Πάντειο Πανεπιστήμιο

Κοινωνικών και Πολιτικών Επιστημών

Τμήμα Δημόσιας Διοίκησης

Πρόγραμμα Μεταπτυχιακών Σπουδών:

«Δίκαιο, Τεχνολογία και Οικονομία»

Διπλωματική Εργασία

«Κυβερνοέγκλημα σε περιβάλλον υπολογιστικού νέφους: τεχνολογικές προκλήσεις & νομικά ζητήματα που προκύπτουν κατά τη διερεύνηση»

Γεωργίου Νικόλαος του Χρήστου
Α.Μ. 7115Μ017

Επιβλέπων: **Καθηγητής Αντώνιος Χάνος**

Αθήνα, Φεβρουάριος 2017

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Με την παρούσα εργασία επιχειρείται ο προσδιορισμός και ανάλυση των κρίσιμων τεχνικών και νομικών πτυχών της διερεύνησης κυβερνοεγκλημάτων στο υπολογιστικό νέφος μέσω της εγκληματολογικής εξέτασης ψηφιακών πειστηρίων. Οι τεχνικές προκλήσεις, προέρχονται από τις ραγδαίες εξελίξεις στην τεχνολογία και την πληροφορική και δυσχεραίνουν το έργο των αρχών επιβολής του νόμου για την εξιχνίαση των κυβερνοεγκλημάτων στο πλαίσιο του υπολογιστικού νέφους. Ενώ, οι νομικές προκλήσεις προκαλούνται από τη δυσκολία του εκάστοτε εφαρμοζόμενου νομικού πλαισίου να συμβαδίσει με τις τεχνολογικές εξελίξεις. Η ψηφιακή εγκληματολογία, συμμορφούμενη με τα θεμελιώδη δικαιώματα, μπορεί να αποτελέσει ένα εργαλείο άμβλυνσης του χάσματος μεταξύ τους.

Λέξεις κλειδιά

Κυβερνοέγκλημα, ηλεκτρονικό έγκλημα, υπολογιστικό νέφος, διερεύνηση, πειστήρια, τεχνολογικές προκλήσεις, νομικές προκλήσεις

SUMMARY

This paper attempts to identify and analyze the critical technical and legal aspects of cybercrime investigation in the cloud environment, through forensic examination. Technical challenges arising from the rapid development in technology and computing hamper the work of law enforcement authorities for the detection of cybercrime within the cloud. While legal challenges are caused by the difficulty of each applicable legal framework to keep up with technological developments. The digital forensics, complying with fundamental rights, may be a gap mitigation tool between them.

Keywords

Cybercrime, cloud computing, investigation, evidence, technological challenges, legal challenges

ΕΙΣΑΓΩΓΗ

Η ψηφιακή επανάσταση που λαμβάνει χώρα στην εποχή μας, χάρη στην αλματώδη εξέλιξη της τεχνολογίας και την ανάπτυξη της πληροφορικής, έχει οδηγήσει στην δημιουργία υποδομών που επιτρέπουν την σύνδεση ολοένα κα περισσότερων συσκευών στο διαδίκτυο, γεγονός που ευνοεί την συνεχώς αυξανόμενη διείσδυση των ηλεκτρονικών επικοινωνιών στην καθημερινότητα των πολιτών[1]. Το νέο αυτό ψηφιακό περιβάλλον και οι δυνατότητες που προσφέρει έχουν επιφέρει σημαντικές αλλαγές στο σύνολο των καθημερινών μας δραστηριοτήτων, στις κοινωνικές αλληλεπιδράσεις, στην οικονομία, την παραγωγική διαδικασία, τις συναλλαγές, ακόμη και στη διασκέδαση. Αναμφισβήτητα η ευρεία πρόσβαση στον κυβερνοχώρο και η μετάβαση στην Κοινωνία της Πληροφορίας συνεπάγεται πολλαπλά οφέλη[2].

Από τη άλλη πλευρά όμως, η ραγδαία αυτή ανάπτυξη της τεχνολογίας και η ευρεία διάδοση της χρήσης του διαδικτύου, καλλιεργεί τις αναγκαίες συνθήκες ανάπτυξης νέων μορφών εγκληματικής δραστηριότητας. Για την περιγραφή αυτής της νέας μορφής εγκλήματος χρησιμοποιούνται ποικίλοι όροι, όπως ηλεκτρονικό έγκλημα, έγκλημα στον κυβερνοχώρο - κυβερνοέγκλημα, έγκλημα με τη χρήση Η/Υ, κλπ. Το έγκλημα στον κυβερνοχώρο είναι μια ταχέως αναπτυσσόμενη πτυχή της εγκληματικότητας. Επηρεασμένοι από την εκθετικά αυξανόμενη διείσδυση της χρήσης του διαδικτύου σε κάθε έκφανση της ζωής μας, όλο και περισσότεροι εγκληματίες εκμεταλλευόμενοι την ταχύτητα και την ανωνυμία του διαδικτύου όπως και τη δυσκολία των διωκτικών αρχών στην διαλεύκανση της ηλεκτρονικής εγκληματικότητας, επιλέγουν πλέον το «ηλεκτρονικό έγκλημα» για να διαπράξουν ένα ευρύ φάσμα των εγκληματικών τους δραστηριοτήτων[3].

---

[1] Διαδικτυακός τόπος της Ανεξάρτητης Αρχής «Συνήγορος του καταναλωτή», Ενημέρωση του Καταναλωτή για την προστασία από το ηλεκτρονικό έγκλημα, 2008, διαθέσιμο εδώ :http://www.synigoroskatanaloti.gr/docs/info/info-Hlektroniko-Egklima.pdf

[2] Διαδικτυακός τόπος της Ελληνικής Αστυνομίας, http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414

[3] Διαδικτυακός τόπος της Interpol, https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

ΚΕΦΑΛΑΙΟ 1^{Ο} : ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ

Α. ΟΡΙΣΜΟΣ ΚΑΙ ΦΥΣΗ ΤΟΥ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ

Στην διεθνή νομοθεσία, νομολογία ή βιβλιογραφία δεν υφίσταται ακόμη ένας γενικά αποδεκτός ορισμός του εγκλήματος στον κυβερνοχώρο. Η δυσκολία διατύπωσης ενός ενιαίου ορισμού που να περιλαμβάνει όλες τις πλευρές του διαδικτυακού εγκλήματος έγκειται στο γεγονός ότι οι παράνομες πράξεις στο διαδίκτυο παρουσιάζουν πολυμορφία ως προς τις μορφές εκδήλωσής τους, η τεχνολογία εξελίσσεται συνεχώς και τα προσβαλλόμενα έννομα αγαθά διαφοροποιούνται και διευρύνονται. Η δομή αυτή του ηλεκτρονικού εγκλήματος (που τελείται με τη χρήση ηλεκτρονικού υπολογιστή) και ειδικότερα του κυβερνοεγκλήματος ή αλλιώς διαδικτυακού εγκλήματος (που τελείται μέσω του διαδικτύου) δυσχεραίνει ιδιαίτερα τον περιορισμό του σε έναν εξαντλητικό ορισμό και από την άλλη μας οδηγεί σε μια ιδιαίτερα ευρεία και αόριστη περιγραφή του ως μια μορφή εγκλήματος που περιλαμβάνει όλες εκείνες τις αξιόποινες πράξεις που τελούνται με τη χρήση του διαδικτύου.

Συνεχώς και περισσότερα κράτη θεσπίζουν ειδική νομοθεσία για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο. Έχει υποστηριχθεί η άποψη ότι δεν απαιτείται κατάρτιση νέας ειδικής νομοθεσίας για την αντιμετώπιση της εγκληματικότητας στο διαδίκτυο και ότι δεν υπάρχει νομικό κενό, διότι αναλογικά το κοινό δίκαιο μπορεί να εφαρμοστεί στον κυβερνοχώρο. Ωστόσο, η άποψη αυτή δεν ευσταθεί καθότι υπάρχουν βεβαίως εγκλήματα που λαμβάνουν χώρα τόσο σε κοινό, όσο και σε ηλεκτρονικό – διαδικτυακό περιβάλλον, υπάρχουν όμως και εγκλήματα που διαπράττονται αποκλειστικά στον κυβερνοχώρο[4].

Προς τη κατεύθυνση της αντιμετώπισης και περιορισμού αυτής της νέας και ραγδαία εξελισσόμενης μορφής εγκληματικότητας διάφορες προσπάθειες εκδηλώθηκαν δίχως τα αναμενόμενα αποτελέσματα, όπως διμερείς συμφωνίες μεταξύ κρατών που προκάλεσαν σύγχυση και διεθνείς κατευθυντήριες οδηγίες και συστάσεις οι οποίες δεν επαρκούσαν για την καταπολέμηση του φαινομένου.

[4] Αγγελής Ι.Μ., «Η προς ψήφιση Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο: η σχέση της με την ελληνική έννομη τάξη», Νομική Επιθεώρηση, Αριθμός τεύχους 30, 2001

Το Συμβούλιο της Ευρώπης πεπεισμένο για την ανάγκη να επιδιωχθεί μια κοινή αντεγκληματική πολιτική που στοχεύει στην προστασία της κοινωνίας έναντι της εγκληματικότητας στον κυβερνοχώρο, με τη θέσπιση κατάλληλης νομοθεσίας και την επίτευξη μιας ταχείας και εύρυθμης διεθνούς συνεργασίας σε ποινικές υποθέσεις, προέβη στη κατάρτιση της υπ' αριθ. 185 Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο», η οποία υπεγράφη στη Βουδαπέστη στις 23.11.2001. Πρόκειται ουσιαστικά για ένα νομικό εργαλείο που υπερέχει έναντι μιας απλής Σύστασης και περιέχει διατάξεις ουσιαστικού ποινικού αλλά και δικονομικού δικαίου καθώς και διαδικασίες διεθνούς (δικαστικής και αστυνομικής) συνεργασίας[5].

Στην εν λόγω Σύμβαση (Σύμβαση της Βουδαπέστης, 2001) δεν δίδεται κάποιος ορισμός του κυβερνοεγκλήματος αλλά περιγράφονται οι κατηγορίες εκείνες των εγκλημάτων που υπάγονται σε αυτό. Πιο συγκεκριμένα, στο δεύτερο κεφάλαιο που αφορά τις ρυθμίσεις στο ουσιαστικό ποινικό δίκαιο περιλαμβάνονται οι εξής κατηγορίες εγκλημάτων:

1. Εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων και συστημάτων υπολογιστών, που αναλύονται σε αυτά της:
    - Παράνομης πρόσβασης (Άρθρο 2)
    - Υποκλοπής (Άρθρο 3)
    - Παρεμβολής σε δεδομένα (Άρθρο 4)
    - Παρεμβολής σε συστήματα (Άρθρο 5)
    - Κακής χρήσης συσκευών (Άρθρο 6)
2. Εγκλήματα σχετικά με υπολογιστές, που αναλύονται σε αυτά της:
    - Πλαστογραφίας σχετιζόμενης με υπολογιστές (Άρθρο 7)
    - Απάτης σχετιζόμενης με υπολογιστές (Άρθρο 8).
3. Εγκλήματα σχετικά με το περιεχόμενο (πορνογραφία ανηλίκων - Άρθρο 9)
4. Εγκλήματα σχετικά με παραβιάσεις δικαιωμάτων πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων (Άρθρο 10)[6].

Το 2007 η Επιτροπή των Ευρωπαϊκών Κοινοτήτων σε ανακοίνωσή της προς την κατεύθυνση γενικής πολιτικής σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο ανανέωσε την ανωτέρω κατηγοριοποίηση των κυβερνοεγκλημάτων.

[5] Προοίμιο της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο
[6] Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο, Βουδαπέστη, No.185, 23/11/2011, διαθέσιμη εδώ : https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Σύμφωνα με αυτήν ο όρος έγκλημα στον κυβερνοχώρο εφαρμόζεται σε τρεις κατηγορίες αξιόποινων δραστηριοτήτων. Η πρώτη καλύπτει τις παραδοσιακές μορφές αδικημάτων όπως την απάτη ή την πλαστογραφία, οι οποίες διαπράττονται μέσω δικτύων ηλεκτρονικής επικοινωνίας και συστημάτων πληροφοριών. Η δεύτερη μορφή αφορά τη δημοσίευση παράνομου περιεχομένου με χρήση ηλεκτρονικών μέσων (π.χ., υλικό σεξουαλικής κακοποίησης παιδιών). Η τρίτη κατηγορία περιλαμβάνει αξιόποινες πράξεις που μπορούν να διαπραχθούν μόνο μέσω ηλεκτρονικών δικτύων, π.χ. επιθέσεις κατά συστημάτων πληροφοριών, άρνηση παροχής υπηρεσιών (Denial of Service) και παράνομη επέμβαση σε σύστημα πληροφοριών (hacking)[7].

Επίσης, προς εκπλήρωση του επιδιωκόμενου σκοπού της προσέγγισης του ποινικού δικαίου των κρατών μελών στον τομέα των επιθέσεων κατά συστημάτων πληροφοριών, εκδόθηκε την 12η Αυγούστου 2013 η οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου αντικαταστώντας την 2005/222/ΔΕΥ απόφαση-πλαίσιο του Συμβουλίου και προέβλεψε ποινικές κυρώσεις για τη δημιουργία των «botnet» (δίκτυα προγραμμάτων ρομπότ), την πράξη δηλαδή της απόκτησης εξ αποστάσεως ελέγχου σε σημαντικό αριθμό υπολογιστών διά της μολύνσεως τους με κακόβουλο λογισμικό μέσω στοχευμένων επιθέσεων στον κυβερνοχώρο[8].

Β. ΜΟΡΦΕΣ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ

Οι βασικότερες και συχνότερα εμφανιζόμενες μορφές του κυβερνοεγλήματος είναι οι εξής:

1. Στη κατηγορία των επονομαζόμενων «γνήσιων ηλεκτρονικών εγκλημάτων», αυτών δηλαδή που εκδηλώθηκαν για πρώτη φορά μετά την εμφάνιση των ηλεκτρονικών υπολογιστών, υπάγονται:
    - Η παράνομη πρόσβαση σε υπολογιστικά συστήματα (hacking & cracking)

[7] Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Ευρωπαϊκή Επιτροπή των Περιφερειών με τίτλο : «Προς την κατεύθυνση γενικής πολιτικής σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο», Βρυξέλλες, 22.5.2007, SEC(2007) 641 & 642, διαθέσιμη εδώ : http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52007DC0267&qid=1488508403454&from=EL , σελίδα 2

[8] Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, L 218/8 Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης

- Οι επιθέσεις κατανεμημένης άρνησης παροχής υπηρεσιών (Distributed Denial of Service - DDoS)
- Η διασπορά κακόβουλου λογισμικού (όπως ιούς, σκουλήκια και δούρειους ίππους)
- Αποστολή μη ζητηθείσας-ανεπιθύμητης αλληλογραφίας (spamming)
- Phishing – Ηλεκτρονικό ψάρεμα (μέθοδος εξαπάτησης χρηστών)
- Πειρατεία λογισμικού
- Υποκλοπή αρχείων υπολογιστή

2. Στη κατηγορία των εγκλημάτων που προϋπήρχαν της εμφάνισης του ηλεκτρονικού υπολογιστή και διευκολύνονται - τελούνται με τη χρήση αυτού, υπάγονται:
    - Η απάτη μέσω του διαδικτύου
    - Η κατοχή και διαμοιρασμός υλικού σεξουαλικής εκμετάλλευσης ανηλίκων
    - Εγκλήματα σχετικά με τα δικαιώματα πνευματικής ιδιοκτησίας κλπ.

Γ. ΝΟΜΟΘΕΣΙΑ ΚΑΙ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ

Ένα από ζητήματα που προκύπτουν από τη ραγδαία ανάπτυξη των δικτύων υπολογιστών και γενικότερα της τεχνολογίας πληροφοριών και επικοινωνίας (ΤΠΕ), είναι η αδυναμία της νομοθεσίας να την προφτάσει. Για τη προσέγγιση των νομικών θεμάτων που αφορούν το έγκλημα στον κυβερνοχώρο απαιτούνται όχι μόνο νομικές αλλά και ειδικές τεχνικές γνώσεις όσων ασχολούνται με αυτό, όπως και η θεσμοθέτηση κατάλληλων τεχνικών όρων.

Το κυβερνοέγκλημα, σε αντίθεση με τις συμβατικές μορφές εγκληματικότητας, δεν περιορίζεται στην εδαφική αρμοδιότητα ενός μόνο κράτους, αλλά είναι εκ φύσεως διασυνοριακό και για τη καταπολέμησή του είναι απαραίτητη η ύπαρξη παγκοσμίως αποδεκτών νομικών κειμένων. Ωστόσο ο τρόπος που κάθε κράτος προσεγγίζει από νομικής πλευράς το διαδικτυακό έγκλημα και την απαιτούμενη διασυνοριακή συνεργασία και ανταλλαγή πληροφοριών είναι αποτέλεσμα ποικίλων παραγόντων και αντικατοπτρίζει τις εκάστοτε εθνικές προτεραιότητες.

Στο νομικό πλαίσιο της Ελλάδας, τα κυβερνοεγκλήματα τιμωρούνταν μέχρι πρόσφατα κατά βάση με τις διατάξεις του Ν. 1805/1988, με τον οποίο είχαν εισαχθεί

τα άρθρα 370Β, 370Γ, 386Α του Ποινικού Κώδικα σχετικά με τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές [computer crimes].

Η Σύμβαση του Συμβουλίου της Ευρώπης για το Έγκλημα στον Κυβερνοχώρο, το Πρόσθετο Πρωτόκολλο αυτής σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσεως, όπως επίσης και η Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών, ενσωματώθηκαν στο Ελληνικό Δίκαιο με τον Ν. 4411/2016 (ΦΕΚ 142/Α'/03-08-2016), με τον οποίο επιφέρονται τροποποιήσεις των άρθρων 13, 292Β, 292Γ, 348Β, 370Γ ως Ε, 381Α, 381Β και 386 του Ποινικού Κώδικα. Ειδικότερα :

- Στο άρθρο 13 του Ποινικού Κώδικα προστίθενται περιπτώσεις η΄ (Πληροφοριακό σύστημα) και θ΄ (Ψηφιακά δεδομένα)
- Προστίθεται το άρθρο 292Β «Παρακώλυση λειτουργίας πληροφοριακών συστημάτων»
- Προστίθεται το άρθρο 292Γ (σχετικά με τη παραγωγή, πώληση κλπ συσκευών και προγραμμάτων σχεδιασμένων για τη διάπραξη των εγκλημάτων που προβλέπονται από το άρθρο 292Β)
- Τροποποιούνται οι παράγραφοι 2 και 5 του άρθρου 348Α του Ποινικού Κώδικα
- Αντικαθίσταται το άρθρο 348Β «Προσέλκυση παιδιών για γενετήσιους λόγους»
- Αντικαθίσταται το άρθρο 370Γ «Παράνομη πρόσβαση σε πληροφοριακό σύστημα»
- Προστίθεται το άρθρο 370Δ (σχετικά με την αθέμιτη παρακολούθηση ή αποτύπωση σε υλικό φορέα μη δημόσιων διαβιβάσεων δεδομένων με τη χρήση τεχνικών μέσων)
- Προστίθεται το άρθρο 370Ε (σχετικά με την παράνομη παραγωγή, πώληση, προμήθεια, κατοχή, διακίνηση: α) συσκευών ή προγραμμάτων υπολογιστών με σκοπό τη διάπραξη κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ και 370Δ ή β) συνθηματικών ή κωδικών πρόσβασης με τα οποία είναι δυνατόν να αποκτηθεί πρόσβαση σε πληροφοριακό σύστημα)
- Προστίθεται το άρθρο 381Α «Φθορά ηλεκτρονικών δεδομένων»
- Προστίθεται το άρθρο 381Β (σχετικά με την παράνομη παραγωγή, πώληση, προμήθεια, κατοχή, διακίνηση: α) συσκευών ή προγραμμάτων υπολογιστών με

σκοπό τη διάπραξη κάποιου από τα εγκλήματα των άρθρων 381Α ή β) συνθηματικών ή κωδικών πρόσβασης με τα οποία είναι δυνατόν να αποκτηθεί πρόσβαση σε πληροφοριακό σύστημα)

- Αντικαθίσταται το άρθρο 386Α «Απάτη με υπολογιστή»
- και τροποποιήθηκε το άρθρο 4 του Ν. 2225/1994 σχετικά με τα αδικήματα εκείνα για τα οποία είναι επιτρεπτή η άρση του απορρήτου.

Δ. ΨΗΦΙΑΚΑ ΑΠΟΔΕΙΚΤΙΚΑ ΜΕΣΑ

Οι υπολογιστές χρησιμοποιούνται ολοένα και περισσότερο κατά τη διάπραξη εγκλημάτων και οι αρχές επιβολής του νόμου στη προσπάθειά τους να ανταποκριθούν στη νέα αυτή πρόκληση, εκμεταλλεύονται την ραγδαία εξέλιξη της επιστήμης της ψηφιακής εγκληματολογίας και χρησιμοποιούν ηλεκτρονικά μέσα για την καταπολέμηση του εγκλήματος. Ο νομοθέτης λοιπόν παρατηρώντας ότι τα αποδεικτικά στοιχεία για τη θεμελίωση της αντικειμενικής υπόστασης του εγκλήματος ή την ενοχή του δράστη έχουν αρκετά συχνά πλέον ψηφιακή μορφή, διεύρυνε την έννοια του εγγράφου (του άρθρου 13, παρ. γ, Π.Κ.) περιλαμβάνοντας σε αυτά και τα ηλεκτρονικά έγγραφα. Υπάρχουν ωστόσο αρκετές διαφορές μεταξύ των παραδοσιακών και των ψηφιακών αποδεικτικών μέσων και αυτό γιατί τα πρώτα έχουν υλική υπόσταση και μπορούν να εντοπιστούν σε συγκεκριμένο τόπο και χρόνο, ενώ αντίθετα τα δεύτερα είναι άυλα, τροποποιούνται εύκολα και απαιτείται ιδιαίτερη διαδικασία προκειμένου να εξασφαλισθούν και να αξιοποιηθούν στην ποινική διαδικασία.

Τα ψηφιακά πειστήρια είναι πληροφορίες που αποθηκεύονται ή μεταδίδονται σε ηλεκτρονική μορφή σε έναν σκληρό δίσκο του υπολογιστή, ένα κινητό τηλέφωνο, έναν οπτικό δίσκο (CD) και σε πολλές ακόμη μορφές και μπορούν να χρησιμοποιηθούν ενώπιον των δικαστικών αρχών. Τα ψηφιακά αποδεικτικά μέσα συνήθως συνδέονται με τα ηλεκτρονικά εγκλήματα ωστόσο δεν αποκλείεται να περιέχουν στοιχεία που βοηθούν στη δίωξη όλων των ειδών εγκλημάτων.

Στο πλαίσιο της προσπάθειας για την αποτελεσματική καταπολέμηση του ηλεκτρονικού εγκλήματος οι υπηρεσίες επιβολής του νόμου υιοθετούν κατά τη δράση τους τις αρχές της επιστήμης της ψηφιακής εγκληματολογίας σχετικά με τη συλλογή και ανάλυση των ψηφιακών πειστηρίων[9]. Στην Ελλάδα η πλέον εξειδικευμένη

[9] Διαδικτυακός τόπος National Institute of Justice (U.S.A.), http://www.nij.gov/topics/forensics/evidence/digital/pages/welcome.aspx

υπηρεσία για τον ανωτέρω σκοπό είναι το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών του Αρχηγείου της Ελληνικής Αστυνομίας[10].

Ε. ΨΗΦΙΑΚΑ ΑΠΟΔΕΙΚΤΙΚΑ ΜΕΣΑ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ

Μια ειδικότερη κατηγορία των ψηφιακών πειστήριων, η οποία θα αποτελέσει το κύριο αντικείμενο της παρούσης εργασίας, αποτελούν εκείνα τα αποδεικτικά μέσα που εντοπίζονται, όχι στα συνηθισμένα ηλεκτρονικά μέσα αποθήκευσης, αλλά σε περιβάλλον υπολογιστικού νέφους. Στα κεφάλαια που ακολουθούν θα παρουσιαστούν οι βασικές αρχές της εγκληματολογικής ανάλυσης ψηφιακών πειστηρίων, η έννοια του υπολογιστικού νέφους και οι τεχνικές και νομικές προκλήσεις που προκύπτουν κατά τη συλλογή και ανάλυση αποδεικτικών μέσων στο περιβάλλον αυτό.

[10] Άρθρο 30 του Π.Δ. 178/2014 «Οργάνωση Υπηρεσιών Ελληνικής Αστυνομίας»

ΚΕΦΑΛΑΙΟ 2ο: ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΑ ΑΠΟΔΕΙΚΤΙΚΑ ΜΕΣΑ

Όπως προκύπτει από τα ανωτέρω εκτεθέντα στο 1ο κεφάλαιο, η ανάγκη της εγκληματολογικής ανάλυσης των ψηφιακών πειστηρίων διευρύνεται παράλληλα με την αυξανόμενη τάση του ηλεκτρονικού εγκλήματος. Ένα πολύτιμο εργαλείο για τη διερεύνηση των κυβερνοεγκλημάτων είναι η επιστήμη της ψηφιακής εγκληματολογίας (Digital Forensics). Παρακάτω θα παρουσιάσουμε ορισμένες βασικές έννοιες και αρχές που την διέπουν.

Α. ΨΗΦΙΑΚΑ ΠΕΙΣΤΗΡΙΑ

Έχουν διατυπωθεί αρκετοί ορισμοί της έννοιας των ψηφιακών πειστηρίων. Σύμφωνα με μια εξ' αυτών τα ψηφιακά πειστήρια ορίζονται ως οποιαδήποτε δεδομένα αποθηκεύονται ή μεταδίδονται με τη χρήση ηλεκτρονικού υπολογιστή και μπορούν να στηρίξουν ή να αντικρούσουν μια θεωρία για τον τρόπο με τον οποίο συνέβη ένα αδίκημα ή να αποκαλύψουν κρίσιμα στοιχεία για αυτό, όπως η πρόθεση ή το άλλοθι[11]. Ο ορισμός που προτείνεται από την Επιστημονική Ομάδα Εργασίας για τα Ψηφιακά Πειστήρια (SWGDE) είναι ότι ψηφιακό πειστήριο αποτελεί κάθε πληροφορία με αποδεικτική ισχύ που είτε είναι αποθηκευμένη ή μεταδίδεται σε ψηφιακή μορφή[12]. Σύμφωνα με τη Σύμβαση για τα εγκλήματα στον Κυβερνοχώρο (Σύμβαση της Βουδαπέστης) αυτά περιγράφονται ως πειστήρια ενός εγκλήματος που συλλέγονται σε ηλεκτρονική μορφή.

