη ως μια τεχνολογία που επιτρέπει τη γνησιότητα, την ακρίβεια και την ακεραιότητα των δεδομένων.[109]

Η μεταχείριση των ηλεκτρονικών αποδεικτικών στοιχείων δεν θα πρέπει να είναι μειονεκτική για τους διαδίκους σε μία ποινική διαδικασία, όπως όταν ο διάδικος στερείται της δυνατότητας να αμφισβητήσει τη γνησιότητα των αποδεικτικών στοιχείων, ή όταν το δικαστήριο ζητά από τον διάδικο να υποβάλει εκτυπώσεις ηλεκτρονικών αποδεικτικών στοιχείων, από τις οποίες απουσιάζουν σημαντικά μεταδεδομένα. Τα μεταδεδομένα παρέχουν το απαραίτητο πλαίσιο για την αξιολόγηση των αποδεικτικών στοιχείων με παρόμοιο τρόπο όπως μια σφραγίδα παρέχει πλαίσιο για την αξιολόγηση της έντυπης επιστολής και του περιεχομένου της.[110] Τα ηλεκτρονικά αποδεικτικά στοιχεία περιλαμβάνουν μεταδεδομένα και μπορούν να χρησιμοποιηθούν για τον εντοπισμό και την ταυτοποίηση της πηγής και του προορισμού μιας επικοινωνίας, των δεδομένων της συσκευής που παρήγαγε τα ηλεκτρονικά αποδεικτικά στοιχεία, της ημερομηνίας, της ώρας, της διάρκειας και του τύπου των αποδεικτικών στοιχείων. Στην Ιρλανδία, στην υπόθεση *Koger Inc. & Koger (Dublin) Ltd*,[111] τα μεταδεδομένα θεωρήθηκαν σημαντικά για την πιστοποίηση της προέλευσης των ηλεκτρονικά δημιουργημένων εγγράφων.

Τα ψηφιακά αποδεικτικά στοιχεία διαδραματίζουν σημαντικό ρόλο σε διάφορες φάσεις των ερευνών για τα εγκλήματα στον κυβερνοχώρο.[112] Σε γενικές γραμμές, είναι δυνατόν να διακριθούν δύο φάσεις: Η πρώτη φάση είναι αυτή της έρευνας, όπου εντοπίζεται το σχετικό

[109] Βλ. *C. Michailidou*, Cybercrime and electronic evidence – a way of identifying its digital prints. Europe at a glance, 2018, ηλεκτρονικά διαθέσιμο σε: https://theartofcrime.gr/cybercrime-and-electronic-evidence-a-way-of-identifying-its-digital-prints-europe-at-a-glance/#_ftnref3

[110] Βλ. *S. Mason (ed.)*, Electronic Evidence: Disclosure, Discovery & Admissibility, 2007, παρ. 2.09.

[111] Βλ. *Koger Inc. & Koger (Dublin) Ltd v O'Donnell & Others* [2010] IEHC 350.

[112] Βλ. *M. Gercke*, ITU publication, Understanding cybercrime: phenomena, challenges and legal response, 2012, σελ. 227.

αποδεικτικό υλικό, συλλέγονται και διατηρούνται τα αποδεικτικά στοιχεία, αναλύεται η τεχνολογία των υπολογιστών και των ψηφιακών αποδεικτικών στοιχείων. Η δεύτερη φάση είναι αυτή της παρουσίασης και χρήσης των αποδεικτικών στοιχείων στην ποινική διαδικασία. Η πρώτη φάση συνδέεται με την εγκληματολογία υπολογιστών, η οποία περιγράφει τη συστηματική ανάλυση του εξοπλισμού πληροφορικής με σκοπό την αναζήτηση ψηφιακών αποδεικτικών στοιχείων. Η εγκληματολογία υπολογιστών περιλαμβάνει έρευνες, όπως η ανάλυση του υλικού και του λογισμικού που χρησιμοποιεί ένας ύποπτος, η ανάκτηση διαγραμμένων αρχείων, η αποκρυπτογράφηση αρχείων ή η ταυτοποίηση χρηστών του διαδικτύου μέσω της ανάλυσης δεδομένων κίνησης. Το Ανώτατο Δικαστήριο της Ιταλίας επέτρεψε, για παράδειγμα, την κατάσχεση ολόκληρου σφραγισμένου διακομιστή ενός δικηγόρου υπό έρευνα προκειμένου να επαληθευτεί το περιεχόμενο του.[113] Η δεύτερη φάση σχετίζεται με την παρουσίαση ψηφιακών αποδεικτικών στοιχείων στο Δικαστήριο και συνδέεται στενά με συγκεκριμένες διαδικασίες που απαιτούνται επειδή οι ψηφιακές πληροφορίες μπορούν να γίνουν ορατές μόνο όταν εκτυπωθούν ή εμφανιστούν με τη χρήση τεχνολογίας υπολογιστών. Η ανάγκη αντιμετώπισης των ψηφιακών αποδεικτικών στοιχείων δημιουργεί προκλήσεις όσον αφορά το γεγονός ότι τα ψηφιακά αποδεικτικά στοιχεία δεν μπορούν να παρουσιαστούν χωρίς εργαλεία, όπως εκτυπωτές ή οθόνες. Οι αίθουσες συνεδριάσεων πρέπει να εξοπλιστούν με οθόνες για να διασφαλιστεί ότι οι δικαστές, ο εισαγγελέας, οι συνήγοροι υπεράσπισης και φυσικά οι κατηγορούμενοι μπορούν να παρακολουθούν την διατήρηση των αποδεικτικών στοιχείων. Ωστόσο, η εγκατάσταση και η συντήρηση τέτοιου εξοπλισμού δημιουργεί σημαντικό κόστος για τα δικαστικά συστήματα.[114]

Γ.3.β.-Τα νομοθετικά μέτρα της ΕΕ για τα ηλεκτρονικά αποδεικτικά στοιχεία

Σήμερα, πολλές από τις χρήσιμες πληροφορίες που απαιτούνται για ποινικές έρευνες και διώξεις αποθηκεύονται στο υπολογιστικό νέφος (cloud), σε διακομιστή σε άλλη χώρα ή/και σε παρόχους υπηρεσιών που βρίσκονται σε άλλες χώρες.[115] Η Ευρωπαϊκή Επιτροπή έχει προτείνει μία σειρά νομοθετικών μέτρων για τη διευκόλυνση και επιτάχυνση της πρόσβασης των αρχών επιβολής

[113] Βλ. Cass sez V, 19.3.2002, n. 2816, *Manganello*, in CP 2004, 1339.

[114] Βλ. *M. Gercke*, ITU publication, Understanding cybercrime: phenomena, challenges and legal response, 2012, σελ. 228 επ.

[115] Βλ. *M. Gercke*, ITU publication, Understanding cybercrime: phenomena, challenges and legal response, 2012, σελ. 241.

του νόμου, αλλά και των δικαστικών αρχών σε ηλεκτρονικά αποδεικτικά στοιχεία για την καλύτερη καταπολέμηση του εγκλήματος και της τρομοκρατίας,[116] με σκοπό να εξοπλιστούν οι φορείς με τα κατάλληλα εργαλεία για τη διερεύνηση και τη δίωξη εγκλημάτων στην ψηφιακή εποχή. Οι νέοι κανόνες που προτάθηκαν αναμένεται ότι θα παράσχουν ένα ταχύτερο και αποτελεσματικό εργαλείο για την απόκτηση ηλεκτρονικών αποδεικτικών στοιχείων.[117]

Η Πρόταση αυτή της Επιτροπής αναφορικά με τις ηλεκτρονικές αποδείξεις θεωρήθηκε ως ένα από τα πιο επείγοντα νομοθετικά σχέδια, απαραίτητο για να μπορέσουν οι αρχές επιβολής του νόμου σε όλη την Ευρωπαϊκή Ένωση να διερευνούν αποτελεσματικά τα εγκλήματα. Ωστόσο, χρειάστηκαν επτά χρόνια από τότε που ζητήθηκε να εξεταστεί το εν λόγω εγχείρημα το 2016 και περισσότερα από πέντε χρόνια από τότε που η Ευρωπαϊκή Επιτροπή πρότεινε τα νομοθετικά μέτρα σχετικά με τα ηλεκτρονικά αποδεικτικά στοιχεία (E-Evidence) σε ποινικές υποθέσεις, με τη νομοθετική διαδικασία να ολοκληρώνεται τελικά το καλοκαίρι του 2023. Κατά τις διαπραγματεύσεις παρουσιάστηκαν έντονα αποκλίνουσες απόψεις. Ωστόσο, κοινό παρονομαστή αποτέλεσε η κοινά αποδεκτή άποψη ότι υπάρχει ανάγκη να υιοθετηθούν το συγκεκριμένο νομοθετικό μέτρο, με το αρχικό κείμενο της Επιτροπής πάντως να έχει τροποποιηθεί ουσιωδώς από το Συμβούλιο και το Κοινοβούλιο.[118]