Τα ψηφιακά πειστήρια μπορούν να εντοπιστούν σε διάφορες τοποθεσίες:

• Τοπικά, σε μια συσκευή τελικού χρήστη – όπως ο υπολογιστής ενός χρήστη, κινητό / έξυπνο τηλέφωνο, σύστημα δορυφορικής πλοήγησης, μονάδα USB ή ψηφιακή φωτογραφική μηχανή.

---

[11] W. J. Chisum, Crime Reconstruction and Evidence Dynamics στο The Forensic Laboratory Handbook Procedures and Practice , Humana Press, 2011, σελ. 105-122

[12] Scientific Working Group on Digital Evidence (SWGDE) & International Organization on Digital Evidence (IOCE), Digital evidence: standard and principles, 2000, διαθέσιμο εδώ : https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm

• Σε έναν απομακρυσμένο πόρο που είναι δημόσια προσβάσιμος - για παράδειγμα ιστοσελίδες που χρησιμοποιούνται για κοινωνική δικτύωση, φόρουμ συζητήσεων κλπ.

• Σε ένα απομακρυσμένο πόρο που είναι ιδιωτικός – όπως τα αρχεία καταγραφής δραστηριότητας των χρηστών του διαδικτύου μιας εταιρείας παροχής υπηρεσιών Internet, αρχεία χρέωσης των πελατών μιας εταιρείας κινητής τηλεφωνίας και στην ολοένα και περισσότερο διαδεδομένη απομακρυσμένη αποθήκευση αρχείων ενός χρήστη μέσω του υπολογιστικού νέφους.

• Σε μεταφορά – όπως για παράδειγμα τα μηνύματα κειμένου μέσω κινητού τηλέφωνου, οι φωνητικές κλήσεις, μηνύματα ηλεκτρονικού ταχυδρομείου κλπ.

Ένα βασικό χαρακτηριστικό των ψηφιακών πειστηρίων είναι ότι τροποποιούνται ιδιαίτερα εύκολα, είτε από λανθασμένη διαχείριση και προσπέλασή τους από τον εκάστοτε ερευνητή τους, είτε με διάφορα εργαλεία και μεθόδους ακόμη και απομακρυσμένα από τον ερευνόμενο. Συνεπώς, η αναζήτηση και συλλογή αυτών θα πρέπει να γίνεται με ιδιαίτερη προσοχή και ακολουθώντας μια ορισμένη διαδικασία.

Β. ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ

Η Ψηφιακή Εγκληματολογία (Digital Forensics), έχει ορισθεί ως η χρήση επιστημονικών και αποδεδειγμένων μεθόδων προς τη διατήρηση, συλλογή, επικύρωση, αναγνώριση, ανάλυση, ερμηνεία, τεκμηρίωση και παρουσίαση των ψηφιακών αποδεικτικών στοιχείων με σκοπό την διευκόλυνση ή προώθηση του επανασχηματισμού των συμβάντων που βρέθηκαν να είναι ποινικώς κολάσιμα ή την πρόβλεψη μη εξουσιοδοτημένων ενεργειών που δείχνουν να διαταράσσουν προγραμματισμένες λειτουργίες[13]. Η πρόκληση που προκύπτει κατά την ανωτέρω διαδικασία είναι ο αποκλεισμός κάθε πιθανότητας αλλοίωσης των ψηφιακών αποδεικτικών μέσων κατά την διαδικασία συλλογής και επεξεργασίας τους έτσι ώστε η έκθεση πραγματογνωμοσύνης – συμπεράσματα των αρμόδιων προς τούτο οργάνων να αποτελεί ακλόνητο στοιχείο στην αποδεικτική διαδικασία, χωρίς περιθώριο αμφισβήτησης και διφορούμενων ερμηνειών.

[13]A Road Map for Digital Forensics στο Digital Forensics Research Conference, 2001, διαθέσιμο εδώ: http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf, σελ. 16

Την γενική αυτή ανάγκη ευθυγράμμισης των διαδικασιών και βελτίωσης της ποιότητας των ψηφιακών εγκληματολογικών υπηρεσιών που παρέχονται από τις αρχές επιβολής του νόμου και τις δικαστικές αρχές υπογραμμίζει και το Συμβούλιο της Ευρωπαϊκής Ένωσης στο «Σχέδιο δράσης για τα απόμενα βήματα με στόχο τη δημιουργία Ευρωπαϊκού εγκληματολογικού χώρου» όπου προβλέπεται η κατάρτιση και χρήση εγχειριδίων βέλτιστων πρακτικών για τις εγκληματολογικές αναλύσεις[14]. Με τον τρόπο αυτό προβλέπονται κανόνες σχετικά με τις ψηφιακές εγκληματολογικές διαδικασίες που πρέπει να ακολουθούνται κατά τον εντοπισμό, συλλογή, απόκτηση, απεικόνιση, ανάλυση και διαφύλαξη των ψηφιακών πειστηρίων. Ο σκοπός αυτών των βέλτιστων πρακτικών είναι να διασφαλίζεται η ακεραιότητα των πειστηρίων και η αλυσίδα των αποδείξεων να είναι παραδεκτή κατά τις διοικητικές, πειθαρχικές και δικαστικές διαδικασίες. Έτσι λοιπόν, προς εκπλήρωση της ανάγκης για τυποποίηση, διάφορα όργανα και οργανισμοί έχουν δημοσιεύσει τέτοιες κατευθυντήριες γραμμές σχετικά με τις ακολουθητέες διαδικασίες κατά την εγκληματολογική ανάλυση ψηφιακών πειστηρίων. Ενδεικτικά αναφέρεται ο οδηγός : «Βέλτιστες πρακτικές για την ψηφιακή Εγκληματολογία» που εκδόθηκε αρχικά το 2004 από την επιστημονική ομάδα εργασίας για τα Ψηφιακά Δεδομένα (SWGDE)[15].

Πρόσφατα η Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF) της Ευρωπαϊκής Επιτροπής δημοσίευσε έναν οδηγό με κατευθυντήριες γραμμές σχετικά με την διαδικασία εγκληματολογικής ανάλυσης ψηφιακών πειστηρίων[16]. Αυτές οι κατευθυντήριες γραμμές λαμβάνουν υπ’ όψιν διεθνώς εγκεκριμένα πρότυπα και καλές πρακτικές, όπως το πρότυπο ISO 27037 (Κατευθυντήριες γραμμές για την αναγνώριση, συλλογή, απόκτηση και διατήρηση των ψηφιακών αποδεικτικών στοιχείων) που καταρτίσθηκε το 2012[17], και τον "οδηγό ορθής πρακτικής για τις

[14]Υπ’ αρίθμ. 8770/16 σχέδιο συμπερασμάτων του Συμβουλίου της Ευρωπαϊκής Ένωσης και σχέδιο δράσης για τα επόμενα βήματα με στόχο τη δημιουργία Ευρωπαϊκού Εγκληματολογικού Χώρου, 24 Μαΐου 2016, διαθέσιμο εδώ : http://data.consilium.europa.eu/doc/document/ST-8770-2016-INIT/el/pdf

[15]Best Practices for Computer Forensics, Scientific Working Group on Digital Evidence, 2014, Διαθέσιμο εδώ: https://swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensics

[16] Ευρωπαϊκή Επιτροπή, Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF), Guidelines on Digital Forensic Procedures for OLAF Staff, 15 Φεβρουαρίου 2016, διαθέσιμο εδώ : https://ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf

[17] Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence, International Organization for Standardization, ISO/IEC 27037:2012, διαθέσιμο εδώ : https://www.iso.org/standard/44381.html

ψηφιακές αποδείξεις» που δημοσιεύθηκε από την Ένωση Ανωτάτων Αξιωματικών της Αστυνομίας του Ηνωμένου Βασίλειου (APCO) τον Μάρτιο του 2012[18].

Γ. ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΕΞΕΤΑΣΗΣ ΨΗΦΙΑΚΩΝ ΠΕΙΣΤΗΡΙΩΝ

Τα ψηφιακά πειστήρια υπόκειται στους ίδιους κανόνες και νόμους που ισχύουν και για τα υπόλοιπα ΄΄παραδοσιακά΄΄ αποδεικτικά στοιχεία προκειμένου αυτά να γίνονται αποδεκτά σε μια νομική διαδικασία. Οι αρχές επιβολής του νόμου θα πρέπει να είναι σε θέση να αποδεικνύουν ενώπιον των Δικαστικών Αρχών ότι τα στοιχεία που τους προσκόμισαν δεν είναι τίποτα περισσότερο και τίποτα λιγότερο από αυτά που αρχικώς βρέθηκαν στην ΄΄σκηνή του εγκλήματος΄΄. Είναι λοιπόν απαραίτητο να παρουσιάζονται με αντικειμενικότητα και ακεραιότητα, παρουσιάζοντας παράλληλα τον τρόπο με τον οποίο τα στοιχεία αυτά ανακτήθηκαν. Επιπλέον, τα αποδεικτικά μέσα πρέπει να διατηρούνται αναλλοίωτα ούτως ώστε να είναι δυνατόν να επαναληφθεί η ίδια διαδικασία και να οδηγήσει στο ίδιο αποτέλεσμα όπως αυτό που παρουσιάστηκε στο δικαστήριο.

Ειδικότερα, προκειμένου τα ψηφιακά πειστήρια να μην επιδέχονται αμφισβήτηση, θα πρέπει σύμφωνα και με τον οδηγό Good Practice Guide for Computer-Based Electronic Evidence της Association of Chief Police Officers (ACPO) τα αρμόδια όργανα που είναι επιφορτισμένα με τη συλλογή και ανάλυση τους να ακολουθούν τις εξής βασικές αρχές:

- Αρχή 1: Κανένα μέτρο που λαμβάνεται από τις υπηρεσίες επιβολής του νόμου δεν θα πρέπει να αλλάζει τα δεδομένα.
- Αρχή 2: Στην περίπτωση όπου ένα άτομο θεωρηθεί ότι είναι απαραίτητο να προσπελάσει τα δεδομένα, το πρόσωπο αυτό θα πρέπει να είναι το αρμόδιο για να το κάνει και να είναι σε θέση να εξηγήσει την αναγκαιότητα και τα αποτελέσματα των ενεργειών του.
- Αρχή 3: Θα πρέπει να καταγράφονται πλήρως και να διατηρούνται όλες οι διεργασίες στις οποίες υπόκεινται τα ψηφιακά πειστήρια. Όταν κάποιος τρίτος το

[18] Good Practice Guide for Digital Evidence, Association of Chief Police Officers, 2012, διαθέσιμο εδώ : http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf, σελ. 4

θελήσει, θα πρέπει να μπορεί να είναι σε θέση να επαναλάβει τις ίδιες ακριβώς διαδικασίες και να λάβει τα ίδια ακριβώς αποτελέσματα.

- Αρχή 4: Το άτομο που είναι υπεύθυνο για την έρευνα έχει την ευθύνη να διασφαλίσει την τήρηση των παραπάνω Αρχών όπως και της νομιμότητας των διαδικασιών[19].

Δ. ΜΕΘΟΔΟΛΟΓΙΑ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗΣ ΑΝΑΛΥΣΗΣ

Έχουν γίνει αρκετές προσπάθειες για την ανάπτυξη ενός μοντέλου εγκληματολογικής ανάλυσης ψηφιακών πειστηρίων, ωστόσο, μέχρι στιγμής κανένα από αυτά δεν έχει κοινά αποδεκτό. Ένας από τους κυριότερους λόγους της έλλειψης ενός τέτοιου παγκοσμίως αποδεκτού μοντέλου είναι ότι πολλά από τα από τα έως τώρα διατυπωμένα έχουν σχεδιαστεί για την εφαρμογή τους σε συγκεκριμένα περιβάλλοντα, όπως π.χ. από τις Αρχές Επιβολής του Νόμου, και δεν αρμόζουν σε διαφορετικές κατηγορίες, όπως αυτή της αντιμετώπισης περιστατικών (Incident Response)[20]. Ένα τέτοιο μοντέλο ψηφιακής έρευνας πρέπει να βασίζεται σε ένα συνεπές και τυποποιημένο πλαίσιο που υποστηρίζει κάθε στάδιο της έρευνας (τεχνικό ή μη) και δεν εξαρτάται από το είδος του εγκλήματος.

Μια λιγότερο τεχνική προσέγγιση της μεθοδολογίας εγκληματολογικής ανάλυσης ψηφιακών πειστηρίων, που εξυπηρετεί τους σκοπούς των Αρχών Επιβολής του Νομού, αποτελείται από τέσσερα βασικά στάδια : τη συλλογή, εξέταση και ανάλυση των πειστηρίων και την παρουσίαση των ευρημάτων[21].

1. Συλλογή ψηφιακών πειστηρίων

Η φάση συλλογής περιλαμβάνει την αναζήτηση, αναγνώριση, συλλογή και καταγραφή των όλων των ηλεκτρονικών αποδεικτικών στοιχείων που σχετίζονται άμεσα ή έμμεσα με το διαπραχθέν έγκλημα. Τα ψηφιακά πειστήρια, όπως και όλα τα άλλα αποδεικτικά στοιχεία, πρέπει να

[19] Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Academic Press, 2011, σελ. 232

[20] Παρουσίαση των περισσότερο διαδεδομένων μοντέλων στο άρθρο του Jawad Abbas, Studying the Documentation Process in Digital Forensic Investigation Frameworks / Models, Journal of Al-Nahrain University, December 2015, διαθέσιμο εδώ: http://www.iasj.net/iasj?func=fulltext&aId=107014, σελ. 153-162

[21] Electronic Crime Scene Investigation: A Guide for First Responders, U.S. Department of Justice Office of Justice Programs National Institute of Justice, July 2001, διαθέσιμο εδώ : https://www.ncjrs.gov/pdffiles1/nij/219941.pdf , σελ. 2-3

αντιμετωπίζονται με ιδιαίτερη προσοχή και με τρόπο που να διατηρεί την αποδεικτική τους αξία. Αυτό αφορά όχι μόνο τη φυσική ακεραιότητα ενός αντικειμένου ή μιας συσκευής, αλλά και τα ηλεκτρονικά δεδομένα που περιέχει. Ορισμένοι τύποι ψηφιακών πειστηρίων απαιτούν ειδική συλλογή, συσκευασία και μεταφορά. Θα πρέπει να υπάρχει μέριμνα για τη προστασία των δεδομένων αυτών που μπορεί να είναι επιρρεπή σε βλάβη ή αλλοίωση από ηλεκτρομαγνητικά πεδία (π.χ. στατικό ηλεκτρισμό, μαγνήτες, ραδιοπομπούς, κλπ). Η φάση αυτή μπορεί να περιλαμβάνει και τη συλλογή σε πραγματικό χρόνο αποθηκευμένων πληροφοριών που ενδέχεται να χαθούν, αν δεν ληφθούν τα κατάλληλα μέτρα για τη διασφάλιση των εύθραυστων δεδομένων και τρεχουσών διαδικασιών.

2. Εξέταση ψηφιακών πειστηρίων

Η διαδικασία της εξέτασης βοηθά στο να γίνουν ορατά τα αποδεικτικά στοιχεία και εξηγεί την προέλευση και τη σημασία τους. Κατά την διαδικασία αυτή θα πρέπει να τεκμηριώνεται το περιεχόμενο και η κατάσταση των στοιχείων στο σύνολό τους επιτρέποντας σε όλα τα μέρη να επεξεργαστούν τα αποδεικτικά στοιχεία. Η εξέταση περιλαμβάνει και την αναζήτηση για πληροφορίες που ενδέχεται να είναι κρυφές ή να έχουν κρυπτογραφηθεί.

Κατά την εξέταση των ψηφιακών αποδεικτικών μέσων ισχύουν οι γενικές αρχές της εγκληματολογικής επιστήμης, ωστόσο τα διαφορετικά είδη των περιπτώσεων και ψηφιακών ευρημάτων μπορεί να απαιτούν διαφορετικές μεθόδους εξέτασης. Τα πρόσωπα που είναι επιφορτισμένα με τη εξέταση των ψηφιακών πειστηρίων θα πρέπει να έχουν λάβει σχετική εκπαίδευση.

Η διαδικασία της εξέτασης δεν θα πρέπει να λαμβάνει χώρα, όποτε αυτό είναι δυνατόν, επί των πρωτότυπων-αρχικών πειστηρίων προς αποφυγή αλλοίωσης δεδομένων. Έτσι λοιπόν, πριν από οποιαδήποτε άλλη διεργασία, θα πρέπει να πραγματοποιείται ¨εξαγωγή¨ των δεδομένων από τα κατασχεθέντα ψηφιακά αποδεικτικά μέσα. Το ακριβές ψηφιακό αντίγραφο παράγεται με ειδικό προς τούτο εξοπλισμό που εμποδίζει την επέμβαση επί του αρχικού υλικού, το οποίο εν συνεχεία αποθηκεύεται κατάλληλα. Η εξέταση λαμβάνει χώρα επί του αντιγράφου που δημιουργήθηκε και επαληθεύθηκε με ειδική διαδικασία (MD5 Hash Value) για να εξασφαλιστεί ότι τα αποδεικτικά στοιχεία είναι ακόμα στην αρχική τους κατάσταση.

Έτσι, αν προκύψει οποιαδήποτε επιπλοκή κατά τη διάρκεια της ανάλυσης και καταστραφεί το ψηφιακό αντίγραφο, υπάρχει πάντα η δυνατότητα να δημιουργηθεί καινούριο και να συνεχιστεί η εξέταση.

Όταν πλέον όλες οι πληροφορίες είναι ορατές, η διαδικασία της μείωσης των προς ανάλυση δεδομένων μπορεί να ξεκινήσει διαχωρίζοντας τις πληροφορίες εκείνες που πιθανόν σχετίζονται με το διαπραχθέν έγκλημα από εκείνες που δεν ενδιαφέρουν την ανακριτική διαδικασία δεδομένης της τεράστιας ποσότητας των πληροφοριών που μπορεί να είναι αποθηκευμένες στα μέσα αποθήκευσης ενός υπολογιστή[22] [23].

3. Ανάλυση ψηφιακών πειστηρίων

Η ανάλυση είναι ίσως το σημαντικότερο στάδιο της έρευνας καθώς εξετάζονται τα στοιχεία που είχαν εξαχθεί κατά την προηγούμενη φάση προκειμένου να προσδιοριστούν ποιες από το σύνολο των συλλεχθέντων πληροφοριών αποτελούν αποδεικτικά στοιχεία. Η ανάλυση διαφέρει από την εξέταση στο ότι παραλαμβάνει το προϊόν της εξέτασης και το επεξεργάζεται προκειμένου να εντοπίσει εκείνα τα στοιχεία που έχουν αυξημένη σημασία και αποδεικτική ισχύ για την υπόθεση. Σε αυτή περιλαμβάνεται η εξέταση της σημασίας και της ισχύος των δεδομένων και η ερμηνεία αυτών προκειμένου να ανακατασκευαστεί η σκηνή του εγκλήματος και να δημιουργηθεί ένα χρονοδιάγραμμα που περιγράφει το ιστορικό του εγκλήματος.

Για κάθε υπό έρευνα στοιχείο, τα αρμόδια προς τούτο όργανα, διερευνούν και προσπαθούν να προσδιορίσουν το πότε και από ποιόν δημιουργήθηκε, προσπελάστηκε, τροποποιήθηκε, διαγράφηκε και παρατηρώντας την ακολουθία των συμβάντων επιχειρούν να τα συσχετίσουν και να οδηγηθούν σε ορισμένα συμπεράσματα. Μπορεί να χρειαστούν αρκετές επαναλήψεις της διαδικασίας ανάλυσης για να υποστηριχθεί τελικά μια θεωρία για το διαπραχθέν έγκλημα.

[22] Shahid Jamal Tubrazy, The Discovery of Digital Evidence and Forensic Laws (Theories and Practices), 2015, S J Tubrazy Publication, σελ. 51
[23] Richard S. Michelson, Crime Scene Investigation: An Introduction to CSI, LawTech Publishing Group, 2015, Κεφάλαιο 22

Η ανάλυση των ψηφιακών πειστηρίων έχει εξελιχθεί σε μια προηγμένη μεθοδολογία για την υποβοήθηση της οποίας αναπτύσσονται συνεχώς και ισχυρότερα και αποτελεσματικότερα ψηφιακά δικανικά εργαλεία[24].

4. Παρουσίαση των ευρημάτων

Το εξειδικευμένο και αρμόδιο για την έρευνα όργανο, θα πρέπει να παρουσιάσει τα ευρήματά του σε μια σαφή αναφορά όπου θα παραθέτει και θα επεξηγεί τα συμπεράσματα στα οποία έχει καταλήξει. Μια τέτοια έκθεση πρέπει να είναι γραμμένη με κατάλληλο τρόπο ώστε να γίνεται κατανοητή από κοινό χωρίς τεχνικές γνώσεις (όπως π.χ. δικαστές, νομικοί κλπ) και οι ψηφιακές αποδείξεις να παρουσιάζονται με τρόπο σαφή και ακριβή ώστε να προσδιορίζεται με σαφήνεια ο ρόλος και η σημασία των πραγματικών στοιχείων στην έρευνα. Τα στοιχεία που παρουσιάζονται στην έκθεση θα πρέπει να εξακριβώνεται πως είναι αυθεντικά, αξιόπιστα και παραδεκτά και θα πρέπει να επεξηγούνται λεπτομερώς ούτως ώστε ένα ανεξάρτητο τρίτο μέρος να είναι σε θέση να αναπαράγει τα συμπεράσματα. Στην έκθεση θα πρέπει επίσης να δηλώνονται επακριβώς τα εργαλεία που χρησιμοποιήθηκαν στην έρευνα ώστε να είναι ευκολότερη η κατανόηση του τρόπου εξαγωγής των συμπερασμάτων[25].

Ε. ΤΟ ΠΑΡΑΔΕΚΤΟ ΤΩΝ ΨΗΦΙΑΚΩΝ ΠΕΙΣΤΗΡΙΩΝ

Ο βασικός στόχος της εγκληματολογικής ανάλυσης ψηφιακών πειστηρίων είναι η διασφάλιση ότι το τελικό αποτέλεσμα/συμπέρασμα δεν έχει χάσει την αποδεικτική ισχύ του και, ως εκ τούτου, είναι παραδεκτό ως αποδεικτικό στοιχείο. Τα ψηφιακά δεδομένα είναι πολύ ευαίσθητα στην αλλαγή ή διαγραφή. Είτε πρόκειται για μια εσκεμμένη μεταβολή, είτε για μια ακούσια αλλαγή που προέρχεται από αστοχία του συστήματος ή ανθρώπινο λάθος, η δομή των δεδομένων αυτών είναι ιδιαιτέρως ευμετάβλητη. Συνεπώς πώς είναι σε θέση το δικαστήριο ή ένας δικηγόρος

[24] Guide to Integrating Forensic Techniques into Incident Response: του National Institute of Standards and Technology (NIST), 2006, διαθέσιμο εδώ : http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf , παρ. 3.6 και 4.14

[25] Electronic evidence - a basic guide for First Responders, European Union Agency for Network and Information Security (ENISA), 2015, διαθέσιμο εδώ: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders, σελ. 14

να εξακριβώσει εάν τα ψηφιακά πειστήρια που παρουσιάζονται τελικώς σε αυτούς είναι ανεπηρέαστα και συνεπώς παραδεκτά; Δεδομένου του γεγονότος ότι η διαδικασία της εγκληματολογικής ανάλυσης ψηφιακών πειστηρίων περιλαμβάνει πολλές μεταβλητές, είναι δύσκολο να υιοθετηθεί ένα περιοριστικό μοντέλο που θα εφαρμοζόταν σε κάθε περίσταση. Η λύση είναι να εφαρμόζονται όσο το δυνατόν περισσότερα κριτήρια και ακολουθείται κατά γράμμα μια αλληλουχία βημάτων κατά την έρευνα (chain of custody) που θα καθορίζουν αν το αποτέλεσμα της ανωτέρω διαδικασίας είναι αξιόπιστο, ακριβές και κατάλληλο ώστε να παρουσιαστεί ενώπιον μιας δικαστικής αίθουσας[26].

ΣΤ. ΤΜΗΜΑ ΕΞΕΤΑΣΗΣ ΨΗΦΙΑΚΩΝ ΠΕΙΣΤΗΡΙΩΝ / Δ.Ε.Ε.

Στην Ελλάδα αρμόδια Υπηρεσία για την εξέταση ψηφιακών πειστηρίων τυγχάνει η Διεύθυνση Εγκληματολογικών Ερευνών του Αρχηγείου της Ελληνικής Αστυνομίας και συγκεκριμένα το **Τμήμα Εξέτασης Ψηφιακών Πειστηρίων**.

Σύμφωνα με το άρθρο 30, παρ. 22 του Π.Δ. 178/2014, το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων είναι αρμόδιο για να εξετάζει ή αναλύει ψηφιακά, ηλεκτρονικά ή ακουστικά μέσα και τα δεδομένα που περιέχονται σ' αυτά, τα οποία περισυλλέγονται από τον τόπο του εγκλήματος από το Τμήμα Εξερευνήσεων της Δ.Ε.Ε., ή αποστέλλονται με σχετική παραγγελία από ανακριτική, εισαγγελική ή δικαστική αρχή, υπό την προϋπόθεση ότι πρόκειται για μέσα που επιδέχονται εργαστηριακές εξετάσεις και μπορούν να συμβάλουν στην εξιχνίαση εγκληματικής πράξης.