Το νομοθετικό αυτό εγχείρημα ξεκίνησε με σκοπό την παροχή ενός καινοτόμου νομικού πλαισίου που θα επιτρέπει την αντιμετώπιση των πρωτοφανών προκλήσεων που αντιμετωπίζουν οι αστυνομικές και δικαστικές αρχές κατά την πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία. Τα ηλεκτρονικά αποδεικτικά στοιχεία είναι απαραίτητα σε ποσοστό μεγαλύτερο του 85% του συνόλου των ποινικών ερευνών, αλλά συχνά βρίσκονται σε άλλες δικαιοδοσίες, στις οποίες είναι εγκατεστημένος ο πάροχος υπηρεσιών, όπως για παράδειγμα

---

[116] Βλ. Πρόταση ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις, COM/2018/225 final - 2018/0108 (COD), Έγγραφο 52018PC0225, Πρόταση ΟΔΗΓΙΑ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον ορισμό νόμιμων εκπροσώπων με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών, COM/2018/226 final - 2018/0107 (COD), Έγγραφο 52018PC0226.

[117] Βλ. *C. Michailidou*, Cybercrime and electronic evidence – a way of identifying its digital prints. Europe at a glance, 2018, ηλεκτρονικά διαθέσιμο σε: https://theartofcrime.gr/cybercrime-and-electronic-evidence-a-way-of-identifying-its-digital-prints-europe-at-a-glance/#_ftnref3

[118] Βλ. επί του ζητήματος, *G. Forlani*, The E-evidence Package. The Happy Ending of a Long Negotiation Saga, EUcrim 2, 2023, σελ. 174 επ.

ένας πάροχος cloud ή μια εταιρία μέσων κοινωνικής δικτύωσης. Τα παραδοσιακά μέσα αμοιβαίας δικαστικής συνδρομής, ή τα νέα μέτρα που βασίζονται στην αρχή της αμοιβαίας αναγνώρισης, με χαρακτηριστικό παράδειγμα την ευρωπαϊκή εντολή έρευνας, τα οποία εξαρτώνται από διακρατικά αιτήματα, θεωρούνται δυσκίνητα και χρονοβόρα.[119]

Τα νομοθετικά μέτρα για τις ηλεκτρονικές αποδείξεις βασίστηκαν σε μία εντελώς διαφορετική προσέγγιση, εισάγοντας έναν μηχανισμό που επιτρέπει στις αρμόδιες αρχές να αιτούνται δεδομένα σχετικά με ποινικές έρευνες απευθείας από τους παρόχους υπηρεσιών. Το νέο νομοθετικό καθεστώς για τις ηλεκτρονικές αποδείξεις αποσκοπεί στη δημιουργία ενός πρωτοφανούς νομικού πλαισίου σε όλη την ΕΕ για την *«απευθείας συνεργασία»* μεταξύ των δικαστικών αρχών και των παρόχων υπηρεσιών στο πεδίο των ποινικών διαδικασιών, χωρίς, καταρχήν, να μεσολαβεί κράτος άλλο από αυτό που εκδίδει την εντολή.[120]

Τα νομοθετικά μέτρα της ΕΕ για της ηλεκτρονικές αποδείξεις αντιπροσωπεύουν μια σημαντική αλλαγή στην αστυνομική και δικαστική συνεργασία με τους παρόχους υπηρεσιών στην ΕΕ. Για πρώτη φορά, οι εθνικές ανακριτικές αρχές θα μπορούν να ζητούν απευθείας από τους παρόχους υπηρεσιών σε άλλα κράτη μέλη να παραδώσουν ή να διασφαλίσουν ηλεκτρονικά αποδεικτικά στοιχεία, μέσω εντολών παράδοσης ή διατήρησης, υποστηριζόμενες από σαφείς προθεσμίες και ομοιόμορφους κανόνες σε ολόκληρη την ΕΕ. Για πρώτη φορά, οι πάροχοι υπηρεσιών θα υποχρεούνται από το ευρωπαϊκό δίκαιο να συμμορφώνονται με τις εν λόγω εντολές, ανεξάρτητα από τη χώρα εγκατάστασής τους ή τον τόπο όπου βρίσκονται τα δεδομένα. Η προσδοκία είναι ότι αυτό το νομοθετικό πακέτο μέτρων, το οποίο βασίζεται στην άμεση συνεργασία μεταξύ των αρχών μιας χώρας της ΕΕ και τους παρόχους υπηρεσιών μιας άλλης χώρας, θα βελτιώσει σημαντικά την αποτελεσματικότητα των διασυνοριακών ποινικών ερευνών και θα επιλύσει πολλά πρακτικά και νομικά προβλήματα που αντιμετωπίζουν σήμερα οι αρχές επιβολής του νόμου σε όλη την Ευρώπη σε ποσοστό μεγαλύτερο από το ήμισυ του συνόλου των

[119] Βλ. *S. Tosza*, All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order, New Journal of European Criminal Law 11-2, 2020, σελ. 161 επ.