Το Τμήμα διαθέτει Εργαστήριο Εξέτασης Πειστηρίων Υπολογιστικών Συστημάτων, το οποίο είναι αρμόδιο πρώτα απ' όλα να ενεργεί ανάγνωση, ανάκτηση – επαναφορά, εξέταση, αποκρυπτογράφηση, ανάλυση, σύγκριση, επεξεργασία, καταγραφή δεδομένων, ευρισκομένων σε αποθηκευτικούς ψηφιακούς χώρους τοπικών δικτύων ηλεκτρονικών υπολογιστών και περιφερειακών ή άλλων ειδικών σταθερών ή φορητών μέσων ψηφιακής αποθήκευσης δεδομένων *(εδ. α αα)*.

Επιπλέον, αποφαίνεται για τον τρόπο λειτουργίας λογισμικού ή ψηφιακού υλικού, διαπιστώνει την αλληλουχία των ενεργειών χρήσης λογισμικού ή υλικού και

[26] Rodney McKemmish, Advances in Digital Forensics IV, Chapter 1 - When is Digital Evidence Forensically Sound?, εκδ. Springer US, 2008, σελ. 1-13

ενεργεί εξετάσεις για την εξακρίβωση του δημιουργού ή του χρήστη εφαρμογών ή δεδομένων επί ψηφιακών πειστηρίων, που είναι πρόσφορα προς ανάγνωση *(εδ. α ββ)*.

Πέρα από τους υπολογιστές, στο Εργαστήριο διενεργούνται εξετάσεις επί ηλεκτρονικών συσκευών ή άλλων ειδικών ηλεκτρονικών διατάξεων, οι οποίες είναι δυνατόν να αποθηκεύουν ψηφιακά δεδομένα, επί κινητών τηλεφώνων και συσκευών εντοπισμού θέσης, αλλά και εξειδικευμένες εξετάσεις, αναγνώσεις, ανακτήσεις και αναλύσεις ψηφιακών δεδομένων επί τραπεζικών ή άλλων καρτών *(εδ. α γγ, δδ, εε)*.

Ακόμα, εφόσον η εξέταση δεν είναι δυνατόν να διενεργηθεί στο Εργαστήριο Διερεύνησης Παραχάραξης – Κιβδηλείας και Πλαστότητας Εντύπων και Αξιών του Τμήματος Εργαστηρίων Δικαστικής Γραφολογίας και Πλαστότητας Εντύπων και Αξιών της Δ.Ε.Ε., διενεργεί εξετάσεις επί συναφών ειδικών ηλεκτρονικών μέσων (ηλεκτρονικών διαβατηρίων) *(εδ. α εε)*.

Τέλος, το Εργαστήριο ενεργεί εξετάσεις σε συστήματα τηλεπικοινωνιών, σε συσκευές λήψης δορυφορικού τηλεοπτικού ή άλλου σήματος τα οποία περιέχουν ψηφιακά δεδομένα πρόσφορα προς ανάγνωση *(εδ. α στστ)*.

Παράλληλα, συνεργάζεται με τις επιληφθείσες Υπηρεσίες για τη διασφάλιση της κατάσχεσης, ορθής διαχείρισης και ταχύτερης αποστολής των προς εξέταση πειστηρίων, παρέχοντας σε αυτές οδηγίες ασφαλούς μεταφοράς και φύλαξης, ενώ σε εξαιρετικά κρίσιμες περιπτώσεις παρέχει τεχνική συνδρομή στην κατάσχεση, δια της αποστολής εξειδικευμένου κλιμακίου *(εδ. α ζζ)*.

Οι υπηρετούντες στο Τμήμα Εξέτασης Ψηφιακών Πειστηρίων[27] συντάσσουν εκθέσεις πραγματογνωμοσύνης για κάθε εργαστηριακή εξέταση, προς χρήση από τις κατά νόμο αρμόδιες Αρχές[28].

Στην περίπτωση που από τις εκάστοτε Αστυνομικές Υπηρεσίες τίθενται στο Τμήμα Εξέτασης Ψηφιακών Πειστηρίων ερωτήματα που αφορούν και στην εξέταση στοιχείων επικοινωνίας, όπως το περιεχόμενο αρχείων ή άλλων στοιχείων που περιλαμβάνονται σε ηλεκτρονική αλληλογραφία (emails), ή ηλεκτρονική συνομιλία (chat), καθώς και το περιεχόμενο γραπτών μηνυμάτων (SMS) από κινητά τηλέφωνα κ.λπ. που περιέχονται στα ψηφιακά πειστήρια, απαιτείται η έκδοση Βουλεύματος

[27] Εφόσον τους έχει απονεμηθεί σχετική ειδικότητα, σύμφωνα με το άρθρο 111 του Π.Δ. 342/1977
[28] Παράγραφος 23 άρθρου 30 Π.Δ. 178/2014, ΦΕΚ 281 - 31.12.2014, Οργάνωση Υπηρεσιών Ελληνικής Αστυνομίας

από το αρμόδιο δικαστικό συμβούλιο, με το οποίο να διατάσσεται η «άρση του απορρήτου των επικοινωνιών» και να διατάσσεται ειδικά το Εργαστήριο Εξέτασης Πειστηρίων Υπολογιστικών Συστημάτων της Δ.Ε.Ε. να πραγματοποιήσει εξετάσεις επί αυτών[29]. Στην περίπτωση που δεν αποσταλεί στη Δ.Ε.Ε. σχετικό Βούλευμα περί «άρσης του απορρήτου των στοιχείων επικοινωνίας», οι εξετάσεις περιορίζονται στα στοιχεία εκείνα για τα οποία αυτό δεν απαιτείται γενόμενης σχετικής μνείας στην συνταχθείσα έκθεση.

Ζ. ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΑΝΑΛΥΣΗ ΨΗΦΙΑΚΩΝ ΠΕΙΣΤΗΡΙΩΝ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ

Στο παρόν κεφάλαιο παρατέθηκαν οι διαδικασίες και οι δυσχέρειες που προκύπτουν κατά την εγκληματολογική εξέταση των ψηφιακών πειστηρίων τα οποία εμπεριέχονται σε συσκευές με υλική διάσταση που προσφέρονται προς κατάσχεση και εξέταση όπως π.χ. ένας σκληρός δίσκος. Οι δυσκολίες κατά την εν λόγω διαδικασία εντείνονται ακόμη περισσότερο λόγω της εμφάνισης την έννοιας του υπολογιστικού νέφους και ανακύπτουν νέες τεχνικές και νομικές προκλήσεις.

[29] Σύμφωνα με τους Ν. 2225/1994, ΦΕΚ 121 – 20/07/1994, «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις» και Π.Δ. 47/2005, ΦΕΚ 64 – 10/03/2005 «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του», όπως τροποποιήθηκαν και ισχύουν

ΚΕΦΑΛΑΙΟ 3ο: ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ

Το υπολογιστικό νέφος (cloud computing) αποτελεί μια σημαντική καινοτομία σχετικά με τον τρόπο με τον οποίο διαχειρίζονται πλέον οι διαθέσιμοι υπολογιστικοί πόροι, καθώς μας παρέχει τη δυνατότητα της προσπέλασης, επεξεργασίας και αποθήκευσης δεδομένων (όπως κείμενα, αρχεία, εικόνες και βίντεο) και λογισμικού απομακρυσμένα από οποιαδήποτε γεωγραφικό σημείο και συσκευή, μέσω του Διαδικτύου και χωρίς να είναι απαραίτητο να φέρουμε μαζί μας το υλικό μέσο αποθήκευσης των δεδομένων μας. Συνεχώς και μεγαλύτερος αριθμός ανθρώπων χρησιμοποιεί το υπολογιστικό νέφος δίχως καν να το γνωρίζει καθώς υπηρεσίες και εφαρμογές που χρησιμοποιούμε καθημερινά, όπως το διαδικτυακό ηλεκτρονικό ταχυδρομείο ή τα κοινωνικά δίκτυα, βασίζονται στην τεχνολογία του υπολογιστικού νέφους. Η ευρεία διάδοση της χρήσης του οφείλεται στο γεγονός ότι αποτελεί μια ταχύτερη, φτηνότερη και πιο ευέλικτη εναλλακτική συγκριτικά με τις παραδοσιακές φυσικές εγκαταστάσεις εξοπλισμού πληροφορικής[30].

Α. ΟΡΙΣΜΟΣ ΤΟΥ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

Το υπολογιστικό νέφος σύμφωνα με τον επικρατέστερο ορισμό του National Institute for Standards and Technology (NIST) των Ηνωμένων Πολιτειών Αμερικής είναι: « Ένα μοντέλο που δίνει τη δυνατότητα της συνεχούς, εύκολης και υψηλών απαιτήσεων πρόσβασης σε μια κοινόχρηστη συλλογή ρυθμιζόμενων υπολογιστικών πόρων (πχ. δίκτυα, εξυπηρετητές, αποθηκευτικοί χώροι, εφαρμογές και υπηρεσίες), οι οποίοι τροφοδοτούνται και απελευθερώνονται με ελάχιστη προσπάθεια διαχείρισης και αλληλεπίδρασης παροχής υπηρεσιών»[31].

Β. ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

Τα βασικά χαρακτηριστικά του υπολογιστικού νέφους, σύμφωνα με το National Institute for Standards and Technology (NIST), είναι τα εξής:

- On-demand self-service: Ο κάθε χρήστης μπορεί ανεξάρτητα και μεμονωμένα να έχει πρόσβαση σε υπολογιστικές υπηρεσίες, όπως συνδεσιμότητα με

[30] Ενημερωτικό Σημείωμα MEMO/12/713 της Ευρωπαϊκής Επιτροπής με θέμα : «Εκμετάλλευση των δυνατοτήτων του υπολογιστικού νέφους (Cloud Computing) στην Ευρώπη – τι είναι και τι σημαίνει αυτό για μένα;», 2012, διαθέσιμο εδώ : http://europa.eu/rapid/press-release_MEMO-12-713_el.htm

[31] Peter Mell & Timothy Grance, The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, Special Publication 800-145, 2011, διαθέσιμο εδώ : http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

ένα δίκτυο και αποθήκευση, αυτομάτως και όποτε το επιθυμεί, χωρίς να απαιτείται ανθρώπινη αλληλεπίδραση με τον εκάστοτε φορέα παροχής υπηρεσιών.

- Ευρεία πρόσβαση στο δίκτυο: Οι υπολογιστικές δυνατότητες που παρέχονται είναι διαθέσιμες μέσω του δικτύου και προσβάσιμες μέσα από τυποποιημένους μηχανισμούς, οι οποίοι επιτρέπουν τη χρήση μέσα από ετερογενείς πλατφόρμες (π.χ. κινητά τηλέφωνα, tablet, φορητούς και σταθερούς υπολογιστές).

- Συγκέντρωση πόρων: Οι υπολογιστικοί πόροι του παρόχου συγκεντρώνονται προκειμένου να εξυπηρετήσουν πολλούς καταναλωτές χρησιμοποιώντας ένα μοντέλο κατά το οποίο οι φυσικοί και εικονικοί πόροι διατίθενται και επαναδιατίθενται δυναμικά, ανάλογα με τις απαιτήσεις του χρήστη. Ο χρήστης δεν έχει γνώση ή έλεγχο επί της φυσικής τοποθεσίας των παρεχόμενων πόρων, αλλά μπορεί κατ΄ επιλογή του να προσδιορίσει την τοποθεσία έως ένα γενικό πλαίσιο, όπως μια χώρα ή μια περιοχή.

- Ταχεία ελαστικότητα (Rapid elasticity): Οι υπολογιστικές δυνατότητες μπορούν να προσφέρονται με ταχύτητα και ελαστικότητα, και σε κάποιες περιπτώσεις αυτόματα, ανάλογα με τη ζήτηση. Έτσι οι χρήστες θεωρούν ότι οι δυνατότητες που τους παρέχονται είναι απεριόριστες και μπορούν να τις χρησιμοποιήσουν ανά πάσα στιγμή.

- Measured Service: Τα συστήματα του υπολογιστικού νέφους αυτόματα ελέγχουν και βελτιστοποιούν τη χρήση των πόρων ανάλογα με το είδος της υπηρεσίας (π.χ. αποθήκευση, bandwidth, ενεργοί λογαριασμοί χρηστών κ.λπ.). Η χρήση των πόρων ελέγχεται και παρακολουθείται συστηματικά, ώστε τόσο ο πελάτης όσο και ο πάροχος να έχουν σαφή εικόνα της κατάστασης της υπηρεσίας.

Γ. ΜΟΝΤΕΛΑ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

Η κατηγοριοποίηση αυτή γίνεται με βασικό κριτήριο το είδος της υπηρεσίας η οποία παρέχεται μέσω του υπολογιστικού νέφους και διακρίνεται στα εξής μοντέλα:

- Λογισμικό ως Υπηρεσία (Software as a Service – SaaS).

  Το μοντέλο της διάθεσης του λογισμικού ως υπηρεσία, είναι ένα συνδρομητικό μοντέλο διάθεσης λογισμικού στο περιβάλλον του νέφους. Ο χρήστης έχει πρόσβαση και τη δυνατότητα να χρησιμοποιεί τις εφαρμογές οι

οποίες φιλοξενούνται, αναπτύσσονται και διαχειρίζονται από τον πάροχο και εκτελούνται σε μια υποδομή νέφους. Σε διαφορετική περίπτωση οι εφαρμογές αυτές θα έπρεπε κανονικά να εγκατασταθούν και να τρέξουν στην επιφάνεια εργασίας του χρήστη. Οι εφαρμογές είναι προσβάσιμες από διάφορες εφαρμογές παροχής λογισμικού όπως ένα πρόγραμμα περιήγησης στο διαδίκτυο. Οι χρήστες του εν λόγω μοντέλου δεν διαχειρίζονται οι ίδιοι την εφαρμογή, αλλά έχουν περιορισμένες δυνατότητες ως προς το πώς μπορούν να τη χρησιμοποιήσουν και να αλληλεπιδράσουν με αυτήν.

- Πλατφόρμα ως Υπηρεσία (Platform as a Service PaaS).

Στο μοντέλο τύπου PaaS, ο πάροχος προσφέρει εργαλεία υλικού και λογισμικού στους χρήστες του ως υπηρεσία. Φιλοξενεί το υλικό και το λογισμικό σε δικές του υποδομές και έτσι απαλλάσσει τους χρήστες από την ανάγκη να διαθέτουν συγκεκριμένο συνδυασμό υλικού και λογισμικού προκειμένου να αναπτύξουν ή να εκτελέσουν μια εφαρμογή. Παρέχεται έτσι η δυνατότητα στον χρήστη να καθορίσει, να αναπτύξει, να διαχειριστεί και να παρακολουθήσει τις εφαρμογές του νέφους. Με τον τρόπο αυτό οι χρήστες επωφελούνται τις δυνατότητες του νέφους, να παρέχει αυτόματα πρόσθετους πόρους αποθήκευσης και υπολογιστικούς, όταν αυτό χρειάζονται. Οι χρήστες δεν διαχειρίζονται τις υποδομές (δίκτυα, εξυπηρετητές, λειτουργικά συστήματα, μέσα αποθήκευσης κ.λπ.) του νέφους, ωστόσο διατηρούν τον έλεγχο των εφαρμογών που έχουν αναπτυχθεί και τη δυνατότητα να παραμετροποιούν το περιβάλλον όπου αυτές φιλοξενούνται.

- Υποδομή ως Υπηρεσία (Infrastructure as a Service PaaS).

Το μοντέλο της υποδομής ως υπηρεσία επιτρέπει στους χρήστες να εκμισθώνουν δυνατότητες βάση της ζήτησης με σκοπό την εξάλειψη της ανάγκης τους να έχουν δικές τους υποδομές. Οι χρήστες δηλαδή αποκτούν πρόσβαση σε εργαλεία υλικού και λογισμικού όπως και σε υπολογιστικούς και δικτυακούς πόρους, για την ικανοποίηση των αναγκών τους. Ο καταναλωτής στην περίπτωση αυτή πάλι δεν διαχειρίζεται ή ελέγχει την υποδομή του νέφους, αλλά έχει τον έλεγχο των λειτουργικών συστημάτων,

του χώρου αποθήκευσης και των εφαρμογών που έχουν αναπτυχθεί και ενδεχομένως περιορισμένο έλεγχο ορισμένων χαρακτηριστικών δικτύωσης.

Δ. ΜΟΝΤΕΛΑ ΑΝΑΠΤΥΞΗΣ

Η κατηγοριοποίηση αυτή γίνεται με βασικό κριτήριο το περιβάλλον όπου παρέχεται η υπηρεσία υπολογιστικού νέφους[32].

- Δημόσιο νέφος (Public Cloud).

  Αυτός ο τύπος του υπολογιστικού νέφους, ο οποίος είναι και ο πιο διαδεδομένος, είναι δομημένος έτσι ώστε να είναι προσβάσιμο από το ευρύ κοινό. Αποτελεί την φθηνότερη (και ορισμένες φορές δωρεάν) επιλογή φιλοξενίας και αυτό την καθιστά την δημοφιλέστερη επιλογή των χρηστών. Το βασικότερο μειονέκτημα του μοντέλου αυτού είναι η ασφάλεια των παρεχόμενων υπηρεσιών και η δυσπιστία που προκαλεί στους καταναλωτές.

- Ιδιωτικό νέφος (Private Cloud).

  Ένας άλλος τύπος του υπολογιστικού νέφους, είναι το ιδιωτικό νέφος, το οποίο πρόκειται για μια υποδομή, που ανήκει σε έναν πάροχο υπηρεσιών ο οποίος είναι υπεύθυνος για τη λειτουργία του και η χρήση του περιορίζεται μόνο σε όσους έχουν εξουσιοδότηση πρόσβασης. Το μοντέλο αυτό προσφέρει στους χρήστες μεγαλύτερη ευελιξία κατανομής της υπολογιστικής ισχύος και παρέχει υψηλότερο επίπεδο ασφάλειας. Η επιλογή αυτού του τύπου υπολογιστικού νέφους, είναι πιο δαπανηρή από άποψη απαιτούμενων πόρων αλλά και ανθρώπινου δυναμικού που απαιτείται, για τη διαχείριση των πόρων συγκριτικά με το δημόσιο νέφος.

- Κοινοτικό νέφος (Community cloud).

  Αυτός ο τύπος του υπολογιστικού νέφους προορίζεται για την αποκλειστική χρήση από μια συγκεκριμένη κοινότητα χρηστών από οργανισμούς που έχουν κοινούς στόχους και παρόμοιους σκοπούς λειτουργίας και μπορούν να χτίσουν ένα κέντρο δεδομένων στο υπολογιστικό νέφος το οποίο θα μοιράζονται και θα έχουν πρόσβαση τα μέλη της κοινότητας. Το γεγονός αυτό, καθιστά το συγκεκριμένο μοντέλο

[32] Keith Jeffery & Burkhard Neidecker-Lutz, The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010, European Commission, DG Information Society and Media, 2010, διαθέσιμο εδώ: https://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf , σελ 9-11

περισσότερο ασφαλές, συγκριτικά με το δημόσιο υπολογιστικό νέφος και λιγότερο κοστοβόρο από το ιδιωτικό υπολογιστικό νέφος. Η διαχείριση και λειτουργία του μπορεί να ανατεθεί σε έναν ή περισσότερούς οργανισμούς της κοινότητας ή έναν τρίτο.

- Υβριδικό νέφος (Hybrid cloud).

  Τέλος, ο υβριδικός τύπος νέφους είναι μια σύνθεση από δύο ή περισσότερους διαφορετικούς τύπους νέφους (ιδιωτικό, δημόσιο ή κοινοτικό) που ενώ παραμένουν ξεχωριστές οντότητες, ενώνονται μαζί μέσω της τεχνολογίας που επιτρέπει τη φορητότητα των δεδομένων και την εφαρμογών. Με τον τρόπο αυτό επιτυγχάνεται η αποθήκευση των σημαντικών και απόρρητων δεδομένων στο ιδιωτικό νέφος και των υπόλοιπων ήσσονος σημασίας δεδομένων στο δημόσιο νέφος.

Δ. ΓΕΩΓΡΑΦΙΚΗ ΘΕΣΗ ΤΩΝ ΚΕΝΤΡΩΝ ΔΕΔΟΜΕΝΩΝ

Ένα από τα περισσότερο επίμαχα ζητήματα που προκύπτουν σχετικά με το εφαρμοστέο δίκαιο και πολιτικές στο περιβάλλον του υπολογιστικού νέφους, είναι ότι οι διακομιστές (cloud servers) μπορεί γεωγραφικά να βρίσκονται οπουδήποτε στον κόσμο, μέσα ή έξω από την ΕΕ. Οι πάροχοι υπηρεσιών υπολογιστικού νέφους έχουν ως στόχο την βέλτιστη κυκλοφορία και αναδιάταξη των δεδομένων μεταξύ των κέντρων δεδομένων τους, προκειμένου να επιτυγχάνουν τα όσο το δυνατόν λιγότερο ¨φορτωμένα¨ servers προς βελτίωση της απόδοσης του συστήματος. Ωστόσο, ορισμένοι από τους χρήστες των υπηρεσιών αυτών, μπορεί να επιθυμούν να διασφαλίσουν ότι τα δεδομένα τους παραμένουν εντός της ΕΕ, ειδικά για την προστασία των δεδομένων τους και για λόγους ασφαλείας και μπορούν να το επιτύχουν διευκρινίζοντας το στις συμβάσεις που συνάπτουν με τον εκάστοτε πάροχο για τις υπηρεσίες υπολογιστικού νέφους.

Στην περίπτωση όπου ένας πάροχος υπηρεσιών υπολογιστικού νέφους είναι εγκατεστημένος εντός της Ευρωπαϊκής Ένωσης και επεξεργάζεται δεδομένα προσωπικού χαρακτήρα δεσμεύεται από την κείμενη Ευρωπαϊκή νομοθεσία. Επιπλέον, σύμφωνα με το άρθρο 25 παρ. 1 και 26 παρ. 2 της Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, τα κράτη μέλη προβλέπουν ότι η

διαβίβαση προς τρίτη χώρα δεδομένων προσωπικού χαρακτήρα, που έχουν υποστεί επεξεργασία ή πρόκειται να υποστούν επεξεργασία μετά τη διαβίβασή τους, επιτρέπεται μόνον εάν, τηρουμένων των εθνικών διατάξεων που θεσπίζονται σύμφωνα με τις λοιπές διατάξεις της παρούσας οδηγίας, η εν λόγω τρίτη χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Σε διαφορετική περίπτωση θα πρέπει ο υπεύθυνος της επεξεργασίας να παρέχει επαρκείς εγγυήσεις για την προστασία της ιδιωτικής ζωής και των θεμελιωδών δικαιωμάτων και ελευθεριών των προσώπων καθώς και την άσκηση των σχετικών δικαιωμάτων- οι εγγυήσεις μπορούν ιδίως να απορρέουν από κατάλληλες συμβατικές ρήτρες.

Δεδομένου ότι μεγάλο μέρος των παρόχων υπηρεσιών υπολογιστικού νέφους εντοπίζεται στις Η.Π.Α., ανακύπτει έντονα η ανάγκη τήρησης της ¨σφαίρας ασφαλείας¨ (Safe Harbor) κατά τη διακίνηση ψηφιακών δεδομένων που περιέχουν προσωπικές πληροφορίες από την Ε.Ε. προς τις Η.Π.Α. Με την απόφαση C-362/14, Schrems, του Δικαστηρίου της Ευρωπαϊκής Ένωσης, επιχειρείται να τεθεί υπό έλεγχο αυτή η τεράστια διακίνηση προσωπικών δεδομένων που λαμβάνει χώρα σε ψηφιακή μορφή μέσω του νέφους και αποθηκεύονται σε έναν παγκόσμιο εικονικό χώρο, όπου η ΕΕ αλλά και όλα τα κράτη δεν έχουν στην πραγματικότητα ιδιαίτερη δύναμη, εξουσία και επιρροή. Σε μία κατάσταση, δηλαδή, με τεράστιο διακύβευμα για τα δικαιώματα και τις ελευθερίες, η οποία δημιουργεί μία απειλή όχι ιδιαίτερα ορατή, που όμως οι κίνδυνοι που πηγάζουν από αυτήν εξελίσσονται πιο γρήγορα απ' ότι η σχετική νομοθεσία[33].

Ε. ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΧΡΗΣΗΣ ΤΟΥ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

Ορισμένα από τα κυριότερα οφέλη που προκύπτουν από την υιοθέτηση της χρήσης της υπηρεσίας του υπολογιστικού νέφους είναι τα εξής:

- Μειωμένες δαπάνες προμήθειας υπολογιστών, καθώς οι εφαρμογές βρίσκονται αποθηκευμένες στο νέφος δεν απαιτείται, προκειμένου να λειτουργήσουν υψηλή επεξεργαστική ισχύς και αποθηκευτικός χώρος στον εκάστοτε

[33] Παρατηρήσεις Παναγιώτας Εμμ. Περράκη, Νομιμότητα επεξεργασίας και μεταφοράς προσωπικών δεδομένων προς τρίτες χώρες. Ακύρωση της απόφασης «ασφαλούς λιμένα». Ρόλος και ανεξαρτησία εθνικών αρχών προστασίας προσωπικών δεδομένων. Έννοια επαρκούς/ικανοποιητικού επιπέδου προστασίας, Τριμηνιαίο νομικό περιοδικό : Ελληνική επιθεώρηση ευρωπαϊκού δικαίου, τόμος 35, 4/2015, σελ. 491-496

υπολογιστή από τον οποίο επιθυμούμε να εργαστούμε. Με λιγότερο ¨φόρτο¨ εφαρμογών που πρέπει να διαχειριστούν αυξάνεται η αποδοτικότητα των υπολογιστών. Έτσι μπορεί να επιτευχθεί μείωση του κόστους με την χρήση υλικού με χαμηλότερες δυνατότητες.