[120] Βλ. *V. Franssen*, The European Commission's E-Evidence Proposal: Toward an EU-Wide Obligation for Service Providers to Cooperate with Law Enforcement?', European Law Blog, 2018, ηλεκτρονικά διαθέσιμο σε: https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wideobligation-for-service-providers-to-cooperate-with-law-enforcement

ποινικών ερευνών, ιδίως στον χώρο του ηλεκτρονικού εγκλήματος. Ωστόσο, αυτός ο φιλόδοξος νέος μηχανισμός άμεσης συνεργασίας εγείρει πολλά νέα νομικά ζητήματα και εγκυμονεί ορισμένους κινδύνους που σχετίζονται με τα θεμελιώδη δικαιώματα, ιδίως με την ιδιωτική ζωή και την προστασία δεδομένων, αλλά και με τα δικονομικά δικαιώματα, λόγω των σημαντικών διαφορών στο ποινικό δίκαιο μεταξύ των κρατών μελών της ΕΕ.[121]

Δ.-ΣΥΜΠΕΡΑΣΜΑΤΙΚΕΣ ΣΚΕΨΕΙΣ

Συμπερασματικά, η οριοθέτηση του τόπου τέλεσης ενός κυβερνοεγκλήματος αποτελεί σύνθετο πρόβλημα. Ελλείψει ύπαρξης κοινών διεθνών κανόνων επί του ζητήματος, η λύση πρέπει να αναζητηθεί στους εθνικούς κανόνες του διεθνούς ποινικού δικαίου. Ωστόσο, η εφαρμογή των εθνικών αυτών κανόνων πρέπει να συμβαδίζει και να είναι προσαρμοσμένη στα ιδιαίτερα χαρακτηριστικά γνωρίσματα του διαδικτύου, με ιδιαίτερη έμφαση στο είδος της αξιόποινης

[121] Αναλυτικά επί του ζητήματος, βλ. *T. Christakis*, From Mutual Trust to the Gordian Knot of Notifications The EU E-Evidence Regulation and Directive, σε: *V. Franssen/ S Tosza (eds)*, The Cambridge Handbook of Digital Evidence in Criminal Matters, 2023, ηλεκτρονικά διαθέσιμο σε: https://ssrn.com/abstract=4306874

πράξης και στη μορφή της χρησιμοποιούμενης τεχνολογίας. Έτσι, η αρχή της εδαφικότητας εφαρμόζεται με δύο διακρίσεις: Πρώτον, η ανάρτηση δεδομένων από χρήστη, στα οποία δεδομένα αποκτάται πρόσβαση από τρίτα πρόσωπα με δικές τους ενέργειες, συνεπάγεται ως τόπο τέλεσης της πράξης, αφενός, τον τόπο στον οποίο παρευρίσκεται φυσικά ο χρήσης, όταν αναρτά τα δεδομένα, αφετέρου, τον τόπο στον οποίο οι διακομιστές αποθηκεύουν τα δεδομένα, υπό την προϋπόθεση της γνώσης του τόπου αποθήκευσης από τον χρήστη. Δεύτερον, η αποστολή δεδομένων από τον χρήστη σε τρίτους συνεπάγεται ως επιπρόσθετο τόπο τέλεσης τον τόπο επέλευσης του αποτελέσματος, είτε αυτό εκδηλωθεί βλάβη, είτε ως συγκεκριμένος κίνδυνος. Κατά τη γνώμη της γράφουσας, η εφαρμογή μίας τέτοιας λύσης εμφανίζεται ως η ορθότερη, καθώς αφενός είναι ικανή να παράσχει ένα ρυθμιστικό πλαίσιο με επαρκές επίπεδο ασφάλειας δικαίου, αφετέρου αποφεύγεται έτσι η σύγκρουση πλειόνων ποινικών δικαιοδοσιών, η οποία αναπόφευκτα προκύπτει από τον κατακερματισμό που δημιουργεί στις δικαιοδοσίες των κρατών ένα διεθνοποιημένο διαδικτυακό περιβάλλον.