- Μειωμένες δαπάνες λογισμικού, καθώς δεν απαιτείται η εγκατάσταση του πακέτου λογισμικού που χρειαζόμαστε σε κάθε υπολογιστή που τυγχάνει να χρησιμοποιήσουμε για να εργαστούμε αλλά η προμήθειά του για μία μόνο φορά και εν συνεχεία χρήση του μέσω του περιβάλλοντος υπολογιστικού νέφους.
- Μειωμένος κίνδυνος απώλειας δεδομένων, καθώς αυτά δεν βρίσκονται αποθηκευμένα σε έναν σκληρό δίσκο ενός συμβατικού υπολογιστή που σε περίπτωση αστοχίας του έχουμε απώλεια των δεδομένων, αλλά σε σύγχρονες δομές δεδομένων των παρόχων του υπολογιστικού νέφους όπου η αστοχία ενός σκληρού δίσκου δεν οδηγεί σε απώλεια των δεδομένων.
- Διευκόλυνση πρόσβασης στα δεδομένα, καθώς ένα αρχείο που δημιουργήθηκε ή τροποποιήθηκε σε μια υπολογιστική συσκευή που είναι εγκατεστημένη σε κάποιο γεωγραφικό σημείο είναι άμεσα προσβάσιμη και από οποιαδήποτε άλλη συσκευή, όπου και αν αυτή βρίσκεται, εφόσον έχει πρόσβαση στο διαδίκτυο. Έτσι, λοιπόν, δεν υπάρχει πλέον δέσμευση σε μια συσκευή αλλά το νέφος δίνει πλήρη ελευθερία επιλογής χρήσης συσκευής και του γεωγραφικού σημείου που αυτή εντοπίζεται. Με τον τρόπο αυτό διευκολύνεται και η συνεργασία και ανταλλαγή δεδομένων μεταξύ ομάδων, όπου άπαντες έχουν πρόσβαση σε κοινά δεδομένα και τους παρέχεται η δυνατότητα επεξεργασίας και επανακοινοποίησης τους.
- Και τέλος, ο απεριόριστος αποθηκευτικός χώρος που παρέχεται στους χρήστες μέσω των κέντρων δεδομένων του υπολογιστικού νέφους και δεν μπορεί να συγκριθεί με την περιορισμένη δυνατότητα αποθήκευσης που τους παρέχεται από οποιοδήποτε φυσικό μέσο αποθήκευσης.

ΣΤ. ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΧΡΗΣΗΣ ΤΟΥ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

Πέρα από τα ανωτέρω εκτεθέντα θετικά χαρακτηριστικά του, το υπολογιστικό νέφος, παρά τη ραγδαία εξάπλωσή του, παρουσιάζει και ορισμένα μειονεκτήματα τα κυριότερα εκ των οποίων είναι τα εξής:

- Ασφάλεια δεδομένων. Μέσω του υπολογιστικού νέφους, οι χρήστες αποθηκεύουν με τη βοήθεια του διαδικτύου τα δεδομένα τους, που συχνά υπάγονται στην κατηγορία των προσωπικών ή ευαίσθητων, στις βάσεις δεδομένων των παρόχων. Με τον τρόπο αυτό η διαχείριση των δεδομένων αυτών μεταβιβάζεται στους παρόχους των υπηρεσιών υπολογιστικού νέφους με ό,τι αυτό συνεπάγεται για την μυστικότητα και ασφάλεια των δεδομένων. Για τον λόγο αυτό οι πάροχοι πρέπει να εγγυόνται το απόρρητο, την ακεραιότητα και την διαθεσιμότητα των δεδομένων[34].
- Διαθεσιμότητα δεδομένων. Δεδομένου του γεγονότος ότι η διαχείριση των δεδομένων και υποδομών μεταβιβάζεται στους παρόχους, μια βλάβη σε ένα υπολογιστικό σύστημα θα μπορούσε να προκαλέσει σοβαρές δυσλειτουργίες σε οποιονδήποτε χρήστη βασίζει τη δραστηριότητά του στις υπηρεσίες του υπολογιστικού νέφους[35].
- Σύνδεση στο διαδίκτυο. Η υπηρεσία του υπολογιστικού νέφους είναι αδύνατον να λειτουργήσει χωρίς πρόσβαση στο διαδίκτυο από τους χρήστες της. Συνεπώς, στη περίπτωση που για οποιονδήποτε λόγο χαθεί η πρόσβαση στο διαδίκτυο, χάνεται και η πρόσβαση στο νέφος με ότι αυτό συνεπάγεται για τους χρήστες που πιθανόν να έχουν την πλειονότητα των δεδομένων των δεδομένων τους στο νέφος και χωρίς την πρόσβαση σε αυτό να καθίστανται ανενεργοί.

Ζ. Η ΠΡΟΣΕΓΓΙΣΗ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ ΓΙΑ ΤΟ ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ

Η Ευρωπαϊκή Ένωση δεν έμεινε αμέτοχη απέναντι στο καταιγιστικό φαινόμενο του υπολογιστικού νέφους. Η Ευρωπαϊκή Επιτροπή με την ανακοίνωσή της με τίτλο «Αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους» το 2012, που ως στόχο είχε την διευκόλυνση της ταχύτερης υιοθέτησης του υπολογιστικού νέφους, ανέδειξε τα βασικά πεδία στα οποία απαιτείται ανάληψη δράσης από την Ε.Ε. Σύμφωνα με την ανακοίνωση, πρέπει να ληφθούν μέτρα σχετικά με :

[34] Lori M. Kaufman, Data Security in the World of Cloud Computing, IEEE Security & Privacy, 2009, διαθέσιμο εδώ: http://web.math.jjay.cuny.edu/fcm745/codes/SecurityCloudComputing.pdf
[35] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica and Matei Zaharia, A view of cloud computing, Communications of the ACM, 2010, διαθέσιμο εδώ: http://dl.acm.org/citation.cfm?id=1721672

- Το ζήτημα που προκύπτει λόγω των διαφορετικών εθνικών νομικών πλαισίων και αβεβαιοτήτων ως προς την ισχύουσα νομοθεσία, τη γεωγραφική θέση του ψηφιακού περιεχομένου και των δεδομένων.
- Το πρόβλημα με τις συμβάσεις μεταξύ χρηστών και παρόχων υπηρεσιών υπολογιστικού νέφους σχετικά με την πρόσβαση, τη φορητότητα και την ιδιοκτησία των δεδομένων. Για παράδειγμα, πρέπει να πρέπει να αποσαφηνισθούν θέματα σχετικά με την ευθύνη για βλάβες υπηρεσίας, όπως χρόνος εκτός λειτουργίας ή απώλεια δεδομένων, με την κυριότητα των δεδομένων που προκύπτουν από εφαρμογές υπολογιστικού νέφους ή με τον τρόπο επίλυσης διαφορών.
- Την πληθώρα προτύπων αποθήκευσης δεδομένων στο υπολογιστικό νέφος που ποικίλλουν ανά πάροχο και προκαλούν σύγχυση και αβεβαιότητα ως προς τη φορητότητα των δεδομένων και τον βαθμό προστασίας των προσωπικών δεδομένων.

Προκειμένου η Ευρώπη να στραφεί ευνοϊκά προς το υπολογιστικό νέφος και να ενεργοποιηθεί προς την κατεύθυνση αυτή πρέπει να αναπτυχθεί πνεύμα ασφάλειας και εμπιστοσύνης. Υπάρχει, συνεπώς, η ανάγκη για μια αλυσίδα από μέτρα οικοδόμησης εμπιστοσύνης. Η δημιουργία σαφούς και προστατευτικού πλαισίου θα εξασφαλίσει ότι αυτή η τεχνολογία παρέχει αξιόπιστη πρόσβαση στους χρήστες. Για την επίτευξη του στόχου αυτού, η Ευρωπαϊκή Επιτροπή δρομολόγησε τρείς ειδικές βασικές δράσεις για το υπολογιστικό νέφος.

(1) Αντιμετώπιση του κυκεώνα των προτύπων

(2) Ασφαλείς και δίκαιοι συμβατικοί όροι και προϋποθέσεις

(3) Συγκρότηση ευρωπαϊκής σύμπραξης για το υπολογιστικό νέφος για την προώθηση καινοτομίας και οικονομικής μεγέθυνσης στον δημόσιο τομέα[36].

Σε συνέχεια της ανωτέρω, η Ευρωπαϊκή Επιτροπή το 2014 εξέδωσε νέα ανακοίνωση, με τίτλο «Προς μια ακμάζουσα οικονομία βασιζόμενη στα δεδομένα». Στην ανακοίνωση αυτή λαμβάνονται υπ΄όψιν αποτελέσματα διαβουλεύσεων[37] και

[36] Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, Αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους, COM/2012/0529 final, διαθέσιμο εδώ : http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52012DC0529&qid=1488501238624&from=EL

[37] Π.χ. στον διαδικτυακό τόπο της Ευρωπαϊκής Επιτροπής - Trusted Cloud Europe Survey (http://ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe-survey)

σχετικές νομοθετικές προτάσεις ούτως ώστε να ορισθούν οι ενέργειες που πρέπει να λάβουν χώρα στον τομέα του υπολογιστικού νέφους. Οι αναγκαίες δράσεις της ευρωπαϊκής στρατηγικής προς την ταχύτερη υιοθέτηση ενός αξιόπιστου υπολογιστικού νέφους σχετίζονται άμεσα με τη διαφάνεια των προτύπων, την πιστοποίηση των παρόχων σε ενωσιακή κλίμακα, τους ασφαλείς και δίκαιους συμβατικούς όρους και προϋποθέσεις για τους χρήστες υπολογιστικού νέφους και τη δημιουργία Ευρωπαϊκής Σύμπραξης για το υπολογιστικό νέφος (ECP). Το 2014 η Ευρωπαϊκή Σύμπραξη για το υπολογιστικό νέφος δημοσίευσε την σχετική με το θέμα έκθεση με τίτλο «Trusted Cloud Europe» (TCE)[38] [39].

Τέλος, στις 19 Απριλίου 2016 η Ευρωπαϊκή Επιτροπή εξέδωσε Δελτίο Τύπου σχετικά με την «Ευρωπαϊκή πρωτοβουλία για το υπολογιστικό νέφος». Παρουσίασε το σχέδιό της για υπηρεσίες βασιζόμενες στο υπολογιστικό νέφος και για υποδομή δεδομένων παγκόσμιας εμβέλειας με σκοπό να διασφαλιστεί ότι η επιστήμη, οι επιχειρήσεις και οι δημόσιες υπηρεσίες επωφελούνται από την επανάσταση των μαζικών δεδομένων.

Η Ευρωπαϊκή Επιτροπή, σύμφωνα με την ανακοίνωση, θα θέσει σταδιακά σε εφαρμογή την ευρωπαϊκή πρωτοβουλία για το υπολογιστικό νέφος μέσω μιας σειράς δράσεων, όπως:

- Από το 2016: τη δημιουργία ενός Ευρωπαϊκού Νέφους Ανοικτής Επιστήμης για τους Ευρωπαίους ερευνητές και τους επιστημονικούς συνεργάτες τους σε όλον τον κόσμο με την ενσωμάτωση και ενοποίηση πλατφορμών ηλεκτρονικών υποδομών, τη συγκέντρωση των υφιστάμενων επιστημονικών υπολογιστικών νεφών και των υποδομών έρευνας και τη στήριξη της ανάπτυξης υπηρεσιών βασιζόμενων στο υπολογιστικό νέφος.
- 2017: το άνοιγμα εξ ορισμού όλων των επιστημονικών δεδομένων που θα παράγονται στο πλαίσιο μελλοντικών έργων του προγράμματος έρευνας και καινοτομίας «Ορίζοντας 2020», ώστε να διασφαλίζεται ότι η επιστημονική

[38] The European Cloud Partnership Steering Board για την Ευρωπαϊκή Επιτροπή, «Establishing a Trusted Cloud Europe: A policy vision document by the Steering Board of the European Cloud Partnership», 2014, διαθέσιμο εδώ: http://ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe

[39] Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, Προς μια ακμάζουσα οικονομία βασιζόμενη στα δεδομένα, COM/2014/0442 final, 2/7/2014, διαθέσιμη εδώ : http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52014DC0442&from=EN

κοινότητα θα μπορεί να επαναχρησιμοποιεί τον τεράστιο όγκο δεδομένων που παράγει.

- 2018: την έναρξη μιας εμβληματικής πρωτοβουλίας για την επιτάχυνση της εκκολαπτόμενης ανάπτυξης της κβαντικής τεχνολογίας, η οποία αποτελεί τη βάση της επόμενης γενιάς υπερυπολογιστών.
- Μέχρι το 2020: ανάπτυξη και αξιοποίηση ευρωπαϊκών υποδομών μεγάλης κλίμακας για υψηλών επιδόσεων πληροφορική, αποθήκευση δεδομένων και δίκτυα, μέσω, μεταξύ άλλων, της απόκτησης δύο πρωτοτύπων υπερυπολογιστών επόμενης γενιάς, εκ των οποίων ο ένας θα συγκαταλέγεται μεταξύ των τριών καλύτερων στον κόσμο, της δημιουργίας ενός ευρωπαϊκού κέντρου μαζικών δεδομένων, και της αναβάθμισης του κεντρικού δικτύου για την έρευνα και την καινοτομία (GEANT).

Τέλος, εκτός από την ευρωπαϊκή ερευνητική κοινότητα, στο Ευρωπαϊκό Νέφος Ανοικτής Επιστήμης και στην ευρωπαϊκή υποδομή δεδομένων θα έχουν πρόσβαση και θα αποκομίζουν οφέλη πολλοί άλλοι χρήστες:

- Οι επιχειρήσεις θα έχουν οικονομικά προσιτή και εύκολη πρόσβαση σε δεδομένα και υποδομές πληροφορικής υψηλού επιπέδου, καθώς και σε πληθώρα επιστημονικών δεδομένων που καθιστούν δυνατή την καινοτομία που βασίζεται στα δεδομένα.
- Η βιομηχανία θα αποκομίσει οφέλη από τη δημιουργία ενός οικοσυστήματος υπολογιστικού νέφους μεγάλης κλίμακας, που υποστηρίζει την ανάπτυξη νέων ευρωπαϊκών τεχνολογιών όπως μικροκυκλωμάτων (τσιπ) χαμηλής κατανάλωσης για υπολογιστές υψηλών επιδόσεων.
- Οι δημόσιες υπηρεσίες θα επωφεληθούν από την αξιόπιστη πρόσβαση σε ισχυρούς υπολογιστικούς πόρους και τη δημιουργία μιας πλατφόρμας για το άνοιγμα των δεδομένων και των υπηρεσιών τους, πράγμα που μπορεί να οδηγήσει σε φθηνότερες, ταχύτερες και καλύτερα διασυνδεδεμένες δημόσιες υπηρεσίες. Οι ερευνητές θα επωφεληθούν επίσης από τη διαδικτυακή πρόσβαση στον πλούτο των δεδομένων που προκύπτουν από τις δημόσιες υπηρεσίες[40].

[40] Ευρωπαϊκή Επιτροπή - Δελτίο Τύπου, «Η ευρωπαϊκή πρωτοβουλία για το υπολογιστικό νέφος θα δώσει στην Ευρώπη το παγκόσμιο προβάδισμα στη βασιζόμενη στα δεδομένα οικονομία», 2016, διαθέσιμο εδώ: http://europa.eu/rapid/press-release_IP-16-1408_el.htm

ΚΕΦΑΛΑΙΟ 4^{Ο} : ΤΕΧΝΙΚΑ ΖΗΤΗΜΑΤΑ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗΣ ΑΝΑΛΥΣΗΣ ΨΗΦΙΑΚΩΝ ΠΕΙΣΤΗΡΙΩΝ ΣΕ ΠΕΡΙΒΑΛΛΟΝ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

Λόγω της έλλειψης εξειδικευμένων μεθοδολογιών και εργαλείων για την εγκληματολογική ανάλυση σε περιβάλλον υπολογιστικού νέφους υιοθετήθηκαν αρχικά οι παραδοσιακές μεθοδολογίες ανάλυσης ψηφιακών πειστηρίων, όπως αυτές εκτέθηκαν ανωτέρω. Ωστόσο, οι υπάρχουσες προσεγγίσεις έχουν ως δεδομένο το γεγονός ότι τα ψηφιακά πειστήρια βρίσκονται στην κατοχή των ερευνητών. Αυτό δεν ισχύει και για το περιβάλλον υπολογιστικού νέφους όπου τα στοιχεία μπορούν να βρίσκονται σε διάφορες γεωγραφικές τοποθεσίες σε κέντρα δεδομένων υπό τον έλεγχο διαφόρων παρόχων υπηρεσιών νέφους. Αυτό επιδρά καθοριστικά στον εντοπισμό και συλλογή των αποδεικτικών στοιχείων. Ο θεμελιώδης στόχος είναι να διασφαλιστεί η ακεραιότητα των αποδείξεων που ανακτώνται από το νέφος, έτσι ώστε να μπορεί να χρησιμοποιηθεί σε νομικές διαδικασίες.

Στην ενότητα αυτή θα γίνει μια προσπάθεια παρουσίασης των τεχνικών προκλήσεων που τίθενται κατά την εγκληματολογική ανάλυση ψηφιακών πειστηρίων στο περιβάλλον του υπολογιστικού νέφους.

Α. ΔΙΑΤΗΡΗΣΗ ΚΑΙ ΣΥΛΛΟΓΗ

Η ψηφιακή εγκληματολογική έρευνα ασχολείται με τη συλλογή δεδομένων από υπολογιστικά συστήματα που μπορεί αργότερα να αποτελέσουν αποδεικτικά στοιχεία σχετικά με τη τέλεση μιας παράνομης πράξης. Η φάση της διατήρησης σε μια παραδοσιακή ψηφιακή εγκληματολογική έρευνα, σύμφωνα με τις διεθνείς πρακτικές και αρχές που εφαρμόζονται σε αυτήν, προϋποθέτει ότι τα ψηφιακά πειστήρια παραμένουν αναλλοίωτα και η διαδικασία που ακολουθήθηκε για τη διατήρηση και συλλογή τους θα πρέπει να μπορεί να επαναληφθεί με το ίδιο αποτέλεσμα. Συνεπώς καθ΄ όλη τη διάρκεια της έρευνας θα πρέπει να διασφαλίζεται η ακεραιότητα των δεδομένων, ότι δηλαδή τα συλλεχθέντα αποδεικτικά στοιχεία είναι μια ακριβής αναπαράσταση των δεδομένων που βρέθηκαν στο ερευνηθέν υπολογιστικό σύστημα. Αρκετές πτυχές της φάσης διατήρησης επηρεάζονται από τη χρήση του υπολογιστικού νέφους.

1. Διεύρυνση δυνατοτήτων αποθήκευσης

Στις συμβατικές έρευνες, προϋπόθεση της διατήρησης των αποδεικτικών στοιχείων είναι η ύπαρξη επαρκούς ψηφιακού αποθηκευτικού χώρου για την αποθήκευση των δεδομένων που συλλέγονται. Το φαινόμενο της συνεχώς και αυξανόμενης παροχής αποθηκευτικής ικανότητας προς τους χρήστες με ολοένα και μειωμένο κόστος δυσχεραίνει το έργο των ερευνητών καθώς αυξάνει τον όγκο των στοιχείων που συλλέγονται κατά τη διάρκεια των εγκληματολογικών ερευνών. Αυτό προκαλεί στον ερευνητή αρχικά το πρόβλημα της εξασφάλισης πόρων (ικανό αποθηκευτικό χώρο) και περαιτέρω αύξηση του απαιτούμενου χρόνου από τον ερευνητή προς εξέταση του όγκου των δεδομένων.

Η χρήση των υπηρεσιών υπολογιστικού νέφους επιδεινώνει ακόμη περισσότερο το πρόβλημα της αποθήκευσης δεδομένων. Από την πλευρά του χρήστη, μια τυπική δημόσια υποδομή υπολογιστικού νέφους φαίνεται να προσφέρει «απεριόριστο» αποθηκευτικό χώρο. Έτσι είναι πολύ πιθανό ένας ερευνητής να βρεθεί αντιμέτωπος με τη πρόκληση της συλλογής ενός εξαιρετικά μεγάλου όγκου δεδομένων που ένας χρήστης έχει «ανεβάσει» σε ένα περιβάλλον υπολογιστικού νέφους. Μία λύση στην οποία θα μπορούσαν να καταφύγουν οι ανακριτικές αρχές είναι η χρήση της υποδομής του δημοσίου υπολογιστικού νέφους για την αποθήκευση των ψηφιακών πειστηρίων, η οποία ωστόσο εγείρει νέες προκλήσεις, τόσο από νομική όσο και από τεχνική άποψη, καθώς θα πρέπει να εξασφαλισθεί η προστασία των προσωπικών δεδομένων που ενδεχομένως εμπεριέχονται στα δεδομένα που αναρτώνται στο νέφος[41].

Ως μια ακόμη εναλλακτική λύση για την μείωση του όγκου των δεδομένων που πρέπει να αναλυθούν από τον ερευνητή προτείνεται η υιοθέτηση του μοντέλου της διαλογής (triage), το οποίο βρίσκει εφαρμογή κυρίως στις περιπτώσεις εκείνες όπου απαιτούνται άμεσα αποτελέσματα εις βάρος της αξιοπιστίας και της σε βάθος χρόνου διαθεσιμότητας των αποδεικτικών στοιχείων (π.χ. σε περιπτώσεις άμεσου κίνδυνου ζωής). Κατά το πρότυπο αυτό με την ονομασία : Cyber Forensic Field Triage Process Model (CFFTPM) η έρευνα και συλλογή των στοιχείων γίνεται επιτόπου σε σύντομο

[41] Grispos, G., Storer, T., & Glisson, W., Calm before the storm: The challenges of cloud computing in digital forensics, International Journal of Digital Crime and Forensics, 2012, διαθέσιμο εδώ: https://arxiv.org/ftp/arxiv/papers/1410/1410.2123.pdf , σελ. 28–48

χρονικό διάστημα και χωρίς να απαιτείται η προσκόμιση των ψηφιακών πειστηρίων στο εργαστήριο για περαιτέρω εξέταση[42].

2. **Αλληλουχία των βημάτων της έρευνας (Chain of custody)**

Όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο, κατά τη διάρκεια μιας συμβατικής εγκληματολογικής έρευνας, είναι απαραίτητο να καταγράφεται και να τηρείται μια αλληλουχία συγκεκριμένων βημάτων ώστε να εξασφαλίζεται η εγκυρότητα των αποδεικτικών στοιχείων που παρουσιάζονται στο δικαστήριο. Σε μια τέτοιου είδους έρευνα, η αλληλουχία των βημάτων ξεκινά όταν ο ερευνητής αποκτήσει το φυσικό έλεγχο του ψηφιακού πειστηρίου που σχετίζεται με την υπό έρευνα υπόθεση, έχοντας την δυνατότητα να αφαιρέσει τις συσκευές αποθήκευσης όπου βρίσκονται τα δεδομένα και να τα μεταφέρει στο εργαστήριο για εξέταση. Η δομή ωστόσο του υπολογιστικού νέφους δεν επιτρέπει την εφαρμογή της εν λόγω διαδικασίας καθώς εάν ο ερευνητής δεν καταφέρει να αποκτήσει άμεσα πρόσβαση στην επίμαχη πλατφόρμα υπολογιστικού νέφους τότε ελλοχεύει ο κίνδυνος απώλειας ή αλλοίωσης των δεδομένων που τηρούνται σε αυτό, είτε από τον χρήστη απομακρυσμένα, είτε από τον πάροχο[43].

3. **Απόκτηση αντιγράφου των ψηφιακών δεδομένων**

Εφόσον ο ερευνητής έχει καταφέρει να αποκτήσει πρόσβαση στην υπηρεσία υπολογιστικού νέφους, το επόμενο βήμα είναι η απόκτηση ενός πιστού αντιγράφου των δεδομένων που τηρούνται στο νέφος έτσι ώστε να ακολουθήσει η ανάλυσή τους. Σύμφωνα με τα πρότυπα για τη συμβατική εξέταση ψηφιακών πειστηρίων είναι απαραίτητη η χρήση ειδικών τεχνικών (Forensic imaging) και εργαλείων (Writeblocker) για την διαδικασία αυτή αποκλείοντας την πιθανότητα αλλοίωσης των δεδομένων.

Η συλλογή, ωστόσο, των αποδεικτικών στοιχείων από ένα περιβάλλον υπολογιστικού νέφους αποτελεί μια πρόκληση για τους ερευνητές καθώς τα ανωτέρω εργαλεία και τεχνικές δεν αποδίδουν το ίδιο αποτελεσματικά. Η ιδιαίτερη δομή (εικονικοποίηση – virtualization) αποθήκευσης των δεδομένων

[42] Marcus K. Rogers, James Goldman, Rick Mislan, Timothy Wedge, Steve Debrota, Computer Forensics Field Triage Process Model, Journal of Digital Forensics, Security and Law, 2014, σελ. 19-20, διαθέσιμο εδώ: http://ojs.jdfsl.org/index.php/jdfsl/article/view/222

[43] Giuliano Giova, Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems, International Journal of Computer Science and Network Security, 2011, διαθέσιμο εδώ: http://paper.ijcsns.org/07_book/201101/20110101.pdf , σελ. 2

στο υπολογιστικό νέφος καθιστά περίπλοκο τον εντοπισμό και την απομόνωση των φυσικών συσκευών αποθήκευσης, που περιέχουν τα δεδομένα των υπό έρευνα χρηστών που χρήζουν συλλογής, και ανήκουν σε κάποιο πάροχο υπηρεσιών υπολογιστικού νέφους. Τα δεδομένα αυτά μπορεί να εξαπλώνονται μεταξύ πολλών διαφορετικών φυσικών συσκευών παρά το γεγονός ότι στους χρήστες αυτά φαίνεται να αποθηκεύονται σε μια ενιαία θέση.