Ταυτόχρονα, ιδιαίτερα σημαντικός είναι ο ρόλος των ενδιάμεσων παρόχων, διότι επιτυγχάνουν την εκμηδένιση των τεράστιων αποστάσεων, στις οποίες δραστηριοποιείται το διαδίκτυο, και τα δεδομένα καθίστανται έτσι προσιτά παγκοσμίως στους χρήστες. Ασχέτως όμως της συμμετοχής ή μη των ενδιάμεσων παρόχων, η σημαντική διαφορά που αναδεικνύει το διαδικτυακό έγκλημα σε ιδιαίτερο ερευνητικό αντικείμενο είναι ο καινοφανής τρόπος με τον οποίο λειτουργούν οι δράστες των αδικημάτων του κυβερνοχώρου, εξαιτίας των ιδιαίτερων γνωρισμάτων του διαδικτύου. Τα εικονικά ιδιωτικά δίκτυα (VPN), οι διακομιστές μεσολάβησης και ο δρομολογητής Onion (TOR) είναι ανεκτίμητα εργαλεία για άτομα που αναζητούν αυξημένη διαδικτυακή ασφάλεια, ωστόσο επωφελούν και τους δράστες των κυβερνοεγκλημάτων μέσω της απόκρυψης των ψηφιακών τους ιχνών, θεμέλιους λίθους στην έρευνα του εγκλήματος στον κυβερνοχώρο. Σε εθνικό επίπεδο, ο Ν. 5002/2022 εξοπλίζει τις αρχές επιβολής του νόμου με το μέτρο της άρσης του απορρήτου των επικοινωνιών, το αντικείμενο του οποίου εκτείνεται και στα εξωτερικά στοιχεία της επικοινωνίας. Λαμβάνοντας υπόψη τη σημασία των ηλεκτρονικών δεδομένων ως αποδεικτικών στοιχείων, η νομοθετική παρέμβαση της ΕΕ για τα ηλεκτρονικά αποδεικτικά στοιχεία συνιστά την επίτευξη ενός κρίσιμου εργαλείου ενόψει των μελλοντικών εξελίξεων στη δικαστική συνεργασία σε ποινικές υποθέσεις. Οι πιο αξιοσημείωτες καινοτομίες του νέου νομικού πλαισίου αφορούν, αφενός, το γεγονός ότι

είναι αδιάφορος ο τόπος όπου βρίσκονται τα δεδομένα, αφετέρου, την προσπάθεια να προβλεφθεί μια άμεση σχέση μεταξύ του αιτούντος κράτους και του παρόχου υπηρεσιών, με την αρμόδια αρχή του κράτους εκτέλεσης να παρεμβαίνει μόνο εξαιρετικά. Παρά τις όποιες επιφυλάξεις έχουν διατυπωθεί για το νέο νομικό πλαίσιο, δοθέντος ότι η δυναμική φύση της τεχνολογίας και το εξελισσόμενο τοπίο του εγκλήματος στον κυβερνοχώρο θέτουν συνεχείς προκλήσεις, κατά τη γνώμη της γράφουσας, ο Ευρωπαίος νομοθέτης κινείται προς τη σωστή κατεύθυνση, διότι η άμεση επικοινωνία των δικαστικών και αστυνομικών αρχών με τους παρόχους υπηρεσιών επιτρέπει την πρόσβαση σε κρίσιμα δεδομένα χρηστών και ενισχύει περαιτέρω την αποτελεσματικότητα της ποινικής έρευνας του ηλεκτρονικού εγκλήματος.

Ε.-ΒΙΒΛΙΟΓΡΑΦΙΑ – ΑΡΘΡΟΓΡΑΦΙΑ

- *Ι. Αγγελής*, Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, ΠοινΔικ 2001, σελ. 1218 επ.
- *Ι. Αγγελής*, Έγκλημα στον κυβερνοχώρο (Cybercrime - Internet Crime), ΠοινΧρον 2000, σελ. 675 επ.
- *Ε. Αλεξανδρίδου*, Το δικαιο του ηλεκτρονικού εμπορίου, 2010.

- *Ν. Ανδρουλάκης*, Ποινικό δίκαιο, Γενικό Μέρος, 2006.
- *Ν. Ανδρουλάκης κ.ά.*, Συστηματική Ερμηνεία Ποινικού Κώδικα, 2005.
- *Κ. Βλαχόπουλος*, Ηλεκτρονικό Έγκλημα, Μορφές, Πρόληψη, Αντιμετώπιση, 2007.
- *Ι. Γιαννίδης*, σε: *Ν. Ανδρουλάκη κ.ά.*, Συστηματική Ερμηνεία Ποινικού Κώδικα, 2005, άρθρο 14.
- *Γ. Γιαννόπουλος*, Η ευθύνη των παρόχων υπηρεσιών στο Internet, 2013.
- *Γ. Γιαννόπουλος*, Ροή πληροφοριών στο διαδίκτυο, τεχνολογία και νομικές ρυθμίσεις, 2002.
- *Θ. Δαλακούρας*, Ηλεκτρονικό έγκλημα, ουσιαστικές και δικονομικές όψεις, 2023.
- *Θ. Δαλακούρας*, Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν 4411/2016) , σε *Θ. Δαλακούρα*, Ηλεκτρονικό έγκλημα, ουσιαστικές και δικονομικές όψεις, 2023.
- *Ε. Διαμαντής*, Ευθύνη των μεσαζόντων παροχής υπηρεσιών στο διαδικτυο κατά το ΠΔ 131/2003 - Ενσωμάτωση της Οδηγίας 2000/31 για το ηλεκτρονικό εμπόριο στο εθνικό δικαιο, Δίκαιο Επιχειρήσεων & Εταιριών 10/2004, σελ. 986 επ.
- *Ε. Μεταξάκης*, Κυβερνοέγκλημα, 2022.
- *Ι. Ιγγλεζάκης*, Δίκαιο Πληροφορικής, 4η εκδ., 2021.
- *Ι. Ιγγλεζάκης*, Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου, 2003.
- *Μ. Καϊάφα- Γκμπάντι*, Ποινικό Δίκαιο και Καταχρήσεις της Πληροφορικής, Αρμ 2007, σελ. 1058 επ.
- *Μ. Καϊάφα- Γκμπάντι*, Κοινώς επικίνδυνα εγκλήματα, 2005.
- *Κ. Κακαβούλης*, Η συμμετοχική ευθύνη των ενδιάμεσων παρόχων Internet στα διαδικτυακά εγκλήματα, ΠοινΧρ 2015, σελ. 326 επ.
- *Ι. Καρακώστας*, Δίκαιο και internet, 2009.
- *Δ. Κιούπης*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, σε *Θ. Δαλακούρα*, Ηλεκτρονικό έγκλημα, ουσιαστικές και δικονομικές όψεις, 2023.
- *Δ. Κιούπης*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος και η απροσδόκητη διεύρυνση της έννοιας της «ημεδαπής» (άρθρο 5 παρ. 3 ΠΚ), ΠοινΧρ, 2014, σελ 561 επ.
- *Δ. Κιούπης*, Δημοσίευση ιστοσελίδων με αξιόποινο περιεχόμενο, ΠΛογ, 2001, σελ. 402 επ.
- *Δ. Κιούπης*, Ποινικό δίκαιο και internet, 1999,

- *Ι. Μανδωλεδάκης/C. Prittwitz*, Διεθνοποίηση του ποινικού δικαίου, 2003.
- *Μ. Μαργαρίτης/Α. Μαργαρίτη*, Ποινικός Κώδικας Ερμηνεία – Εφαρμογή, έκδοση 4η, 2020.
- *Χ. Μυλωνόπουλος*, Διεθνές και Ευρωπαϊκό Ποινικό Δίκαιο, 2021.
- *Χ. Μυλωνόπουλος*, Ποινικό Δίκαιο - Γενικό Μέρος, Ι, 2007.
- *Χ. Μυλωνόπουλος*, σε: *Ν. Ανδρουλάκη κ.ά.*, Συστηματική Ερμηνεία Ποινικού Κώδικα, 2005, άρθρο 16.
- *Χ. Μυλωνόπουλος*, Διεθνές Ποινικό Δίκαιο, Τα τοπικά όρια των ποινικών νόμων, 1993.
- *Γ. Πάγκαλος/ Ι. Μαυρίδης*, Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων, 2002.
- *Ε. Συμεωνίδου – Καστανίδου*, Νέοι Νόμοι - Ο νόμος 5002/2022 σχετικά με την άρση του απορρήτου των επικοινωνιών (ΦΕΚ Α΄ 228/9-12-2022): κρίσιμες για τις θεμελιώδεις ελευθερίες «αστοχίες», ΠοινΔικ, 2023, σελ. 108 επ.
- *Ε. Συμεωνίδου- Καστανίδου*, Η διαβάθμιση του κινδύνου στα εγκλήματα διακινδύνευσης, Τιμ. Τόμος για τον Δ. Σπινέλλη, 2001, σελ. 1041 επ.
- *Γ. Τσόλια*, Το νομικό πλαίσιο άρσης του απορρήτου των ηλεκτρονικών επικοινωνιών για τη διακρίβωση εγκλημάτων σύμφωνα με τις διατάξεις του Ν 5002/2022και η απολεσθείσα ευκαιρία εκσυγχρονισμού του, ΠοινΔικ, 2023, σελ. 242 επ.
- *G.O. Boussia/ H. Gupta/S. A. Hossain*, Financial Crime: A Conceptual Framework Implementation for Prevention of Malicious Request from a VPN or Proxy Server, Scope 13, 2023, σελ. 375 επ.
- *W. Buchanan*, Transmission Control Protocol (TCP) and Internet Protocol (IP), σε: *W. Buchanan*, Applied Data Communications and Networks, 1996.
- *W. Buchanan*, Applied Data Communications and Networks, 1996.
- *S. Burnett/S. Paine*, RSA Security's Official Guide to Cryptography, 2001.
- *T. Christakis*, From Mutual Trust to the Gordian Knot of Notifications The EU E-Evidence Regulation and Directive, σε: *V. Franssen/ S Tosza (eds)*, The Cambridge Handbook of Digital Evidence in Criminal Matters, 2023, ηλεκτρονικά διαθέσιμο σε: https://ssrn.com/abstract=4306874