Επίσης, κατά τις συμβατικές μεθόδους εγκληματολογικής ανάλυσης ψηφιακών πειστηρίων προβλέπεται κατάσχεση του συνόλου των συσκευών αποθήκευσης που περιέχουν σχετικές πληροφορίες με το υπό έρευνα αδίκημα. Στην περίπτωση ωστόσο της έρευνας σε περιβάλλον υπολογιστικού νέφους, η κατάσχεση αντίστοιχα όλων των συσκευών αποθήκευσης που περιέχουν τα επίμαχα δεδομένα είναι ιδιαίτερα περίπλοκη και χρονοβόρα για τον ερευνητή και προκαλεί έντονα προβλήματα στον πάροχο των υπηρεσιών. Επιπλέον, συχνό είναι το φαινόμενο να συλλέγεται μεγάλος όγκος δεδομένων εκ του οποίου ένα μικρό μόνο μέρος είναι σχετικό με την ερευνόμενη υπόθεση, τονίζοντας ακόμη περισσότερο την ανάγκη ανάπτυξης μεθόδων που επιτρέπουν τη μερική ανάκτηση των δεδομένων χωρίς όμως να υπάρχουν περιθώρια αμφισβήτησης της εγκυρότητας του παραχθέντος πειστηρίου. Έτσι, λοιπόν, κατά την κατάσχεση μέσων αποθήκευσης που χρησιμοποιεί το υπολογιστικό νέφος είναι αρκετά πιθανό να περιέχονται σε αυτά προσωπικά δεδομένα και έτερων χρηστών, που δεν σχετίζονται με την ερευνόμενη υπόθεση και η προσπέλασή τους να συνιστά παραβίαση της εκάστοτε ισχύουσας νομοθεσίας περί προσωπικών δεδομένων.

Στην περίπτωση κατά την οποία ο ερευνητής έχει αποκτήσει πρόσβαση στην υπηρεσία του υπολογιστικού νέφους, είναι δυνατή η διεξαγωγή «ζωντανής» έρευνας επί των δεδομένων αυξάνοντας την ποσότητα των πληροφοριών που ένας ερευνητής είναι σε θέση να συλλέξει[44]. Ωστόσο, ακόμη και σε αυτή τη περίπτωση η λήψη ενός πιστού αντιγράφου των δεδομένων θα μπορούσε να παρεμποδιστεί περαιτέρω με τη χρήση της δυνατότητας κρυπτογράφησης. Δεδομένου της ανασφάλειας των χρηστών του

[44] Sameera Abdulrahman Almulla, Youssef Iraqi, Andrew Jones, A STATE-OF-THE-ART REVIEW OF CLOUD FORENSICS, The Journal of Digital Forensics, Security and Law, 2014, διαθέσιμο εδώ : http://ojs.jdfsl.org/index.php/jdfsl/article/viewFile/253/234, σελ. 10

υπολογιστικού νέφους για την εμπιστευτικότητα των δεδομένων που αναρτούν σε αυτό, οι πάροχοι στρέφονται προς την λύση της κρυπτογράφησης προκειμένου να εμπνεύσουν εμπιστοσύνη στους χρήστες. Έτσι, τα δεδομένα κρυπτογραφούνται πριν να αποθηκευτούν στο υπολογιστικό νέφος, ενώ τα κλειδιά που απαιτούνται για την αποκρυπτογράφηση των δεδομένων δεν μεταβιβάζονται σε αυτό. Κατ΄ αυτόν τον τρόπο, ακόμη και αν ο πάροχος των υπηρεσιών υπολογιστικού νέφους διαταχθεί κατόπιν εισαγγελικής παραγγελίας να προβεί στην αποκρυπτογράφηση των δεδομένων, αυτό θα είναι τεχνικά αδύνατο καθώς το «κλειδί» αποκρυπτογράφησης θα βρίσκεται αποκλειστικώς στον ιδιοκτήτη των δεδομένων[45].

4. Η πρόκληση των διαγραμμένων αρχείων

Κατά τη διάρκεια μιας εγκληματολογικής ανάλυσης ψηφιακών πειστήριων, ο ερευνητής έρχεται συχνά αντιμέτωπος με τη πρόκληση της άντλησης στοιχείων από διαγραμμένα αρχεία όπως και της ακολουθητέας διαδικασίας για τη αποφυγή διαγραφής αυτών. Στην περίπτωση της συμβατικής έρευνας ψηφιακών δεδομένων, η συσκευή στη οποία είναι αποθηκευμένα τα ψηφιακά δεδομένα μπορεί να βρίσκεται στη κατοχή του δράστη παρέχοντας του έτσι τη δυνατότητα της καταστροφής της. Το υπολογιστικό νέφος θα μπορούσε και να διευκολύνει αλλά και να δυσχεράνει το έργο των ερευνητών για την ανάκτηση των διαγραμμένων δεδομένων ή την αποφυγή διαγραφής τους. Απαιτούνται εξιδεικευμένες γνώσεις ή δικαιώματα διαχειριστή της υπηρεσίας του νέφους για να επιτευχθεί οριστική διαγραφή ή αλλοίωση των δεδομένων, σε διαφορετική περίπτωση είναι διαθέσιμα στον ερευνητή προς εξερεύνηση[46]. Ωστόσο, ενώ στη συμβατική έρευνα, τα ΄΄διαγραμμένα΄΄ αρχεία από μια συσκευή αποθήκευσης αποτελούν συνήθως μια πλούσια πηγή στοιχείων, στο περιβάλλον του υπολογιστικού νέφους η ανάκτηση των διαγραμμένων δεδομένων είναι μια περίπλοκη διαδικασία. Ορισμένα από τα δεδομένα που έχουν διαγραφεί μπορεί να εξακολουθούν να υπάρχουν εγείρεται όμως η πρόκληση για το πώς θα ανακτηθούν από τον ερευνητή τα διαγραμμένα

[45] Sashank Dara, Cryptography Challenges for Computational Privacy in Public Clouds, IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), 2013, διαθέσιμο εδώ : https://eprint.iacr.org/2013/272.pdf

[46] Eric Slack, How do you know that "Delete" means Delete in Cloud, 2011, διαθέσιμο εδώ : http://www.storage-switzerland.com/Articles/Entries/2011/8/16_How_do_you_know_that_Delete_means_Delete_in_Cloud_Storage.html

αυτά δεδομένα και επιπλέον θα προσδιοριστεί το ιδιοκτησιακό καθεστώς των δεδομένων που κατάφεραν να ανακτηθούν[47].

5. Η ανακύπτουσα ανάγκη συνεργασίας με οργανισμούς

Στην περίπτωση που δεν είναι δυνατό για έναν ερευνητή να αποκτήσει πρόσβαση σε μια υπηρεσία υπολογιστικού νέφους, υπάρχει η εναλλακτική λύση της απόκτησης των επίμαχων δεδομένων από το πάροχο. Ωστόσο, αυτή η προσέγγιση είναι προβληματική για διάφορους λόγους. Με την παρεμβολή του παρόχου για την απόκτηση των δεδομένων, ο ερευνητής δεν ελέγχει την τήρηση της αλληλουχίας των βημάτων της έρευνας (Chain of custody) από τους υπαλλήλους του παρόχου, που εμπλέκονται για την εξαγωγή του αντιγράφου των δεδομένων. Επίσης, όπως είδαμε και σε προηγούμενο κεφάλαιο, οι αρμόδιοι για την έρευνα θα πρέπει να είναι καταλλήλως εκπαιδευμένοι και με συναφή εμπειρία για να διασφαλίζεται η αξιοπιστία του εξαγόμενου πειστηρίου, κάτι που δεν μπορεί να ελεγχθεί αν ισχύει για τους εμπλεκόμενους υπαλλήλους του παρόχου. Μια ενδεχόμενη λύση μπορεί να είναι η ύπαρξη ειδικά εκπαιδευμένων υπαλλήλων για τη διεξαγωγή των απαιτούμενων διαδικασιών της εγκληματολογικής έρευνας μεταξύ του ανθρώπινου δυναμικού του οργανισμού του παρόχου. Τα άτομα αυτά θα τηρούν την απαιτούμενη αλληλουχία βημάτων κατά τα πρώτα στάδια και εν συνεχεία θα μεταβιβάζεται στις ανακριτικές αρχές.

Τέλος, μία ακόμη πρόκληση κατά τη φάση της συλλογής των ψηφιακών πειστηρίων στο υπολογιστικό νέφος είναι ο καθορισμός της χρησιμοποιούμενης ζώνης ώρας. Το στοιχείο αυτό είναι ιδιαίτερα σημαντικό για την ανασυγκρότηση της αλληλουχίας των γεγονότων σχετικά με την διερευνώμενη υπόθεση. Κατά τις συμβατικές διαδικασίες έρευνας και εφόσον πρόκειται για μεμονωμένα υπολογιστικά συστήματα, ο καθορισμός της χρησιμοποιούμενης ζώνης ώρας είναι ευκολότερος. Στο περιβάλλον υπολογιστικού νέφους η διαδικασία αυτή είναι ιδιαίτερα περίπλοκη καθώς τα

[47] Keyun Ruan, Joe Carthy, Tahar Kechadi and Mark Crosbie, Cloud Forensics - Advances in Digital Forensics VII, 2011, διαθέσιμο εδώ: https://link.springer.com/chapter/10.1007/978-3-642-24212-0_3#enumeration , σελ. 35-46

αποθηκευμένα δεδομένα είναι πιθανό να είναι διαμοιρασμένα σε διάφορες φυσικές τοποθεσίες, με περισσότερες από μια τηρούμενες ζώνες ώρας[48].

Β. ΕΞΕΤΑΣΗ ΚΑΙ ΑΝΑΛΥΣΗ

Εφόσον ολοκληρωθεί η φάση της συλλογής των πειστηρίων, χρησιμοποιούνται ορισμένα ευρέως διαδεδομένα εργαλεία με σκοπό την εξέταση και ανάλυση των δεδομένων που έχουν συγκεντρωθεί. Η έλλειψη διαθέσιμων εξειδικευμένων εργαλείων για την εγκληματολογική ανάλυση των ψηφιακών πειστηρίων στο περιβάλλον υπολογιστικού νέφους, αναγκάζει τους ερευνητές να χρησιμοποιούν τα συμβατικά εργαλεία ψηφιακής εγκληματολογίας τα οποία σε ορισμένες περιπτώσεις δεν ανταποκρίνονται πλήρως στις νέες απαιτήσεις.

Η πλειονότητα των αποδεικτικών στοιχείων που συλλέγονται στο υπολογιστικό νέφος έχει την ίδια μορφή με αυτά που συγκεντρώνονται κατά την διάρκεια των συμβατικών ψηφιακών ερευνών. Εντοπίζονται, ωστόσο, και ορισμένα στοιχεία με νέα μορφή, όπως τα αρχεία δραστηριοτήτων των χρηστών υπολογιστικού νέφους. Προκειμένου ένας ερευνητής να καταφέρει να συλλέξει αυτά τα αρχεία καταγραφής, θα πρέπει να έχει ο ίδιος πρόσβαση με ρόλο διαχειριστή στην υπηρεσία του υπολογιστικού νέφους, διαφορετικά θα πρέπει να του μεταβιβασθούν από τον πάροχο, με τα ανακύπτοντα ζητήματα όμως που αναφέρθηκαν παραπάνω σχετικά με την τήρηση της αλληλουχίας των βημάτων της έρευνας[49].

Γ. ΠΑΡΟΥΣΙΑΣΗ

Τα στοιχεία που συγκεντρώθηκαν κατά τη διάρκεια μιας ψηφιακής εγκληματολογικής έρευνας μπορούν να συνοψιστούν σε μια έκθεση, με παράλληλη παρουσίαση των συμπερασμάτων. Απώτερος σκοπός της εν λόγω έκθεσης είναι η χρήση της στην δικαστική διαδικασία. Η επιστημονική εγκυρότητα της εν λόγω έκθεσης πραγματογνωμοσύνης, η οποία είναι απαραίτητο στοιχείο ούτως ώστε να γίνει αποδεκτή από το δικαστήριο, εξαρτάται από διάφορους παράγοντες συμπεριλαμβανομένου του κατά πόσο η θεωρία ή τεχνική που εφαρμόσθηκε μπορεί να

[48] Sean Thorpe - Indrajit Ray, File Timestamps for Digital Cloud Investigations, Journal of Information Assurance and Security, 2011, διαθέσιμο εδώ : http://fenc-utech.net/scit/uploads/Paper52.pdf
[49] Deevi Radha Rani, Sk. Nazma Sultana, Pasala Lourdu Sravani, Challenges of Digital Forensics in Cloud Computing Environment, Indian Journal of Science and Technology, 2016, διαθέσιμο εδώ : http://www.indjst.org/index.php/indjst/article/view/93051/69863 , σελ. 3

(και έχει) δοκιμαστεί, αν έχει δημοσιευθεί και αξιολογηθεί από ειδικούς του είδους, αν είναι γνωστό το πιθανό ποσοστό σφάλματος και βρίσκεται εντός αποδεκτού πλαισίου και τέλος αν αποτελεί αντικείμενο ευρείας αποδοχής από τη σχετική επιστημονική κοινότητα[50].

Κρίνεται συνεπώς αναγκαίο να αποκρυσταλλωθεί η ακολουθητέα μεθοδολογία εγκληματολογικής εξέτασης ψηφιακών πειστηρίων στο υπολογιστικό νέφος, πράγμα ιδιαίτερα δύσκολο λόγω της ραγδαίας εξέλιξης της τεχνολογίας που εφαρμόζεται σ' αυτό (νέφος), και εν συνεχεία να τεκμηριωθεί κατάλληλα ώστε να είναι αποδεκτή κατά τη δικαστική διαδικασία. Επί του παρόντος δεν υπάρχει ένα αποδεκτό πρότυπο για τη διεξαγωγή ερευνών στο υπολογιστικό νέφος, γεγονός που καθιστά προβληματική την παρουσίαση των συλλεχθέντων αποδεικτικών στοιχείων ενώπιον της δικαστικής διαδικασίας[51].

[50] U.S. Supreme Court, Daubert v. Merrell Dow Pharmaceuticals, Inc. 509 U.S. 579 (1993), διαθέσιμη εδώ : https://supreme.justia.com/cases/federal/us/509/579/case.pdf , σελ. 580

[51] Grispos, G., Storer, T., & Glisson, W., Calm before the storm: The challenges of cloud computing in digital forensics. International Journal of Digital Crime and Forensics, 2012, διαθέσιμο εδώ: https://arxiv.org/ftp/arxiv/papers/1410/1410.2123.pdf , σελ. 28–48

ΚΕΦΑΛΑΙΟ 5ο : ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗΣ ΑΝΑΛΥΣΗΣ ΨΗΦΙΑΚΩΝ ΠΕΙΣΤΗΡΙΩΝ ΣΕ ΠΕΡΙΒΑΛΛΟΝ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

Η εκθετικά αυξανόμενη χρήση των προσφερόμενων υπηρεσιών υπολογιστικού νέφους οδηγεί στην αντίστοιχη ανάγκη εγκληματολογικών ερευνών στο περιβάλλον αυτό (νέφος), όταν αυτό απαιτείται για τη διερεύνηση ενός εγκλήματος. Αυτού του είδους η εγκληματολογική έρευνα αντιμετωπίζει μια σειρά από προκλήσεις, που απορρέουν όχι μόνο από τις τεχνικές δυσκολίες και ιδιαιτερότητες, όπως αναλύθηκαν παραπάνω, αλλά και από τα νομικά ζητήματα που προκύπτουν κατά την προσπάθεια των αρχών επιβολής του νόμου να αποκτήσουν πρόσβαση στα ψηφιακά δεδομένα που αποτελούν πειστήρια τέλεσης ενός εγκλήματος και φιλοξενούνται από τους παρόχους υπηρεσιών υπολογιστικού νέφους σε «άγνωστη τοποθεσία».

Κατά την προσπάθεια, λοιπόν, των αρχών επιβολής του νόμου για τον εντοπισμό της προέλευσης μιας άδικης πράξης, και κατ΄ επέκταση του δράστη αυτής, εγείρονται ορισμένα νομικά ζητήματα που σχετίζονται με την ακολουθητέα διαδικασία για την απόκτηση πρόσβασης σε δεδομένα κίνησης, δεδομένα περιεχομένου, πληροφορίες συνδρομητή και οτιδήποτε άλλο καταστεί αναγκαίο και βρίσκεται αποθηκευμένο σε μια υποδομή υπολογιστικού νέφους.

Α. ΕΦΑΡΜΟΣΤΕΟ ΔΙΚΑΙΟ ΚΑΙ ΕΔΑΦΙΚΟΤΗΤΑ

Το υπολογιστικό νέφος εγείρει μια σειρά από προκλήσεις για την ποινική δικαιοσύνη, ιδίως σε σχέση με το εφαρμοστέο δίκαιο και τη δικαιοδοσία. Ένεκα της ιδιαίτερης δομής του, οι αρμόδιες για την έρευνα αρχές αντιμετωπίζουν το πρόβλημα του καθορισμού της δικαιοδοσίας και του νομικού καθεστώτος όπου υπάγονται τα δεδομένα που αποθηκεύονται σε αυτό (νέφος). Ένας πάροχος υπηρεσιών υπολογιστικού νέφους μπορεί να έχει την έδρα του σε μία τοποθεσία, να εφαρμόζει το νομικό καθεστώς έτερης δικαιοδοσίας και τα δεδομένα να αποθηκεύονται σε τοποθεσία τρίτης δικαιοδοσίας.

Λόγω της δομής και του τρόπου λειτουργίας του, οι υπηρεσίες που παρέχονται μέσω αυτού αφορούν σε μεγάλο ποσοστό διαβιβάσεις δεδομένων προσωπικού χαρακτήρα. Η διαβίβαση και αποθήκευση των δεδομένων του χρήστη σε κέντρα δεδομένων πραγματοποιείται χωρίς ο ίδιος να γνωρίζει την ακριβή τοποθεσία αυτών. Οι διατάξεις της οδηγίας 95/46/ΕΚ εφαρμόζονται στους παρόχους υπηρεσιών υπολογιστικού νέφους, όταν επεξεργάζονται δεδομένα προσωπικού χαρακτήρα τα οποία εμπίπτουν στο πεδίο της δικαιοδοσίας της ΕΕ και, αντίστοιχα, της εθνικής δικαιοδοσίας κράτους μέλους της ΕΕ[52].

Τα κριτήρια βάσει των οποίων προσδιορίζεται το εκάστοτε εφαρμοστέο δίκαιο ορίζονται στο άρθρο 4 της οδηγίας, το οποίο αναφέρεται στη νομοθεσία που διέπει τους υπεύθυνους της επεξεργασίας. Σύμφωνα με αυτό :

Κάθε κράτος μέλος εφαρμόζει τις εθνικές διατάξεις, που θεσπίζει δυνάμει της οδηγίας, σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφόσον:

α) η επεξεργασία εκτελείται στα πλαίσια των δραστηριοτήτων υπευθύνου εγκατεστημένου στο έδαφος του κράτους μέλους. Όταν ο ίδιος υπεύθυνος είναι εγκατεστημένος στο έδαφος περισσοτέρων του ενός κρατών μελών, πρέπει να λαμβάνει τα αναγκαία μέτρα ώστε να εξασφαλίζεται ότι κάθε εγκατάστασή του πληροί τις απαιτήσεις που προβλέπει η εφαρμοστέα εθνική νομοθεσία.

β) ο υπεύθυνος δεν είναι εγκατεστημένος στο έδαφος του κράτους μέλους, αλλά σε τόπο όπου εφαρμόζεται η εθνική του νομοθεσία δυνάμει του δημοσίου διεθνούς δικαίου.

γ) ο υπεύθυνος της επεξεργασίας δεν είναι εγκατεστημένος στο έδαφος της Κοινότητας και για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προσφεύγει σε μέσα, αυτοματοποιημένα ή όχι, ευρισκόμενα στο έδαφος του εν λόγω κράτους μέλους, εκτός εάν τα μέσα αυτά χρησιμοποιούνται μόνο με σκοπό τη διέλευση από το έδαφος της Ευρωπαϊκής Κοινότητας. Στην περίπτωση αυτή, ο υπεύθυνος της επεξεργασίας πρέπει να υποδείξει έναν αντιπρόσωπο εγκατεστημένο στο έδαφος του εν λόγω κράτους μέλους. Δεν θίγεται η τυχόν ανάληψη νομικών ενεργειών κατά του ιδίου του υπευθύνου της επεξεργασίας.

[52] Γνώμη 05/2012 της Ομάδας Εργασίας του άρθρου 29 για την προστασία των δεδομένων, «σχετικά με τη νεφοϋπολογιστική», 1η Ιουλίου 2012, διαθέσιμη εδώ : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_el.pdf

Στην πρώτη περίπτωση, το κριτήριο για την εφαρμογή της νομοθεσίας είναι η τοποθεσία και οι δραστηριότητες. Εφαρμόζεται, δηλαδή, το δίκαιο της χώρας στην οποία είναι εγκατεστημένος ο υπεύθυνος της επεξεργασίας των υπηρεσιών υπολογιστικού νέφους. Με τον όρο εγκατάσταση νοείται ο εξοπλισμός που χρησιμοποιεί ο πάροχος ο οποίος βρίσκεται σε χώρα της ΕΕ για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η παρουσία κέντρων δεδομένων αρκεί για να πληρείται η προϋπόθεση αυτή. Η γεωγραφική τοποθεσία του εξοπλισμού (κέντρα δεδομένων) που χρησιμοποιείται για την παροχή υπηρεσιών υπολογιστικού νέφους φαίνεται να είναι σημαντική για τον καθορισμό της εξαγωγής δεδομένων.

Στην τρίτη περίπτωση, εάν κάποιος χρήστης υπηρεσιών υπολογιστικού νέφους βρίσκεται εκτός Ε.Ε. αλλά ο πάροχος είναι εγκατεστημένος εντός τότε η νομοθεσία που διέπει τον πάροχο επεκτείνεται και στον χρήστη.

Συνεπώς, όταν ο πάροχος υπηρεσιών υπολογιστικού νέφους είναι εγκατεστημένος σε ένα ή περισσότερα κράτη μέλη της Ευρωπαϊκής Ένωσης και παρέχει όλες τις υπηρεσίες του από αυτά τα κράτη, είναι ξεκάθαρο ότι υπόκειται στους κανόνες και στην νομοθεσία της Ευρωπαϊκής Ένωσης για την προστασία προσωπικών δεδομένων. Όταν όμως ο πάροχος, δεν είναι εγκατεστημένος εντός της Ευρωπαϊκής Ένωσης απαιτείται ανάλυση και εξέταση της εκάστοτε κατάστασης λαμβάνοντας υπ΄ όψιν τον ρόλο και τις δραστηριότητές του παρόχου, ώστε να καθοριστεί η εφαρμοστέα νομοθεσία[53].

Β. ΔΙΕΘΝΗΣ ΔΙΑΒΙΒΑΣΗ ΔΕΔΟΜΕΝΩΝ

Το άρθρο 25 της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών[54] προβλέπει τις εξής βασικές αρχές ως προς τη διαβίβαση δεδομένων:

---

[53] Μήτρου Λ., Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος, Στο Περιοδικό ΔιΜΕΕ, Τεύχος 4/2015

[54] Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, αριθ. L 281 της 23/11/1995, διαθέσιμη εδώ: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:el:HTML

1. Τα κράτη μέλη προβλέπουν ότι η διαβίβαση προς τρίτη χώρα δεδομένων προσωπικού χαρακτήρα, που έχουν υποστεί επεξεργασία ή πρόκειται να υποστούν επεξεργασία μετά τη διαβίβασή τους, επιτρέπεται μόνον εάν, τηρουμένων των εθνικών διατάξεων που θεσπίζονται σύμφωνα με τις λοιπές διατάξεις της παρούσας οδηγίας, η εν λόγω τρίτη χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας.
2. Η επάρκεια της προστασίας που παρέχεται από τρίτη χώρα σταθμίζεται λαμβανομένων υπ' όψιν όλων των περιστάσεων που επηρεάζουν μια διαβίβαση ή κατηγορία διαβιβάσεων δεδομένων, ειδικότερα, εξετάζονται η φύση των δεδομένων, οι σκοποί και η διάρκειά της ή των προβλεπομένων επεξεργασιών, η χώρα προέλευσης και τελικού προορισμού, οι γενικοί ή τομεακοί κανόνες δικαίου, οι επαγγελματικοί κανόνες και τα μέτρα ασφαλείας που ισχύουν στην εν λόγω τρίτη χώρα.
3. Τα κράτη μέλη και η Επιτροπή ενημερώνονται αμοιβαία οσάκις θεωρούν ότι μια τρίτη χώρα δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας κατά την έννοια της παραγράφου 2.
4. Όταν η Επιτροπή διαπιστώνει, με τη διαδικασία που αναφέρεται στο άρθρο 31 παράγραφος 2, ότι μια τρίτη χώρα δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας κατά την έννοια της παραγράφου 2 του παρόντος άρθρου, τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα ώστε να αποφευχθεί οποιαδήποτε διαβίβαση τέτοιου είδους δεδομένων προς την εν λόγω τρίτη χώρα.
5. Η Επιτροπή αρχίζει την κατάλληλη στιγμή διαπραγματεύσεις ώστε να επανορθωθεί η κατάσταση που προκύπτει από τη διαπίστωση που έχει γίνει κατ' εφαρμογή της παραγράφου 4.
6. Η Επιτροπή μπορεί να αποφανθεί, με τη διαδικασία που αναφέρεται στο άρθρο 31 παράγραφος 2, ότι μια τρίτη χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας κατά την έννοια της παραγράφου 2 του παρόντος άρθρου, λόγω της εσωτερικής της νομοθεσίας ή των διεθνών δεσμεύσεων που έχει αναλάβει, ιδίως κατόπιν των διαπραγματεύσεων που αναφέρονται στην παράγραφο 5, ώστε να εξασφαλίζει την προστασία της ιδιωτικής ζωής και των θεμελιωδών ελευθεριών και δικαιωμάτων των προσώπων.