  R. Dingledine/N. Mathewson/P.F. Syverson, Tor: The second-generation onion router, USENIX security symposium 4, 2004, ηλεκτρονικά διαθέσιμο σε:

https://www.usenix.org/legacy/publications/library/proceedings/sec04/tech/full_papers/dingledine/dingledine.pdf

- *D. Dorr/S. Janich*, The Criminal Responsibility of Internet Service Providers in Germany, Mississippi Law Journal 80, 2010, σελ. 1247 επ.
- *P. Ferguson/G. Huston*, What is a VPN?, 1998, ηλεκτρονικά διαθέσιμο σε: https://courses.e-ce.uth.gr/CE370/vpn.pdf
- *G. Forlani*, The E-evidence Package. The Happy Ending of a Long Negotiation Saga, EUcrim 2, 2023, σελ. 174 επ.
- *B. A. Forouzan*, Introduction to cryptography and network security, 2008.
- *V. Franssen/ S Tosza (eds)*, The Cambridge Handbook of Digital Evidence in Criminal Matters, 2023.
- *V. Franssen*, The European Commission's E-Evidence Proposal: Toward an EU-Wide Obligation for Service Providers to Cooperate with Law Enforcement?', European Law Blog, 2018, ηλεκτρονικά διαθέσιμο σε:
- https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wideobligation-for-service-providers-to-cooperate-with-law-enforcement
- *M. Gercke*, ITU publication, Understanding cybercrime: phenomena, challenges and legal response, 2012.
- *J. Goldsmith/T. Wu*, Who controls the Internet, 2006.
- *O. Hutt, κ.ά.,* Data and evidence challenges facing place-based policing, Policing: An International Journal 41/3, 2018, σελ. 339 επ.
- *G. Huston*, Web caching, The Internet Protocol Journal 2-3, 1999, ηλεκτρονικά διαθέσιμο σε: https://www.potaroo.net/papers/ipj/2-3-caching.pdf
- *N. Ianelli/A. Hackworth*, Botnets as a vehicle for online crime, CERT Coordination Center 1/1, 2005, ηλεκτρονικά διαθέσιμο σε: https://insights.sei.cmu.edu/documents/273/2005_019_001_51249.pdf
- *E. Jardine*, The Dark Web dilemma: Tor, anonymity and online policing, Global Commission on Internet Governance Paper Series 21, 2015, ηλεκτρονικά διαθέσιμο σε: https://www.cigionline.org/sites/default/files/no.21.pdf