Με το άρθρο 26 της οδηγίας προβλέπονται ορισμένες περιπτώσεις εξαιρέσεων από τις ανωτέρω αρχές ως εξής:

1. Κατά παρέκκλιση από το άρθρο 25, και με την επιφύλαξη αντιθέτων διατάξεων της εθνικής νομοθεσίας που διέπουν κατ' ιδίαν περιπτώσεις, τα κράτη μέλη προβλέπουν ότι η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα που δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας κατά την έννοια του άρθρου 25 παράγραφος 2, μπορεί να πραγματοποιηθεί εφόσον:

α) το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει συναινέσει ρητώς στη διαβίβαση ή

β) η διαβίβαση είναι αναγκαία για την εκτέλεση σύμβασης μεταξύ του προσώπου στο οποίο αναφέρονται τα δεδομένα και του υπευθύνου επεξεργασίας ή για την εκτέλεση προσυμβατικών μέτρων ληφθέντων κατ' αίτηση του προσώπου αυτού ή

γ) η διαβίβαση είναι αναγκαία για τη συνομολόγηση ή την εκτέλεση σύμβασης που έχει συναφθεί ή πρόκειται να συναφθεί μεταξύ του υπευθύνου επεξεργασίας και τρίτου προς το συμφέρον του προσώπου στο οποίο αναφέρονται τα δεδομένα ή

δ) η διαβίβαση είναι αναγκαία ή απαιτείται εκ του νόμου για τη διασφάλιση σημαντικού δημοσίου συμφέροντος ή για την αναγνώριση, άσκηση ή υπεράσπιση ενός δικαιώματος ενώπιον του δικαστηρίου ή

ε) η διαβίβαση είναι αναγκαία για τη διασφάλιση ζωτικού συμφέροντος του προσώπου στο οποίο αναφέρονται τα δεδομένα ή

στ) η διαβίβαση πραγματοποιείται από δημόσιο μητρώο το οποίο προορίζεται βάσει νομοθετικών ή κανονιστικών διατάξεων για την παροχή πληροφοριών στο κοινό και είναι προσιτό είτε στο κοινό γενικά είτε σε οποιοδήποτε πρόσωπο μπορεί να αποδείξει έννομο συμφέρον, εφόσον στη συγκεκριμένη περίπτωση πληρούνται οι σχετικές νόμιμες προϋποθέσεις.

Σύμφωνα με τα ανωτέρω άρθρα της οδηγίας προβλέπεται συγκεκριμένο νομικό καθεστώς ως προς τις διασυνοριακές ροές το οποίο συνίσταται στα εξής :

Επιτρέπονται οι διαβιβάσεις δεδομένων σε χώρες, οι οποίες εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας με την επιφύλαξη της έγκρισης από την αρμόδια αρχή προστασίας δεδομένων ή βάσει απόφασης περί επάρκειας την οποία εκδίδει η Ευρωπαϊκή Επιτροπή (άρθρο 26 της Οδηγίας 95/46/ΕΚ). Αρκετοί εκ των παρόχων

υπηρεσιών υπολογιστικού νέφους έχουν προσχωρήσει οικειοθελώς στις Αρχές του Ασφαλούς Λιμένα (Safe Harbour Principles), το σύνολο δηλαδή των αρχών που εξέδωσε το Υπουργείο Εμπορίου των ΗΠΑ με στόχο τη διευκόλυνση της διαβίβασης δεδομένων σε εταιρείες εγκατεστημένες στις ΗΠΑ, το οποίο η Ευρωπαϊκή Επιτροπή ενέκρινε με την υπ΄ αρίθμ. 2000/520/ΕΚ Απόφαση της Επιτροπής της 26ης Ιουλίου 2000 βάσει της Οδηγίας 95/46/ΕΚ[55]. Ωστόσο, η ομάδα εργασίας του άρθρου 29 για την προστασία των προσώπων έναντι της επεξεργασίας των προσωπικών δεδομένων, η οποία αποτελεί ανεξάρτητο συμβουλευτικό όργανο για την προστασία των δεδομένων και της ιδιωτικής ζωής, που έχει συσταθεί βάσει του άρθρου 29 της οδηγίας για την προστασία των δεδομένων 95/46/ΕΚ, με αφορμή σχετικής απόφασης του Δικαστηρίου της Ευρωπαϊκής Ένωσης, εξέδωσε την 15 Οκτωβρίου 2015 ανακοίνωση[56] όπου μεταξύ άλλων αναφέρει πως είναι σαφές πλέον το γεγονός ότι οι διαβιβάσεις από την Ευρωπαϊκή Ένωση προς τις Ηνωμένες Πολιτείες της Αμερικής δεν μπορούν πλέον να πραγματοποιούνται με βάση την απόφαση περί επάρκειας της Ευρωπαϊκής Επιτροπής 2000/520/ΕΚ (τη λεγόμενη «απόφαση Ασφαλούς Λιμένα»). Η απόφαση του ΔΕΕ που προκάλεσε αυτή την αμφισβήτηση είναι η υπ΄ αρίθμ. C-362/14 της 6ης Οκτωβρίου 2015, έπειτα από αίτηση του High Court Irlande (Ιρλανδία) για την έκδοση προδικαστικής αποφάσεως — Maximillian Schrems κατά Data Protection Commissioner[57]. Συνοπτικά, το προδικαστικό ερώτημα που τέθηκε ήταν εάν σε περίπτωση όπου ενώπιον ανεξάρτητης αρχής, επιφορτισμένης εκ του νόμου με τη θέσπιση και εφαρμογή της νομοθεσίας περί προστασίας δεδομένων προσωπικού χαρακτήρα, κατατέθηκε καταγγελία σύμφωνα με την οποία δεδομένα προσωπικού χαρακτήρα διαβιβάζονται σε τρίτη χώρα (στην υπό κρίση υπόθεση, στις Ηνωμένες

[55] Απόφαση της Επιτροπής, της 26ης Ιουλίου 2000, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ, 2000/520/ΕΚ, Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, αριθ. L 215 της 25/08/2000, διαθέσιμη εδώ: http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32000D0520&qid=1488106864125&from=EL

[56] Ανακοίνωση της Ομάδας Εργασίας του άρθρου 29 για την προστασία των προσώπων έναντι της επεξεργασίας των προσωπικών δεδομένων, Βρυξέλες 16 Οκτωβρίου 2015, διαθέσιμη εδώ: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

[57] Απόφαση του Δικαστηρίου (τμήμα μείζονος συνθέσεως) της 6ης Οκτωβρίου 2015 [αίτηση του High Court της Ιρλανδίας για την έκδοση προδικαστικής αποφάσεως] — Maximillian Schrems κατά Data Protection Commissioner, Υπόθεση C-362/14, 30/11/2015, διαθέσιμη εδώ : http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62014CA0362&qid=1488114654054&from=EL

Πολιτείες Αμερικής) της οποίας η νομοθεσία και η πρακτική δεν παρέχουν ικανοποιητικό επίπεδο προστασίας στα υποκείμενα των δεδομένων, δεσμεύεται πλήρως η εν λόγω αρχή από τη διαπίστωση της Επιτροπής περί του αντιθέτου, όπως η διαπίστωση αυτή εκτίθεται στην απόφαση 2000/520/ΕΚ της Επιτροπής, ανεξαρτήτως των διατάξεων του άρθρου 25, παράγραφος 6, της οδηγίας 95/46/ΕΚ , ή επικουρικώς, μπορεί και/ή πρέπει η αρχή να διεξαγάγει τη δική της έρευνα ως προς το εν λόγω ζήτημα υπό το φως των πραγματικών εξελίξεων που επήλθαν. Ενώ στην απόφαση τονίζεται χαρακτηριστικά ότι η απόφαση 2000/520/ΕΚ είναι ανίσχυρη.

Προέκυψε, συνεπώς, η ανάγκη εξεύρεσης νέας νομικής και τεχνικής λύσης που θα επιτρέπει τις διαβιβάσεις δεδομένων στο έδαφος των Ηνωμένων Πολιτειών, σεβόμενες τα θεμελιώδη δικαιώματα. Μια τέτοια λύση για ένα νέο Ασφαλή Λιμένα θα μπορούσε να επιτευχθεί διαμέσου διαπραγματεύσεων για μια διακυβερνητική συμφωνία που θα παρέχει ισχυρότερες εγγυήσεις στους Ευρωπαίους πολίτες στους οποίους αναφέρονται τα δεδομένα. Έτσι, λοιπόν, με την υπ΄αρίθμ. 2016/2220 απόφαση του Συμβουλίου της 2ας Δεκεμβρίου 2016[58] ανακοινώθηκε η έγκριση για τη σύναψη συμφωνίας μεταξύ των Ηνωμένων Πολιτειών της Αμερικής και της Ευρωπαϊκής Ένωσης σχετικά με την προστασία των πληροφοριών προσωπικού χαρακτήρα για την πρόληψη, τη διερεύνηση, την ανίχνευση και τη δίωξη ποινικών αδικημάτων. Ως βάση για την συμφωνία αυτή τίθεται η υπ΄ αρίθμ. 2016/680 Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, και την κατάργηση της απόφασης-πλαισίου 2008/977/ΔΕΥ του Συμβουλίου[59].

---

[58] Απόφαση 2016/2220 του Συμβουλίου της Ευρωπαϊκής Ένωσης της 2ας Δεκεμβρίου 2016 για τη σύναψη, εξ ονόματος της Ευρωπαϊκής Ένωσης, της συμφωνίας μεταξύ των Ηνωμένων Πολιτειών της Αμερικής και της Ευρωπαϊκής Ένωσης σχετικά με την προστασία των πληροφοριών προσωπικού χαρακτήρα για την πρόληψη, τη διερεύνηση, την ανίχνευση και τη δίωξη ποινικών αδικημάτων, διαθέσιμη εδώ : http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016D2220&from=EN

[59] Οδηγία 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου, διαθέσιμη εδώ: http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L0680&qid=1488108374735&from=EL

Σύμφωνα με την οδηγία 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, η οδηγία 95/46 εφαρμόζεται σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα στα κράτη μέλη, τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Ωστόσο, δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία πραγματοποιείται στο πλαίσιο δραστηριοτήτων που δεν εμπίπτουν στο πεδίο εφαρμογής του κοινοτικού δικαίου, όπως δραστηριότητες στους τομείς της δικαστικής συνεργασίας σε ποινικές υποθέσεις και της αστυνομικής συνεργασίας. Στις περιπτώσεις αυτές εφαρμόζονται αυτά που ορίζει το 5ο κεφάλαιο της οδηγίας 2016/680 περί διαβίβασης δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες ή διεθνείς οργανισμούς.

Έτσι, λοιπόν, κατά το άρθρο 35 της οδηγίας που ορίζει τις γενικές αρχές που διέπουν τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα ισχύουν τα εξής:

1. Τα κράτη μέλη προβλέπουν ότι κάθε διαβίβαση, από αρμόδιες αρχές, δεδομένων προσωπικού χαρακτήρα τα οποία υποβάλλονται σε επεξεργασία ή προορίζονται να υποβληθούν σε επεξεργασία μετά τη διαβίβασή τους προς τρίτη χώρα ή διεθνή οργανισμό, συμπεριλαμβανομένων των περαιτέρω διαβιβάσεων προς άλλη τρίτη χώρα ή διεθνή οργανισμό, επιτρέπεται να πραγματοποιηθεί μόνον υπό την προϋπόθεση της τήρησης των εθνικών διατάξεων που θεσπίζονται σύμφωνα με τις λοιπές διατάξεις της παρούσας οδηγίας, μόνον εφόσον πληρούνται οι όροι που ορίζονται στο παρόν κεφάλαιο και συγκεκριμένα:

α) η διαβίβαση είναι αναγκαία για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους.

β) τα δεδομένα προσωπικού χαρακτήρα διαβιβάζονται σε υπεύθυνο επεξεργασίας σε τρίτη χώρα ή διεθνή οργανισμό που αποτελεί αρμόδια αρχή για τους ανωτέρω σκοπούς

γ) σε περίπτωση που τα δεδομένα προσωπικού χαρακτήρα διαβιβάζονται ή καθίστανται διαθέσιμα από άλλο κράτος μέλος, το εν λόγω κράτος μέλος έχει δώσει προηγουμένως την έγκρισή του για τη διαβίβαση σύμφωνα με το εθνικό του δίκαιο

δ) η Επιτροπή έχει προβεί σε απόφαση περί επάρκειας δυνάμει του άρθρου 36 ή, ελλείψει τέτοιας απόφασης, όταν έχουν παρασχεθεί ή υπάρχουν κατάλληλες

εγγυήσεις σύμφωνα με το άρθρο 37 ή, ελλείψει τόσο απόφασης περί επάρκειας δυνάμει του άρθρου 36 όσο και κατάλληλων εγγυήσεων σύμφωνα με το άρθρο 37, ισχύουν παρεκκλίσεις για ειδικές καταστάσεις σύμφωνα με το άρθρο 38, και

ε) σε περίπτωση περαιτέρω διαβίβασης σε άλλη τρίτη χώρα ή διεθνή οργανισμό, η αρμόδια αρχή που διενήργησε την αρχική διαβίβαση ή άλλη αρμόδια αρχή στο ίδιο κράτος μέλος επιτρέπει την περαιτέρω διαβίβαση, αφού λάβει δεόντως υπόψη όλους τους σχετικούς παράγοντες, συμπεριλαμβανομένων της σοβαρότητας του ποινικού αδικήματος, των σκοπών για τους οποίους διαβιβάστηκαν αρχικά τα δεδομένα προσωπικού χαρακτήρα και του επιπέδου προστασίας των δεδομένων στην τρίτη χώρα ή τον διεθνή οργανισμό στα οποία διαβιβάζονται περαιτέρω τα δεδομένα προσωπικού χαρακτήρα.

2. Τα κράτη μέλη προβλέπουν ότι οι διαβιβάσεις χωρίς την προηγούμενη έγκριση άλλου κράτους μέλους επιτρέπονται μόνον εφόσον η διαβίβαση των δεδομένων προσωπικού χαρακτήρα είναι απαραίτητη για την αποτροπή άμεσης και σοβαρής απειλής για τη δημόσια ασφάλεια κράτους μέλους ή τρίτης χώρας ή για τα ουσιώδη συμφέροντα κράτους μέλους και η προηγούμενη έγκριση δεν μπορεί να ληφθεί εγκαίρως. Η αρχή που είναι υπεύθυνη για την παροχή της προηγούμενης έγκρισης ενημερώνεται χωρίς καθυστέρηση.

Γ. ΧΡΟΝΙΚΟΣ ΠΕΡΙΟΡΙΣΜΟΣ ΔΙΑΤΗΡΗΣΗΣ ΔΕΔΟΜΕΝΩΝ

Με την οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)[60] καθορίστηκαν ειδικοί κανόνες με στόχο την εξασφάλιση του δικαιώματος στο απόρρητο των επικοινωνιών (άρθρο 5) και την υποχρέωση των παρόχων να διαγράφουν τα δεδομένα κίνησης όταν δεν είναι πλέον απαραίτητα για τον σκοπό της μετάδοσης της επικοινωνίας (άρθρο 6), εκτός εάν είναι απαραίτητα για τη χρέωση των συνδρομητών και την πληρωμή των διασυνδέσεων ή εφόσον ο περιορισμός αυτός

[60] Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 Σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες), διαθέσιμη εδώ : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:el:PDF

αποτελεί αναγκαίο, κατάλληλο και ανάλογο μέτρο σε μια δημοκρατική κοινωνία για τη διαφύλαξη της εθνικής ασφάλειας (δηλαδή της ασφάλειας του κράτους), της εθνικής άμυνας, της δημόσιας ασφάλειας, και για την πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών αδικημάτων ή της άνευ αδείας χρησιμοποίησης του συστήματος ηλεκτρονικών επικοινωνιών, όπως προβλέπεται στο άρθρο 13, παράγραφος 1 της οδηγίας 95/46/ΕΚ.

Σχετικά με το ίδιο θέμα εξεδόθη η οδηγία 2006/24/ΕΚ Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της 15ης Μαρτίου 2006 για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ[61]. Σύμφωνα με την οδηγία αυτή τα κράτη μέλη δεσμεύονται να διατηρούν για χρονικό διάστημα όχι μικρότερο του εξαμήνου και όχι μεγαλύτερο της διετίας ορισμένες κατηγορίες δεδομένων, όπως η ημερομηνία της επικοινωνίας, η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης με το Διαδίκτυο με βάση συγκεκριμένη ωριαία ζώνη, καθώς και η διεύθυνση πρωτοκόλλου του διαδικτύου (IP), που έδωσε στην επικοινωνία ο πάροχος υπηρεσιών πρόσβασης στο Διαδίκτυο, στοιχεία που για τη διερεύνηση ενός κυβερνοεγκλήματος θεωρούνται άκρως σημαντικά.

Η εν λόγω Οδηγία ενσωματώθηκε στην ελληνική νομοθεσία με το νόμο 3917/2011[62]. Στο άρθρο 6 του εν λόγω νόμου αναφέρει ότι τα δεδομένα του άρθρου 5 της Οδηγίας 2006/24/ΕΚ διατηρούνται επί 12 μήνες από την ημερομηνία της επικοινωνίας. Μετά το πέρας του ανωτέρω χρονικού διαστήματος τα δεδομένα αυτά καταστρέφονται με αυτοματοποιημένη διαδικασία από τον πάροχο.

[61] Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2006 για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ, διαθέσιμη εδώ : http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32006L0024&from=el

[62] Νόμος 3917, ΦΕΚ 22 - 21.02.2011, Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.

Δ. ΚΑΝΟΝΕΣ ΔΙΕΘΝΟΥΣ ΣΥΝΕΡΓΑΣΙΑΣ ΓΙΑ ΤΗΝ ΑΠΟΤΕΛΕΣΜΑΤΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΑΙ ΔΙΕΥΡΕΥΝΗΣΗ ΤΩΝ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΩΝ

Η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο που υπογράφηκε στη Βουδαπέστη στις 23 Νοεμβρίου 2001 και κυρώθηκε από την Ελλάδα με τον νόμο 4411 στις 3 Αυγούστου 2016 προβλέπει στα άρθρα 23 έως 35 ορισμένους κανόνες διεθνούς συνεργασίας. Ένας από τους στόχους της Σύμβασης είναι και η θέσπιση ενός γρήγορου και αποτελεσματικού συστήματος διεθνούς συνεργασίας μεταξύ των κρατών για την ταχεία και αποτελεσματική αντιμετώπιση των κυβερνοεγκλημάτων. Οι διατάξεις διεθνούς συνεργασίας αναφέρονται:

(α) στις γενικές αρχές που ισχύουν περί διεθνούς συνεργασίας (άρθρο 23),
(β) στην έκδοση (άρθρο 24),
(γ) σε κανόνες αμοιβαίας συνδρομής, οι οποίοι διακρίνονται:
(i) στις γενικές αρχές που ισχύουν περί αμοιβαίας συνδρομής (άρθρα 25-26),

(ii) στις διαδικασίες που ισχύουν σε αιτήματα αμοιβαίας συνδρομής σε περίπτωση απουσίας εφαρμοστέων διεθνών συμβάσεων (άρθρα 27-28),
(iii) σε ειδικές διατάξεις που αφορούν την αμοιβαία συνδρομή που σχετίζεται με προσωρινά μέτρα (άρθρα 29-30) καθώς και με ερευνητικά μέτρα (άρθρα 31-34),
(iv) στη σύσταση ενός δικτύου με συνεχόμενη λειτουργία (24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα) για τη διασφάλιση ταχείας συνδρομής μεταξύ των συμβαλλομένων μερών (άρθρο 35).
Πιο αναλυτικά:

1. Γενικές αρχές διεθνούς συνεργασίας (άρθρο 23)

   Το άρθρο 23 προωθεί τρεις γενικές αρχές σε σχέση με τη διεθνή συνεργασία: (α) η διεθνής συνεργασία παρέχεται μεταξύ των συμβαλλομένων μερών στο μέτρο του ευρύτερου δυνατού, (β) η συνεργασία εκτείνεται σε όλα τα ποινικά αδικήματα που σχετίζονται με ένα σύστημα υπολογιστή και δεδομένα, ή για τη συλλογή αποδεικτικών στοιχείων ενός ποινικού αδικήματος που βρίσκονται σε ηλεκτρονική μορφή και, (γ) η συνεργασία λαμβάνει χώρα σύμφωνα με τις διατάξεις της παρούσας Σύμβασης και μέσω της εφαρμογής των σχετικών διεθνών συμβάσεων για τη διεθνή συνεργασία σε ποινικά θέματα, αμοιβαίων διευθετήσεων μεταξύ των μερών και εσωτερικών νόμων περί διεθνούς συνεργασίας.

Γενικότερα, οι διατάξεις της Σύμβασης για διεθνή συνεργασία υπόκεινται σε υφιστάμενες διεθνείς συμφωνίες, καθώς και στο εσωτερικό δίκαιο των συμβαλλομένων μερών. Σχετικά με την αμοιβαία συνδρομή (άρθρο 25), στην παρ. 257 του Επεξηγηματικού Σημειώματος[63], επεξηγείται ότι κανένα περιοριστικό μέτρο, όπως η έρευνα και κατάσχεση, δεν εκτελείται για λογαριασμό ενός συμβαλλόμενου μέρους, εκτός αν δεν έχουν πρώτα ικανοποιηθεί οι βασικές προϋποθέσεις για την εφαρμογή ενός τέτοιου μέτρου στο εσωτερικό του δίκαιο.

2. Έκδοση (άρθρο 24)

Το άρθρο 24 αναφέρεται στην έκδοση εγκληματιών μεταξύ των συμβαλλομένων μερών της Σύμβασης. Η υποχρέωση της έκδοσης εφαρμόζεται μόνο για τα εγκλήματα που θεσπίζονται στα άρθρα 2 έως 11 της Σύμβασης με την προϋπόθεση ότι τιμωρούνται, σύμφωνα με τους νόμους και των δύο εμπλεκόμενων μερών, με στερητική της ελευθερίας ποινή διάρκειας τουλάχιστον ενός έτους (άρθρο 24 παρ. 1 στοιχ. α΄).

Στην περίπτωση που εφαρμόζεται μία διαφορετική ελάχιστη τιμωρία που έχει διευθετηθεί δυνάμει μίας ενιαίας ή αμοιβαίας νομοθεσίας ή μίας σύμβασης σχετικά με την έκδοση, συμπεριλαμβανομένης της Ευρωπαϊκής Σύμβασης για την έκδοση (1957), η οποία εφαρμόζεται μεταξύ δύο ή περισσοτέρων μερών, θα ισχύσει η ελάχιστη τιμωρία που παρέχεται στα πλαίσια αυτής της διευθέτησης ή σύμβασης (άρθρο 24 παρ. 1 στοιχ. β΄).

Τα ποινικά αδικήματα που περιγράφονται στην παρ. 1 του άρθρου 24 θα πρέπει να θεωρηθούν ότι περιλαμβάνονται στα αδικήματα εκδόσεως σε κάθε σύμβαση εκδόσεως που υφίσταται επί του παρόντος μεταξύ δύο ή περισσοτέρων μερών και θα πρέπει να συμπεριλαμβάνονται, ως τέτοια, σε κάθε μελλοντική σύμβαση εκδόσεως που θα καταρτίζεται μεταξύ τους (παρ. 2).

Αν ένα κράτος μέλος, για το οποίο η έκδοση υπόκειται σε υφιστάμενη συμφωνία, λάβει αίτημα εκδόσεως από ένα άλλο κράτος μέλος με το οποίο δεν έχει συνάψει συμφωνία εκδόσεως, μπορεί να θεωρήσει τη Σύμβαση για το

[63] Επεξηγηματικό Σημείωμα του Συμβουλίου σχετικά με την Σύμβαση για το κυβερνοέγκλημα, διαθέσιμο εδώ : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b , σελ. 45

Κυβερνοέγκλημα ως νομική βάση για την έκδοση, όσον αφορά τα ποινικά αδικήματα που προβλέπονται στην παρ. 1 του άρθρου αυτού (παρ. 3).

Τα μέρη για τα οποία η έκδοση δεν υπόκειται σε υφιστάμενη συμφωνία, θα αναγνωρίσουν τα ποινικά αδικήματα που προβλέπονται στην παρ. 1 του άρθρου αυτό, ως αδικήματα εκδόσεως μεταξύ τους (παρ. 4).

Η έκδοση θα υπόκειται στις προϋποθέσεις που προβλέπει το εσωτερικό δίκαιο του κράτους από το οποίο ζητείται η έκδοση ή στις εφαρμοστέες συμβάσεις εκδόσεως, συμπεριλαμβανομένων των λόγων για τους οποίους το μέρος προς το οποίο απευθύνεται η αίτηση μπορεί να την αρνηθεί (παρ. 5).

Αν αποκλειστικός λόγος άρνησης ενός αιτήματος έκδοσης για ένα ποινικό αδίκημα, κατά την παρ. 1 του άρθρου αυτού, αποτελεί μόνο η εθνικότητα του προσώπου του οποίου ζητείται η έκδοση, ή γιατί το προς ό η αίτηση μέρος θεωρεί ότι έχει αρμοδιότητα για το αδίκημα, το τελευταίο αυτό μέρος, κατόπιν αιτήσεως του αιτούντος μέρους, θα υποβάλει την υπόθεση στις αρμόδιες αρχές του για την άσκηση δίωξης και θα ενημερώσει το αιτούν μέρος για το τελικό αποτέλεσμα μέσα σε εύλογο χρονικό διάστημα. Οι αρμόδιες αρχές θα λάβουν την απόφασή τους και θα διενεργήσουν τις έρευνες και διαδικασίες κατά τον ίδιο τρόπο, όπως σε κάθε άλλη περίπτωση αδικήματος ανάλογης φύσης, σύμφωνα με το εσωτερικό δίκαιο του μέρους αυτού (παρ. 6)

3. Γενικές αρχές αμοιβαίας συνδρομής (άρθρο 25)
   i) Τα Συμβαλλόμενα Μέρη θα παρέχουν την ευρύτερη δυνατή αμοιβαία συνδρομή μεταξύ τους για την πραγματοποίηση ερευνών ή την άσκηση διώξεων σε περιπτώσεις ποινικών αδικημάτων σχετιζόμενων με συστήματα υπολογιστή και δεδομένων, ή για την συλλογή αποδεικτικών στοιχείων σε ηλεκτρονική μορφή που αφορούν σε ένα ποινικό αδίκημα.
   ii) Κάθε Συμβαλλόμενο Μέρος, θα λάβει επίσης, τα νομοθετικά και άλλα μέτρα που απαιτούνται για την εκτέλεση των υποχρεώσεων που καθορίζονται στα άρθρα 27 έως 35.
   iii) Κάθε Συμβαλλόμενο Μέρος, σε επείγουσες περιστάσεις, μπορεί να απευθύνει αιτήσεις αμοιβαίας συνδρομής ή σχετικά μηνύματα με γρήγορα μέσα επικοινωνίας όπως τηλεομοιοτυπία ή ηλεκτρονικό ταχυδρομείο υπό την προϋπόθεση ότι τα μέσα αυτά εξασφαλίζουν τα απαραίτητα επίπεδα ασφάλειας και γνησιότητας (συμπεριλαμβανόμενης και της χρήσης

κρυπτογραφίας στις περιπτώσεις που απαιτείται), και ότι θα επακολουθεί επίσημη επιβεβαίωση, όταν αυτή ζητείται από το μέρος, προς το οποίο απευθύνεται το αίτημα. Το Συμβαλλόμενο Μέρος, προς το οποίο απευθύνεται το αίτημα, θα αποδέχεται και θα απαντά στο αίτημα με οποιονδήποτε από τα γρήγορα μέσα επικοινωνίας.

iv) Εκτός εάν προβλέπεται διαφορετικά σε άρθρα του παρόντος κεφαλαίου, η αμοιβαία συνδρομή θα υπόκειται στις προϋποθέσεις που προβλέπονται από τους νόμους του Συμβαλλόμενου Μέρους, προς το οποίο απευθύνεται το αίτημα, ή από τις ισχύουσες συμβάσεις περί αμοιβαίας συνδρομής, περιλαμβανόμενων των λόγων για τους οποίους το Συμβαλλόμενο Μέρος, προς το οποίο απευθύνεται το αίτημα, μπορεί να αρνηθεί τη συνεργασία. Το Συμβαλλόμενο Μέρος, προς το οποίο απευθύνεται το αίτημα, δεν θα ασκεί το δικαίωμα άρνησης της αμοιβαίας συνδρομής για τα εγκλήματα που αναφέρονται στα άρθρα 2 έως 11 με μόνη αιτιολογία ότι το αίτημα αφορά ένα έγκλημα το οποίο θεωρεί ως φορολογικό.

v) Στην περίπτωση που σύμφωνα με τις διατάξεις του παρόντος άρθρου, το Συμβαλλόμενο Μέρος, προς το οποίο απευθύνεται το αίτημα, έχει το δικαίωμα να θέσει ως προϋπόθεση για την παροχή αμοιβαίας συνδρομής την ύπαρξη διπλού αξιόποινου, η προϋπόθεση αυτή θα θεωρείται ότι εκπληρώνεται, ασχέτως εάν οι νόμοι του κατατάσσουν το έγκλημα στην ίδια κατηγορία εγκλημάτων ή εάν περιγράφουν το έγκλημα με την ίδια ορολογία με το αιτούν Συμβαλλόμενο Μέρος, εάν η περιγραφόμενη συμπεριφορά για την οποία ζητείται η συνδρομή, αποτελεί ποινικό αδίκημα σύμφωνα με τους δικούς του νόμους.

Η παρ. 5 είναι πολύ σημαντική γιατί επιτρέπει στα συμβαλλόμενα μέρη να ερμηνεύσουν τον όρο του διττού αξιοποίνου, για τους σκοπούς της αμοιβαίας συνδρομής, με ένα πιο ευέλικτο τρόπο. Η διάταξη αυτή κρίθηκε αναγκαία δεδομένου των διαφορών μεταξύ των εθνικών νομικών συστημάτων όσον αφορά την ορολογία και την κατηγοριοποίηση των ποινικών αδικημάτων. Σύμφωνα με αυτή, εφόσον μία συμπεριφορά συνιστά ποινικό αδίκημα κατά το εσωτερικό δίκαιο και των δύο μερών, τέτοιες διαφορές τεχνικής φύσεως δεν θα έπρεπε να αποτελούν εμπόδιο για την παροχή αμοιβαίας συνδρομής.

4. Αυθόρμητη ενημέρωση (άρθρο 26)
   i) Κάθε Συμβαλλόμενο Μέρος, μέσα στα όρια του εσωτερικού του δικαίου και χωρίς προηγουμένως να του ζητηθεί, μπορεί να αποστείλει σε άλλο Συμβαλλόμενο Μέρος πληροφορίες που έχει λάβει στα πλαίσια των 105 δικών του ερευνών, όταν κρίνει ότι η γνωστοποίηση των πληροφοριών αυτών θα μπορούσε να βοηθήσει το Συμβαλλόμενο Μέρος, που λαμβάνει τις πληροφορίες, να ξεκινήσει ή να διενεργήσει έρευνες ή να ασκήσει διώξεις για ποινικά αδικήματα που θεμελιώνονται σύμφωνα με την παρούσα Σύμβαση ή που θα μπορούσαν να οδηγήσουν σε αίτημα συνεργασίας από εκείνο το Συμβαλλόμενο Μέρος δυνάμει του παρόντος κεφαλαίου.
   ii) Πριν χορηγήσει τις πληροφορίες αυτές, το παρέχον Συμβαλλόμενο Μέρος μπορεί να ζητήσει να τηρηθεί εμπιστευτικότητα ως προς αυτές ή να χρησιμοποιηθούν αυτές υπό όρους. Εάν το λαμβάνον Συμβαλλόμενο Μέρος δεν μπορεί να συμμορφωθεί με το αίτημα αυτό, πρέπει να ειδοποιεί σχετικά το παρέχον τις πληροφορίες Συμβαλλόμενο Μέρος, το οποίο στη συνέχεια θα κρίνει εάν οι πληροφορίες αυτές πρέπει να δοθούν. Εάν το λαμβάνον Συμβαλλόμενο Μέρος αποδεχθεί τις πληροφορίες με τους όρους αυτούς, τότε θα δεσμεύεται από αυτούς

5. Διαδικασίες που αφορούν τις αιτήσεις αμοιβαίας συνδρομής ελλείψει ισχυουσών διεθνών συμβάσεων (άρθρο 27)

   Σε περίπτωση που μεταξύ του αιτούντος και του Συμβαλλόμενου Μέρος, προς το οποίο απευθύνεται η αίτηση, δεν υπάρχει σύμβαση ή ρύθμιση αμοιβαίας συνδρομής στην βάση της ενιαίας ή αμοιβαίας νομοθεσίας, θα ισχύουν οι διατάξεις του παρόντος άρθρου. Οι διατάξεις αυτές δεν θα ισχύουν στην περίπτωση που υφίσταται τέτοιου είδους σύμβαση, ρύθμιση ή νομοθεσία, εκτός εάν τα Συμβαλλόμενα Μέρη συμφωνήσουν να εφαρμόσουν αντ' αυτών το σύνολο ή μέρος του υπόλοιπου του παρόντος άρθρου.

6. Κατεπείγουσα διατήρηση αποθηκευμένων δεδομένων υπολογιστών (άρθρο 29)
   i) Κάθε Συμβαλλόμενο Μέρος μπορεί να ζητήσει από ένα άλλο Συμβαλλόμενο Μέρος να διατάξει ή με άλλο τρόπο εξασφαλίσει την κατεπείγουσα διατήρηση δεδομένων που είναι αποθηκευμένα σε ένα

σύστημα υπολογιστή, το οποίο ευρίσκεται στην επικράτεια του άλλου Συμβαλλομένου Μέρους, για τα οποία το αιτούν Συμβαλλόμενο Μέρος προτίθεται να υποβάλει αίτηση αμοιβαίας συνδρομής με σκοπό την έρευνα ή με παρόμοιο τρόπο πρόσβαση, κατάσχεση, εξασφάλιση ή αποκάλυψη των δεδομένων.

ii) Κάθε αίτηση διατήρησης που υποβάλλεται σύμφωνα με την παράγραφο 1 πρέπει να αναφέρει: α. την αρχή που ζητεί την διατήρηση, β. το έγκλημα που αποτελεί το αντικείμενο της ποινικής έρευνας ή δίωξης και συνοπτική περιγραφή των συναφών πραγματικών περιστατικών, γ. τα προς διατήρηση αποθηκευμένα δεδομένα υπολογιστή και την σχέση τους με το έγκλημα, δ. κάθε διαθέσιμη πληροφορία που τακτοποιεί τον κατέχοντα τα αποθηκευμένα δεδομένα υπολογιστή ή τη θέση του συστήματος υπολογιστή, ε. την αναγκαιότητα της διατήρησης και στ. ότι το Συμβαλλόμενο Μέρος προτίθεται να υποβάλει αίτηση αμοιβαίας δικαστικής συνδρομής για την έρευνα ή με παρόμοιο τρόπο πρόσβαση, κατάσχεση, εξασφάλιση ή αποκάλυψη των αποθηκευμένων δεδομένων υπολογιστή.

iii) Με την λήψη της αίτησης από Συμβαλλόμενο Μέρος, το Συμβαλλόμενο Μέρος, προς το οποίο απευθύνεται η αίτηση, θα λάβει όλα τα αναγκαία μέτρα για την κατεπείγουσα διατήρηση των συγκεκριμένων δεδομένων, σύμφωνα με το εσωτερικό του δίκαιό. Για τους σκοπούς της ανταπόκρισης στην αίτηση, δεν θα απαιτείται η ύπαρξη διπλού αξιόποινου ως προϋπόθεση για την εν λόγω διατήρηση.

iv) Κάθε Συμβαλλόμενο Μέρος που έχει θέσει ως προϋπόθεση την ύπαρξη διπλού αξιοποίνου για την ανταπόκριση σε μία αίτηση για αμοιβαία συνδρομή με σκοπό την έρευνα ή τη με ανάλογο τρόπο πρόσβαση, κατάσχεση ή την με ανάλογο τρόπο εξασφάλιση ή γνωστοποίηση των αποθηκευμένων δεδομένων υπολογιστή, μπορεί, για εγκλήματα άλλα από εκείνα που ποινικοποιούνται σύμφωνα με τα Άρθρα 2 έως 11 της Σύμβασης, να διατηρήσει το δικαίωμα να αρνηθεί την ανταπόκριση στην αίτηση για διατήρηση δυνάμει του παρόντος άρθρου, στις περιπτώσεις που έχει λόγους να πιστεύει ότι κατά την στιγμή της γνωστοποίησης των δεδομένων δεν μπορεί να εκπληρωθεί η προϋπόθεση του διπλού αξιόποινου.

v) Επί πλέον, μία αίτηση για διατήρηση μπορεί να απορριφθεί μόνον εάν: α. η αίτηση αφορά έγκλημα το οποίο το Συμβαλλόμενο Μέρος, προς το οποίο απευθύνεται η αίτηση, χαρακτηρίζει ως πολιτικό έγκλημα ή έγκλημα που σχετίζεται με πολιτικό έγκλημα, ή β. Το Συμβαλλόμενο Μέρος, προς το οποίο απευθύνεται η αίτηση, θεωρεί ότι η αποδοχή της αίτησης είναι πιθανόν να θίξει την κυριαρχία, την ασφάλεια, την δημόσια τάξη ή άλλα θεμελιώδη συμφέροντά του.

vi) Στην περίπτωση που το Συμβαλλόμενο Μέρος, προς το οποίο απευθύνεται η αίτηση, θεωρεί ότι η διατήρηση δεν θα εξασφαλίσει την μελλοντική διαθεσιμότητα των δεδομένων ή ότι θα απειλήσει την εμπιστευτικότητα ή άλλως θα βλάψει την έρευνα του αιτούντος Συμβαλλομένου Μέρους, θα ενημερώσει αμέσως σχετικά το αιτούν Συμβαλλόμενο Μέρος το οποίο θα κρίνει εάν η αίτηση θα πρέπει να γίνει αποδεκτή σε κάθε περίπτωση.

vii) Κάθε διατήρηση που πραγματοποιείται σε ανταπόκριση της αίτησης που αναφέρεται στην παράγραφο 1, θα γίνεται για χρονικό διάστημα όχι μικρότερο των εξήντα ημερών, με σκοπό να δοθεί η δυνατότητα στο αιτούν Συμβαλλόμενο Μέρος να υποβάλει αίτηση για την έρευνα ή με παρόμοιο τρόπο πρόσβαση, κατάσχεση ή με παρόμοιο τρόπο εξασφάλιση ή αποκάλυψη των δεδομένων. Μετά τη λήψη μιας τέτοιας αίτησης, τα δεδομένα θα συνεχίσουν να διατηρούνται μέχρι να εκδοθεί απόφαση επί της αίτησης αυτής.

7. Κατεπείγουσα γνωστοποίηση διατηρηθέντων δεδομένων κίνησης (άρθρο 30)

i) Σε περίπτωση που κατά τη διαδικασία αποδοχής του αιτήματος που υποβλήθηκε σύμφωνα με το Άρθρο 29 για διατήρηση δεδομένων κίνησης που αφορούν σε μια συγκεκριμένη επικοινωνία, το Συμβαλλόμενο Μέρος, προς το οποίο απευθύνεται η αίτηση, διαπιστώσει ότι ένας πάροχος υπηρεσιών σε άλλο Κράτος αναμίχθηκε στη διαβίβαση της επικοινωνίας, το Συμβαλλόμενο αυτό Μέρος θα γνωστοποιήσει κατεπειγόντως στο αιτούν Συμβαλλόμενο Μέρος επαρκή ποσότητα δεδομένων κίνησης για να ταυτοποιηθεί ο εν λόγω πάροχος υπηρεσιών και η διαδρομή μέσω της οποίας διαβιβάσθηκε η επικοινωνία αυτή.

ii) Η γνωστοποίηση των δεδομένων κίνησης δυνάμει της παραγράφου 1 μπορεί να απορριφθεί μόνον εάν: α. η αίτηση αφορά έγκλημα το οποίο το Συμβαλλόμενο Μέρος, προς το οποίο απευθύνεται η αίτηση, χαρακτηρίζει ως πολιτικό έγκλημα ή έγκλημα που σχετίζεται με πολιτικό έγκλημα ή β. Το Συμβαλλόμενο Μέρος, προς το οποίο απευθύνεται η αίτηση, θεωρεί ότι η εκτέλεση της αίτησης είναι πιθανόν να θίξει την κυριαρχία, την ασφάλεια, την δημόσια τάξη ή άλλα θεμελιώδη συμφέροντά του.

8. Αμοιβαία συνδρομή σχετικά με την πρόσβαση σε αποθηκευμένα δεδομένα υπολογιστή (άρθρο 31)

i) Κάθε Συμβαλλόμενο Μέρος μπορεί να ζητήσει από άλλο Συμβαλλόμενο Μέρος να ερευνήσει ή με παρόμοιο τρόπο αποκτήσει πρόσβαση, κατάσχει ή με παρόμοιο τρόπο εξασφαλίσει ή αποκαλύψει δεδομένα που είναι αποθηκευμένα σε ένα σύστημα υπολογιστή που βρίσκεται στην επικράτεια του Συμβαλλόμενου Μέρους, προς το οποίο απευθύνεται η αίτηση, περιλαμβανόμενων των δεδομένων που έχουν διατηρηθεί κατ' εφαρμογή του Άρθρου 29.

ii) Το Συμβαλλόμενο Μέρος, προς το οποίο απευθύνεται η αίτηση, θα ανταποκρίνεται στην αίτηση αυτή εφαρμόζοντας τις διεθνείς συμβάσεις, ρυθμίσεις και νόμους που αναφέρονται στο Άρθρο 23, και σύμφωνα με τις λοιπές σχετικές διατάξεις του παρόντος κεφαλαίου.

iii) Το αίτημα θα αντιμετωπίζεται σε κατεπείγουσα βάση όταν: α. λογίζεται βάσιμα ότι τα σχετικά δεδομένα είναι ιδιαίτερα ευάλωτα σε απώλεια ή τροποποίηση, ή β. οι συμβάσεις, ρυθμίσεις και νόμοι που αναφέρονται στην παράγραφο 2 προβλέπουν κατεπείγουσα συνεργασία.

9. Διασυνοριακή πρόσβαση σε αποθηκευμένα δεδομένα υπολογιστή, μετά από συναίνεση ή σε περίπτωση που αυτά είναι διαθέσιμα στο κοινό (άρθρο 32)

Κάθε Συμβαλλόμενο Μέρος μπορεί, χωρίς την εξουσιοδότηση του άλλου Συμβαλλομένου Μέρους: α. να έχει πρόσβαση σε αποθηκευμένα δεδομένα υπολογιστή που είναι διαθέσιμα στο κοινό (ανοικτή πηγή), ασχέτως της γεωγραφικής θέσης των δεδομένων, ή β. να αποκτήσει πρόσβαση ή να

λάβει, μέσω ενός συστήματος υπολογιστή στην επικράτειά του, δεδομένα υπολογιστή που είναι αποθηκευμένα σε άλλο Συμβαλλόμενο Μέρος, εάν το Συμβαλλόμενο Μέρος λάβει την νόμιμη και οικειοθελή συναίνεση του προσώπου που έχει την νόμιμη εξουσία να γνωστοποιεί τα δεδομένα στο Συμβαλλόμενο Μέρος μέσω του συστήματος υπολογιστή του.

10. Δικαστική συνδρομή για την συλλογή δεδομένων κίνησης σε πραγματικό χρόνο (άρθρο 33)
    i) Τα Συμβαλλόμενα Μέρη θα παρέχουν αμοιβαία συνδρομή για τη συλλογή σε πραγματικό χρόνο δεδομένων κίνησης σχετικά με συγκεκριμένες επικοινωνίες στην επικράτειά τους, που διαβιβάζονται μέσω ενός συστήματος υπολογιστή. Τηρουμένων των διατάξεων της παραγράφου 2, η εν λόγω συνδρομή θα διέπεται από τους όρους και τις διαδικασίες που προβλέπονται από το εσωτερικό δίκαιο.
    ii) Κάθε Συμβαλλόμενο Μέρος θα παρέχει παρόμοια συνδρομή τουλάχιστον αναφορικά με αδικήματα για τα οποία επιτρέπεται, η συλλογή δεδομένων κίνησης σε πραγματικό χρόνο σε παρόμοιες υποθέσεις σύμφωνα με το εσωτερικό του δίκαιο.

11. Αμοιβαία συνδρομή σχετικά με την άρση απορρήτου δεδομένων περιεχομένου (άρθρο 34)

    Τα Συμβαλλόμενα Μέρη θα παρέχουν αμοιβαία συνδρομή για την συλλογή ή καταγραφή σε πραγματικό χρόνο δεδομένων περιεχομένου σχετικά με συγκεκριμένες επικοινωνίες στην επικράτειά τους, που διαβιβάζονται μέσω ενός συστήματος υπολογιστή, στον βαθμό που επιτρέπεται από τις ισχύουσες συμβάσεις και το εσωτερικό τους δίκαιο.

12. Δίκτυο 24/7 (άρθρο 35)
    i) Κάθε Συμβαλλόμενο Μέρος θα ορίσει ένα σημείο επαφής που θα είναι διαθέσιμο σε εικοσιτετράωρη βάση, επτά ημέρες την εβδομάδα, έτσι ώστε να διασφαλίζεται η παροχή άμεσης συνδρομής σε περιπτώσεις έρευνας ή δίωξης αναφορικά με ποινικά αδικήματα σχετιζόμενα με συστήματα και δεδομένα υπολογιστή, ή με σκοπό την συλλογή των αποδεικτικών στοιχείων σε ηλεκτρονική μορφή για ένα ποινικό αδίκημα. Η εν λόγω

συνδρομή θα περιλαμβάνει την διευκόλυνση ή, εάν αυτό επιτρέπεται από το εσωτερικό δίκαιο και την πρακτική, την άμεση εφαρμογή των ακόλουθων μέτρων: α. την παροχή τεχνικών συμβουλών, β. τη διατήρηση των δεδομένων σύμφωνα με τα Άρθρα 29 και 30, γ. τη συλλογή αποδεικτικών στοιχείων, παροχή νομικής ενημέρωσης και τον εντοπισμό των υπόπτων.

ii) α. Το σημείο επαφής κάθε Συμβαλλομένου Μέρους θα είναι αρμόδιο να επικοινωνεί σε κατεπείγουσα βάση με το σημείο επαφής ενός άλλου Συμβαλλομένου Μέρους. β. Εάν το σημείο επαφής που θα ορίσει ένα Συμβαλλόμενο Μέρος δεν ανήκει στην αρχή (ή τις αρχές) του Συμβαλλόμενου αυτού Μέρους που είναι αρμόδια (ή αρμόδιες) για την παροχή αμοιβαίας συνδρομής ή για την έκδοση, το σημείο επαφής θα διασφαλίζει ότι είναι σε θέση να συντονίζεται με την αρχή (ή τις αρχές) αυτή (ή αυτές) σε κατεπείγουσα βάση.

iii) Κάθε Συμβαλλόμενο Μέρος θα εξασφαλίζει την ύπαρξη διαθέσιμου εκπαιδευμένου και καταρτισμένου προσωπικού για την διευκόλυνση της λειτουργίας του δικτύου

Ε. Η ΔΙΕΘΝΗΣ ΔΙΚΑΣΤΙΚΗ ΣΥΝΕΡΓΑΣΙΑ ΚΑΤΑ ΤΟ ΕΛΛΗΝΙΚΟ ΔΙΚΑΙΟ

Η διεθνής δικαστική συνεργασία σε ποινικές υποθέσεις ασκείται επί τη βάσει διακρατικών συμβάσεων διμερών ή πολυμερών και το Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων λειτουργεί εν προκειμένω ως συντονιστική και μεσολαβητική αρχή προς το σκοπό της πραγμάτωσης της συνεργασίας αυτής. Το μεγαλύτερο δε μέρος της συνεργασίας καταλαμβάνει η παροχή της δικαστικής συνδρομής (βοήθειας) των δικαστικών και εισαγγελικών αρχών της χώρας προς τις αντίστοιχες των αντισυμβαλλομένων χωρών και αντίστροφα. Για την υλοποίηση των στόχων του δικτύου, το Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων έχει ορίσει ως συνδέσμους δικαστές και εισαγγελείς των Εφετείων Αθηνών, Πειραιώς και Θεσσαλονίκης, δύο δικαστικούς υπαλλήλους της Εισαγγελίας Εφετών Αθηνών, καθώς και δύο υπαλλήλους της Κεντρικής Υπηρεσίας του Υπουργείου Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων[64].

[64] Διαδικτυακός τόπος του Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων, http://www.ministryofjustice.gr

Σύμφωνα με το εθνικό μας δίκαιο, τα αιτήματα αμοιβαίας δικαστικής συνδρομής διακινούνται όπως ορίζει το άρθρο 457 παρ. 1 του Κώδικα Ποινικής Δικονομίας, κατά το οποίο «οι αιτήσεις των ελληνικών δικαστικών Αρχών προς αλλοδαπές Αρχές για την εξέταση μαρτύρων και κατηγορουμένων, για την ενέργεια αυτοψίας και πραγματογνωμοσύνης και για την κατάσχεση πειστηρίων διαβιβάζονται από τον αρμόδιο εισαγγελέα εφετών στο Υπουργείο Δικαιοσύνης, που προκαλεί την εκτέλεσή τους μέσω του Υπουργείου Εξωτερικών με την τήρηση και των διεθνών συνθηκών και εθίμων. Σε επείγουσες περιπτώσεις οι αιτήσεις αυτές διαβιβάζονται και απευθείας στις επιτόπιες προξενικές Αρχές που ασκούν ανακριτικά καθήκοντα, ειδοποιείται όμως σχετικά το Υπουργείο Δικαιοσύνης». Από την άλλη πλευρά, σε ότι αφορά αιτήσεις ξένων δικαστικών Αρχών για ανακριτικές πράξεις, σύμφωνα με το άρθρο 458 του Κ.Π.Δ., αυτές «διαβιβάζονται από το Υπουργείο Δικαιοσύνης και εκτελούνται με παραγγελία του αρμόδιου εισαγγελέα εφετών από τον ανακριτή στην περιφέρεια του οποίου πρόκειται να διεξαχθεί η ανακριτική πράξη, εκτός αν αυτή αντιβαίνει στις διατάξεις του κώδικα ή του οργανισμού δικαστηρίων. Κατά τα λοιπά τηρούνται οι σχετικές διατάξεις του κώδικα, οι διεθνείς συνθήκες και τα έθιμα».

ΣΤ. ΕΥΡΩΠΑΪΚΟ ΈΝΤΑΛΜΑ ΣΥΛΛΗΨΗΣ

Το ευρωπαϊκό ένταλμα σύλληψης (ΕΕΣ) αποτελεί μια απλουστευμένη διασυνοριακή δικαστική διαδικασία παράδοσης προς τον σκοπό της άσκησης δίωξης ή της εκτέλεσης ποινής ή μέτρου στερητικού της ελευθερίας. Ένταλμα σύλληψης που έχει εκδοθεί από δικαστική αρχή κράτους μέλους της ΕΕ ισχύει σε ολόκληρη την επικράτεια της ΕΕ. Το ευρωπαϊκό ένταλμα σύλληψης έχει τεθεί σε εφαρμογή κατόπιν της υπ΄ αρίθμ. 2002/584/ΔΕΥ Απόφασης-πλαίσιο του Συμβουλίου, για το ευρωπαϊκό ένταλμα σύλληψης και τις διαδικασίες παράδοσης μεταξύ των κρατών μελών[65], αντικαθιστώντας τις χρονοβόρες διαδικασίες έκδοσης που ακολουθούνταν κατά το παρελθόν μεταξύ των κρατών μελών της. Το ευρωπαϊκό ένταλμα σύλληψης όπως ορίζεται στο άρθρο 1 παρ. 1 της απόφασης «είναι δικαστική απόφαση η οποία εκδίδεται από κράτος μέλος προς το σκοπό της σύλληψης και της παράδοσης από άλλο κράτος

[65] Απόφαση-πλαίσιο του Συμβουλίου, της 13ης Ιουνίου 2002, για το ευρωπαϊκό ένταλμα σύλληψης και τις διαδικασίες παράδοσης μεταξύ των κρατών μελών - Δηλώσεις τις οποίες έκαναν ορισμένα κράτη μέλη με την ευκαιρία της έκδοσης της απόφασης-πλαισίου, 2002/584/ΔΕΥ, Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, αριθ. L 190 της 18/07/2002, διαθέσιμη εδώ : http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32002F0584&from=EL

μέλος προσώπου που καταζητείται για την άσκηση ποινικής δίωξης ή για την εκτέλεση ποινής ή μέτρου στερητικών της ελευθερίας».

Οι διαφορές του ευρωπαϊκού εντάλματος σύλληψης από την παραδοσιακή διαδικασία έκδοσης είναι οι εξής:

1. Αυστηρά χρονικά όρια.