- *P. Kedia*, Crime mapping and analysis using GIS, International Institute of Information Technology 1-1, 2016, σελ. 1 επ.
- *D.Y. Kao /W. Shiuh-Jeng*, The IP address and time in cyber-crime investigation, Policing: an international Journal of Police strategies & Management 32/2, 2009, σελ. 194 επ.
- S. *Kaur/S. Randhawa,* Dark web: A web of crimes, Wireless Personal Communications 112, 2020, σελ. 2131 επ.
- *A. Krunoslav /I. Varjačić /M. Jelenski*, Combating Cyber Crime, Academic and Applied Research in Military and Public Management Science 17/3, 2018, σελ. 19 επ.
- *A. Luotonen*, Web proxy servers, 1998.
- *S. Mason*, Council of Europe, European Committee on legal co-operation (CDCJ), The use of electronic evidence in civil and administrative law proceedings and its effect on the rules of evidence and modes of proof, A comparative study and analysis, CDCJ (2015) 14 final, 2016.
- *S. Mason*, International Electronic Evidence, 2008.
- *S. Mason (ed.)*, Electronic Evidence: Disclosure, Discovery & Admissibility, 2007.
- *C. Michailidou*, Cybercrime and electronic evidence – a way of identifying its digital prints. Europe at a glance, 2018, ηλεκτρονικά διαθέσιμο σε: https://theartofcrime.gr/cybercrime-and-electronic-evidence-a-way-of-identifying-its-digital-prints-europe-at-a-glance/#_ftnref3
- *J. Morinigiello/W. Reynolds*, The new territorialism in the not-so-new frontier of cyberspace, Cornell Law Review, 2014, σελ. 1415 επ.
- *U. Neumann*, Η αρχή της παγκοσμιοποιημένης δικαιοσύνης σε μία παγκοσμιοποιημένη κοινότητα δικαίου, σε: *I. Μανδωλεδάκη/C. Prittwitz*, Διεθνοποίηση του ποινικού δικαίου, 2003.
- *J. Petersilia/S. Turner*, Intensive probation and parole, Crime and justice 17, 1993, σελ. 281 επ.
- *G. Sartor*, Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?, International Data Privacy Law 3-1, 2013, ηλεκτρονικά διαθέσιμο σε: https://academic.oup.com/idpl/article/3/1/3/643990
- *R. Snader/N. Borisov,* A Tune-up for Tor: Improving Security and Performance in the Tor Network, 15th Network and Distributed System Security Symposium (NDSS) 8, 2008, ηλεκτρονικά διαθέσιμο σε: https://www.freehaven.net/anonbib/cache/snader08.pdf
- *F. Steven*, Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, 2006.

- *S. Turner/J. Petersilia/E.P. Deschenes*, Evaluating intensive supervision probation/parole (ISP) for drug offenders, Crime & Delinquency 38/4, 1992, σελ. 539 επ.
- *S. Tosza*, All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order, New Journal of European Criminal Law 11-2, 2020, σελ. 161 επ.
- *Z. Zhang κ.ά.*, An overview of virtual private network (VPN): IP VPN and optical VPN, Photonic network communications 7, 2004.
- *A.T. Zulkarnine κ.ά.* Surfacing collaborated networks in dark web to find illicit and criminal content, 2016 IEEE Conference on Intelligence and Security Informatics (ISI), 2016, σελ. 109 επ.

ΣΤ.-ΝΟΜΟΛΟΠΑ

- Ολομ ΑΠ 7/2002, ΠοινΧρ ΝΒ, σελ. 704
- ΑΠ 586/2021, ΤΝΠ ΝΟΜΟΣ.
- ΑΠ 1177/2019, ΤΝΠ ΝΟΜΟΣ.
- ΑΠ 318/2019, ΤΝΠ ΝΟΜΟΣ.
- ΑΠ 286/2019, ΤΝΠ ΝΟΜΟΣ.

- ΑΠ 2080/2017, ΤΝΠ ΝΟΜΟΣ.
- ΑΠ 752/2017, ΤΝΠ ΝΟΜΟΣ.
- ΑΠ 1613/2000, ΤΝΠ ΝΟΜΟΣ.
- ΑΠ 1500/2006, ΠοινΧρ ΝΖ, σελ. 704.
- ΑΠ 2334/2004, ΤΝΠ ΝΟΜΟΣ.
- ΑΠ 136/2004, ΤΝΠ ΝΟΜΟΣ.
- ΑΠ 905/1981, ΠοινΧρ ΛΒ, σελ. 162.
- ΑΠ 761/1975, ΠοινΧρ ΚΣΤ, σελ. 150.
- ΕφΑθ 6613/2016, ΤΝΠ ΝΟΜΟΣ
- ΕφΑΘ 226/1982, ΠοινΧρ ΛΒ, σελ. 434.
- ΠλημμΑθ 3087/2022, ΤΝΠ ΝΟΜΟΣ.
- ΠλημμΑθ 1794/2008, ΤΝΠ ΝΟΜΟΣ.
- ΠλημμΝαυπλ 78/1991, ΠοινΧρ ΜΒ, σελ. 71.
- ΠλημμΑθ 3169/1975, ΠοινΧρ Λ, σελ. 85.
- *Koger Inc. & Koger (Dublin) Ltd v O'Donnell & Others* [2010] IEHC 350
- Cass sez V, 19.3.2002, n. 2816, *Manganello*, in CP 2004, 1339.
- *Eparhos Lemesou v Giorgalla* [2003] 2 CLR 298.