   Το κράτος στο οποίο συλλαμβάνεται κάποιος υποχρεούται να επιστρέψει το πρόσωπο αυτό στο κράτος στο οποίο εκδόθηκε το ένταλμα εντός μέγιστης προθεσμίας 60 ημερών από τη σύλληψη. Εάν το πρόσωπο συναινεί στην παράδοσή του, η απόφαση παράδοσης πρέπει να ληφθεί εντός 10 ημερών.
2. Δεν απαιτείται πλέον διττό αξιόποινο της πράξης.

   Για 32 κατηγορίες σοβαρών αδικημάτων, δεν απαιτείται να χαρακτηρίζεται η πράξη ως ποινικό αδίκημα σε αμφότερες τις χώρες. Η μόνη απαίτηση που τίθεται είναι η πράξη να τιμωρείται με φυλάκιση τουλάχιστον 3 ετών στο κράτος μέλος έκδοσης του εντάλματος.
3. Δεν υπάρχει πολιτική ανάμειξη.

   Οι αποφάσεις λαμβάνονται αποκλειστικά από δικαστικές αρχές, χωρίς να υπεισέρχονται πολιτικές σκοπιμότητες.
4. Παράδοση υπηκόων.

   Τα κράτη μέλη της ΕΕ δεν μπορούν πλέον να αρνούνται την παράδοση δικών τους υπηκόων, εκτός εάν αναλαμβάνουν τα ίδια την εκτέλεση της ποινής φυλάκισης του καταζητούμενου.
5. Εγγυήσεις.

   Το κράτος που εκτελεί το ένταλμα μπορεί να ζητήσει εγγυήσεις περί του ότι: α) Αν η επιβληθείσα ποινή είναι ισόβια κάθειρξη ή στέρηση της ελευθερίας εφ' όρου ζωής, το πρόσωπο θα έχει, έπειτα από ορισμένο χρονικό διάστημα, το δικαίωμα να ζητήσει την επανεξέταση της ποινής και β) Το καταζητούμενο πρόσωπο θα μπορεί να εκτίσει την ποινή που θα απαγγελθεί εναντίον του στο κράτος το οποίο προβαίνει στην παράδοση του καταζητούμενου προσώπου, εφόσον το εν λόγω πρόσωπο είναι υπήκοος ή κάτοικος του κράτους αυτού.
6. Περιορισμένοι λόγοι άρνησης.

   Κράτος μπορεί να αρνηθεί να παραδώσει το καταζητούμενο πρόσωπο μόνον εάν συντρέχει κάποιος από τους λόγους προαιρετικής ή υποχρεωτικής άρνησης:

Υποχρεωτικοί λόγοι:

- το πρόσωπο έχει ήδη δικασθεί για το ίδιο αδίκημα
- ανηλικότητα (το πρόσωπο δεν έχει συμπληρώσει την απαιτούμενη ελάχιστη ηλικία για να θεωρείται ποινικώς υπεύθυνο στο κράτος στο οποίο συνελήφθη)
- αμνηστία (το κράτος στο οποίο συνελήφθη το πρόσωπο θα μπορούσε να είχε ασκήσει δίωξη για τη σχετική αξιόποινη πράξη και η αξιόποινη πράξη καλύπτεται από αμνηστία στο εν λόγω κράτος).

Προαιρετικοί λόγοι:

- έλλειψη διττού αξιοποίνου για αδικήματα πέραν των 32 που αναφέρονται παραπάνω
- δικαιοδοσία βάσει του τόπου τέλεσης της πράξης
- εκκρεμής ποινική διαδικασία στο κράτος εκτέλεσης του εντάλματος
- παραγραφή[66].

Το ευρωπαϊκό ένταλμα σύλληψης τέθηκε σε ισχύ στο εσωτερικό δίκαιο με το Ν. 3251/2004[67] και αποτελείται από 6 κεφάλαια και 39 άρθρα. Συνοπτικά, το πρώτο κεφάλαιο ασχολείται με τις γενικές διατάξεις του νόμου, το δεύτερο με τα θέματα έκδοσης του εντάλματος, το τρίτο με την εκτέλεσή του, το τέταρτο διαπραγματεύεται τους όρους παράδοσης του καταζητούμενου προσώπου, το πέμπτο υποδεικνύει τα επακόλουθα της προσαγωγής και το έκτο αναφέρεται στις τελικές διατάξεις του νόμου. Επίσης, με το Ν. 3251/2004 αποδίδεται η αρμοδιότητα για το ευρωπαϊκό ένταλμα σύλληψης σε τρεις δικαστικές αρχές :α) τον Εισαγγελέα Εφετών, β) το Εφετείο και γ) τον Άρειο Πάγο.

Ζ. Ο ΘΕΣΜΟΣ ΤΗΣ EUROJUST

Με την Απόφαση 2002/187/ΔΕΥ του Συμβουλίου, όπως τροποποιήθηκε από την Απόφαση 2009/426/ΔΕΥ του Συμβουλίου, της 16ης Δεκεμβρίου 2008 συστήθηκε η Eurojust, με σκοπό την ενίσχυση της καταπολέμησης των σοβαρών μορφών οργανωμένου εγκλήματος. Απαρτίζεται από ένα εθνικό μέλος από κάθε κράτος - μέλος, το οποίο αποσπάται

[66] Διαδικτυακός τόπος της Ευρωπαϊκής ηλεκτρονικής δικαιοσύνης, https://e-justice.europa.eu/content_european_arrest_warrant-90-el.do

[67] Νόμος 3251/2004, Ευρωπαϊκό ένταλμα σύλληψης, τροποποίηση του Ν. 2928/2001 για τις εγκληματικές οργανώσεις και άλλες διατάξεις, ΦΕΚ 127 - 09.07.2004

στην έδρα της, που έχει προσωρινά ορισθεί η Χάγη. Οι στόχοι της μονάδας είναι η προώθηση και βελτίωση του συντονισμού μεταξύ των αρμοδίων αρχών, όσον αφορά σε έρευνες και διώξεις εντός των κρατών - μελών και όπου εμπλέκονται τουλάχιστον δύο κράτη μέλη, καθώς και η υποστήριξη με κάθε τρόπο των αρχών αυτών στο έργο τους. Η Eurojust εκτελεί τα καθήκοντά της μέσω των εθνικών της μελών ή ως συλλογικό όργανο και δύναται να καλεί τις αρμόδιες αρχές των κρατών μελών να εξετάζουν το ενδεχόμενο να προβαίνουν σε διώξεις, να συστήνουν κοινές ομάδες έρευνας κλπ.

Η Eurojust συνεργάζεται με άλλους φορείς όπως την Europol, την Ευρωπαϊκή υπηρεσία καταπολέμησης της απάτης (OLAF), δύναται δε να συνάπτει συμφωνίες συνεργασίας και με αρχές τρίτων κρατών με σκοπό την καλύτερη δικαστική συνεργασία. Στο πλαίσιο αυτό συνεργάζεται στενά με το Ευρωπαϊκό Δικαστικό Δίκτυο. Η προστιθέμενη αξία της μονάδας αυτής στηρίζεται στην ύπαρξη μιας κεντρικής δομής, που μπορεί να εντοπίσει τα νομικά εμπόδια, τις καθυστερήσεις στην παροχή αμοιβαίας δικαστικής συνδρομής, αλλά και να συντονίσει σε εξέλιξη έρευνες σοβαρού οργανωμένου εγκλήματος. Εκπρόσωπος της χώρας μας στη Eurojust έχει οριστεί Αντεισαγγελέας Πρωτοδικών[68].

[68] Δικτυακός τόπος της Μονάδας Δικαστικής Συνεργασίας της Ευρωπαϊκής Ένωσης (Eurojust), http://www.eurojust.europa.eu/Pages/languages/el.aspx

ΕΠΙΛΟΓΟΣ

Όπως σαφώς προκύπτει από την έως τώρα ανάλυση, το υπολογιστικό νέφος καθιστά την συλλογή και ανάλυση των ψηφιακών αποδεικτικών μέσων ιδιαίτερα πολύπλοκη διαδικασία. Η εγκληματολογική ανάλυση ψηφιακών πειστηρίων απαιτεί περισσότερο χρόνο και προσπάθεια, από μια συμβατική ψηφιακή έρευνα, λόγω της πληθώρας των δεδομένων που απαιτούν εξέταση αναλογιζόμενη την απεριόριστη αποθηκευτική ικανότητα που παρέχει το νέφος στους χρήστες του. Επιπλέον, η ιδιαίτερη δομή του υπολογιστικού νέφους δεν επιτρέπει στον ερευνητή να αποκτήσει φυσική πρόσβαση στα ψηφιακά αποθηκευτικά μέσα όπου τηρούνται τα ερευνητέα δεδομένα και να λάβει ακριβή αντίγραφα αυτών τηρώντας την αλληλουχία των βημάτων που απαιτείται ώστε τα ληφθέντα πειστήρια να είναι αποδεκτά σε μια δικαστική διαδικασία.

Η πρόκληση της εγκληματολογικής εξέτασης ψηφιακών πειστηρίων εντείνεται ακόμη περισσότερο όταν τα προς διερεύνηση δεδομένα υπάγονται σε διαφορετικές δικαιοδοσίες. Στην περίπτωση αυτή, όπου τα δεδομένα αποθηκεύονται σε διαφορετικές χώρες, λόγω της ιδιαίτερης δομής του υπολογιστικού νέφους, απαιτούνται περίπλοκες και χρονοβόρες διαδικασίες για την ανταλλαγή των αιτούμενων δεδομένων μεταξύ των εμπλεκομένων χωρών. Οι καθυστερήσεις που προκύπτουν από τις διαδικασίες αυτές θα μπορούσαν δυνητικά να οδηγήσουν σε απώλεια δεδομένων, τα οποία διαγράφονται αυτοματοποιημένα προτού να τεθούν στη διάθεση του ερευνητή.

Όπως έχει αναφερθεί σε προηγούμενο κεφάλαιο, προς το παρόν δεν υπάρχουν τυποποιημένα και καθολικώς αποδεκτά πρότυπα διεξαγωγής εγκληματολογικής έρευνας σε περιβάλλον υπολογιστικού νέφους. Στις εν λόγω έρευνες εφαρμόζονται τα μοντέλα που έχουν καθοριστεί για τις συμβατικές μεθόδους ψηφιακής εγκληματολογίας, ωστόσο αυτές οι κατευθυντήριες γραμμές σε πολλές περιπτώσεις αποδεικνύονται ανεπαρκείς όταν εφαρμόζονται σε περιβάλλον υπολογιστικού νέφους. Προκύπτει συνεπώς η ανάγκη ανάπτυξης καθολικώς αποδεκτών μεθόδων και εργαλείων λογισμικού προς το σκοπό της επίτευξης ορθολογικής εγκληματολογικής εξέτασης ψηφιακών πειστηρίων.

Εν κατακλείδι

Η εγκληματολογική εξέταση ψηφιακών πειστηρίων στο υπολογιστικό νέφος πρέπει να συμβαδίζει με την ραγδαία τεχνολογική πρόοδο στον τομέα της πληροφορικής. Προκειμένου να επιτευχθεί ο σκοπός αυτός, είναι αναγκαίο να αξιολογηθούν οι διαδικασίες, τα εργαλεία και το νομικό πλαίσιο, ώστε να αναπτυχθούν καθολικώς αποδεκτά μοντέλα εγκληματολογικής έρευνας στο υπολογιστικό νέφος, τα οποία θα συμμορφώνονται με την ανάγκη παροχής αξιόπιστων και παραδεκτών αποδεικτικών μέσων. Επίσης, η ευρεία χρήση του υπολογιστικού νέφους εντείνει ακόμη περισσότερο την ανάγκη για μια αποτελεσματικότερη και ταχύτερη διεθνή συνεργασία προκειμένου να αντιμετωπισθούν οι νομικές προκλήσεις, όπως η «πολύ-δικαιοδοσία» των παρόχων υπολογιστικού νέφους, η κατάσχεση αποθηκευτικών μέσων και η ανταλλαγή δεδομένων μεταξύ χωρών. Οι αρχές επιβολής του νόμου θα πρέπει, λοιπόν, να «εφοδιαστούν» με τα κατάλληλα νομικά και τεχνικά εργαλεία προκειμένου να διεξάγουν αποτελεσματικά τις απαιτούμενες έρευνες στο περιβάλλον του υπολογιστικού νέφους, αλλά πρωτίστως χωρίς να παραβιάζουν την εκάστοτε εθνική νομοθεσία περί προστασίας των προσωπικών δεδομένων, διαφύλαξης της εμπιστευτικότητας και άλλων συγγενικών δικαιωμάτων των χρηστών.

ΒΙΒΛΙΟΓΡΑΦΙΑ – ΠΗΓΕΣ

Α. ΒΙΒΛΙΑ

- Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Academic Press, 2011
- Richard S. Michelson, Crime Scene Investigation: An Introduction to CSI, LawTech Publishing Group, 2015
- Rodney McKemmish, Advances in Digital Forensics IV, Chapter 1 - When is Digital Evidence Forensically Sound?, εκδ. Springer US, 2008
- Shahid Jamal Tubrazy, The Discovery of Digital Evidence and Forensic Laws (Theories and Practices), S J Tubrazy Publication, 2015
- W. J. Chisum, Crime Reconstruction and Evidence Dynamics στο The Forensic Laboratory Handbook Procedures and Practice , Humana Press, 2011

Β. ΆΡΘΡΑ

- Αγγελής Ι.Μ., «Η προς ψήφιση Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο: η σχέση της με την ελληνική έννομη τάξη», Νομική Επιθεώρηση, Αριθμός τεύχους 30, 2001
- Μήτρου Λ., Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος, Στο Περιοδικό ΔιΜΕΕ, Τεύχος 4/2015
- Παναγιώτα Εμμ. Περράκη, Νομιμότητα επεξεργασίας και μεταφοράς προσωπικών δεδομένων προς τρίτες χώρες. Ακύρωση της απόφασης «ασφαλούς λιμένα». Ρόλος και ανεξαρτησία εθνικών αρχών προστασίας προσωπικών δεδομένων. Έννοια επαρκούς/ικανοποιητικού επιπέδου προστασίας, Τριμηνιαίο νομικό περιοδικό : Ελληνική επιθεώρηση ευρωπαϊκού δικαίου, τόμος 35, 4/2015, σελ. 491-496
- Deevi Radha Rani, Sk. Nazma Sultana, Pasala Lourdu Sravani, Challenges of Digital Forensics in Cloud Computing Environment, Indian Journal of Science and Technology, 2016, διαθέσιμο εδώ: http://www.indjst.org/index.php/indjst/article/view/93051/69863
- Eric Slack, How do you know that “Delete” means Delete in Cloud, 2011, διαθέσιμο εδώ : http://www.storage-

switzerland.com/Articles/Entries/2011/8/16_How_do_you_know_that_Delete_means_Delete_in_Cloud_Storage.html

- Giuliano Giova, Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems, International Journal of Computer Science and Network Security, 2011, διαθέσιμο εδώ: http://paper.ijcsns.org/07_book/201101/20110101.pdf
- Grispos, G., Storer, T., & Glisson, W., Calm before the storm: The challenges of cloud computing in digital forensics, International Journal of Digital Crime and Forensics, 2012, διαθέσιμο εδώ: https://arxiv.org/ftp/arxiv/papers/1410/1410.2123.pdf
- Jawad Abbas, Studying the Documentation Process in Digital Forensic Investigation Frameworks / Models, Journal of Al-Nahrain University, 2015, διαθέσιμο εδώ: http://www.iasj.net/iasj?func=fulltext&aId=107014
- Lori M. Kaufman, Data Security in the World of Cloud Computing, IEEE Security & Privacy, 2009, διαθέσιμο εδώ: http://web.math.jjay.cuny.edu/fcm745/codes/SecurityCloudComputing.pdf
- Marcus K. Rogers, James Goldman, Rick Mislan, Timothy Wedge, Steve Debrota, Computer Forensics Field Triage Process Model, Journal of Digital Forensics, Security and Law, 2014, διαθέσιμο εδώ: http://ojs.jdfsl.org/index.php/jdfsl/article/view/222
- Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica and Matei Zaharia, A view of cloud computing, Communications of the ACM, 2010, διαθέσιμο εδώ: http://dl.acm.org/citation.cfm?id=1721672
- Sameera Abdulrahman Almulla, Youssef Iraqi, Andrew Jones, A STATE-OF-THE-ART REVIEW OF CLOUD FORENSICS, The Journal of Digital Forensics, Security and Law, 2014, διαθέσιμο εδώ : http://ojs.jdfsl.org/index.php/jdfsl/article/viewFile/253/234
- Sean Thorpe - Indrajit Ray, File Timestamps for Digital Cloud Investigations, Journal of Information Assurance and Security, 2011, διαθέσιμο εδώ : http://fenc-utech.net/scit/uploads/Paper52.pdf

Γ. ΠΡΑΚΤΙΚΑ ΣΥΝΕΔΡΙΩΝ – ΕΚΘΕΣΕΙΣ

- A Road Map for Digital Forensics στο Digital Forensics Research Conference, 2001, διαθέσιμο εδώ: http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf
- Keith Jeffery & Burkhard Neidecker-Lutz, The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010, European Commission, DG Information Society and Media, 2010, διαθέσιμο εδώ: https://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf
- Keyun Ruan, Joe Carthy, Tahar Kechadi and Mark Crosbie, Cloud Forensics - Advances in Digital Forensics VII, 2011, διαθέσιμο εδώ: https://link.springer.com/chapter/10.1007/978-3-642-24212-0_3#enumeration
- Sashank Dara, Cryptography Challenges for Computational Privacy in Public Clouds, IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), 2013, διαθέσιμο εδώ : https://eprint.iacr.org/2013/272.pdf
- The European Cloud Partnership Steering Board για την Ευρωπαϊκή Επιτροπή, «Establishing a Trusted Cloud Europe: A policy vision document by the Steering Board of the European Cloud Partnership», 2014, διαθέσιμο εδώ: http://ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe

Δ. ΕΓΧΕΙΡΙΔΙΑ

- Ενημερωτικό Σημείωμα MEMO/12/713 της Ευρωπαϊκής Επιτροπής με θέμα : «Εκμετάλλευση των δυνατοτήτων του υπολογιστικού νέφους (Cloud Computing) στην Ευρώπη – τι είναι και τι σημαίνει αυτό για μένα;», 2012, διαθέσιμο εδώ : http://europa.eu/rapid/press-release_MEMO-12-713_el.htm
- Ευρωπαϊκή Επιτροπή, Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης (OLAF), Guidelines on Digital Forensic Procedures for OLAF Staff, 15 Φεβρουαρίου 2016, διαθέσιμο εδώ : https://ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf
- Best Practices for Computer Forensics, Scientific Working Group on Digital Evidence (SWGDE), 2014, Διαθέσιμο εδώ: https://swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensics

- Digital evidence: standard and principles, Scientific Working Group on Digital Evidence (SWGDE) & International Organization on Digital Evidence (IOCE), 2000, διαθέσιμο εδώ : https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm
- Electronic Crime Scene Investigation: A Guide for First Responders, U.S. Department of Justice Office of Justice Programs National Institute of Justice, July 2001, διαθέσιμο εδώ : https://www.ncjrs.gov/pdffiles1/nij/219941.pdf
- Electronic evidence - a basic guide for First Responders, European Union Agency for Network and Information Security (ENISA), 2015, διαθέσιμο εδώ: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders
- Good Practice Guide for Digital Evidence, Association of Chief Police Officers, 2012, διαθέσιμο εδώ : http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
- Guide to Integrating Forensic Techniques into Incident Response: του National Institute of Standards and Technology (NIST), 2006, διαθέσιμο εδώ : http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf
- Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence, International Organization for Standardization, ISO/IEC 27037:2012, διαθέσιμο εδώ : https://www.iso.org/standard/44381.html
- Peter Mell & Timothy Grance, The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, Special Publication 800-145, 2011, διαθέσιμο εδώ : http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Ε. ΝΟΜΙΚΑ ΚΕΙΜΕΝΑ

- Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο, Βουδαπέστη, No.185, 23/11/2011, διαθέσιμη εδώ: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

- Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2006 για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ, διαθέσιμη εδώ : http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32006L0024&from=el
- U.S. Supreme Court, Daubert v. Merrell Dow Pharmaceuticals, Inc. 509 U.S. 579 (1993), διαθέσιμη εδώ: https://supreme.justia.com/cases/federal/us/509/579/case.pdf
- Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Ευρωπαϊκή Επιτροπή των Περιφερειών με τίτλο : «Προς την κατεύθυνση γενικής πολιτικής σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο», Βρυξέλλες, 22.5.2007, SEC(2007) 641 & 642, διαθέσιμη εδώ : http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52007DC0267&qid=1488508403454&from=EL
- Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, Αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους, COM/2012/0529 final, διαθέσιμο εδώ : http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52012DC0529&qid=1488501238624&from=EL
- Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, Προς μια ακμάζουσα οικονομία βασιζόμενη στα δεδομένα, COM/2014/0442 final, 2/7/2014, διαθέσιμη εδώ : http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52014DC0442&from=EN
- Ανακοίνωση της Ομάδας Εργασίας του άρθρου 29 για την προστασία των προσώπων έναντι της επεξεργασίας των προσωπικών δεδομένων, Βρυξέλες 16 Οκτωβρίου 2015, διαθέσιμη εδώ: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-

release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

- Απόφαση 2016/2220 του Συμβουλίου της Ευρωπαϊκής Ένωσης της 2ας Δεκεμβρίου 2016 για τη σύναψη, εξ ονόματος της Ευρωπαϊκής Ένωσης, της συμφωνίας μεταξύ των Ηνωμένων Πολιτειών της Αμερικής και της Ευρωπαϊκής Ένωσης σχετικά με την προστασία των πληροφοριών προσωπικού χαρακτήρα για την πρόληψη, τη διερεύνηση, την ανίχνευση και τη δίωξη ποινικών αδικημάτων, διαθέσιμη εδώ : http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016D2220&from=EN
- Απόφαση της Επιτροπής, της 26ης Ιουλίου 2000, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ, 2000/520/ΕΚ, Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, αριθ. L 215 της 25/08/2000, διαθέσιμη εδώ: http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32000D0520&qid=1488106864125&from=EL
- Απόφαση του Δικαστηρίου (τμήμα μείζονος συνθέσεως) της 6ης Οκτωβρίου 2015 [αίτηση του High Court της Ιρλανδίας για την έκδοση προδικαστικής αποφάσεως] — Maximillian Schrems κατά Data Protection Commissioner, Υπόθεση C-362/14, 30/11/2015, διαθέσιμη εδώ : http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62014CA0362&qid=1488114654054&from=EL
- Απόφαση-πλαίσιο του Συμβουλίου, της 13ης Ιουνίου 2002, για το ευρωπαϊκό ένταλμα σύλληψης και τις διαδικασίες παράδοσης μεταξύ των κρατών μελών - Δηλώσεις τις οποίες έκαναν ορισμένα κράτη μέλη με την ευκαιρία της έκδοσης της απόφασης-πλαισίου, 2002/584/ΔΕΥ, Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, αριθ. L 190 της 18/07/2002, διαθέσιμη εδώ : http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32002F0584&from=EL
- Γνώμη 05/2012 της Ομάδας Εργασίας του άρθρου 29 για την προστασία των δεδομένων, «σχετικά με τη νεφοϋπολογιστική», 1η Ιουλίου 2012, διαθέσιμη

εδώ : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_el.pdf

- Επεξηγηματικό Σημείωμα του Συμβουλίου σχετικά με την Σύμβαση για το κυβερνοέγκλημα, διαθέσιμο εδώ : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b
- Ευρωπαϊκή Επιτροπή - Δελτίο Τύπου, «Η ευρωπαϊκή πρωτοβουλία για το υπολογιστικό νέφος θα δώσει στην Ευρώπη το παγκόσμιο προβάδισμα στη βασιζόμενη στα δεδομένα οικονομία», 2016, διαθέσιμο εδώ: http://europa.eu/rapid/press-release_IP-16-1408_el.htm
- Νόμος 2225/1994, ΦΕΚ 121 – 20/07/1994, «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις»
- Νόμος 3251/2004, Ευρωπαϊκό ένταλμα σύλληψης, τροποποίηση του Ν. 2928/2001 για τις εγκληματικές οργανώσεις και άλλες διατάξεις, ΦΕΚ 127 – 09/07/2004
- Νόμος 4411, ΦΕΚ 142 - 03.08.2016, Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών - Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις
- Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 Σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες), διαθέσιμη εδώ : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:el:PDF
- Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την

αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, L 218/8 Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης

- Οδηγία 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου, διαθέσιμη εδώ: http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L0680&qid=1488108374735&from=EL
- Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, αριθ. L 281 της 23/11/1995, διαθέσιμη εδώ: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:el:HTML
- Π.Δ. 178/2014, ΦΕΚ 281 - 31.12.2014, «Οργάνωση Υπηρεσιών Ελληνικής Αστυνομίας»
- Π.Δ. 47/2005, ΦΕΚ 64 – 10/03/2005 «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του»
- Υπ' αρίθμ. 8770/16 σχέδιο συμπερασμάτων του Συμβουλίου της Ευρωπαϊκής Ένωσης και σχέδιο δράσης για τα επόμενα βήματα με στόχο τη δημιουργία Ευρωπαϊκού Εγκληματολογικού Χώρου, 24 Μαΐου 2016, διαθέσιμο εδώ : http://data.consilium.europa.eu/doc/document/ST-8770-2016-INIT/el/pdf

ΣΤ. ΔΙΑΔΙΚΤΥΑΚΕΣ ΠΗΓΕΣ

- Διαδικτυακός τόπος της Ανεξάρτητης Αρχής «Συνήγορος του καταναλωτή», Ενημέρωση του Καταναλωτή για την προστασία από το ηλεκτρονικό έγκλημα, 2008, διαθέσιμο εδώ : http://www.synigoroskatanaloti.gr/docs/info/info-Hlektroniko-Egklima.pdf
- Διαδικτυακός τόπος της Ελληνικής Αστυνομίας, http://www.astynomia.gr

- Διαδικτυακός τόπος της Ευρωπαϊκής Επιτροπής - Trusted Cloud Europe Survey, http://ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe-survey
- Διαδικτυακός τόπος της Ευρωπαϊκής ηλεκτρονικής δικαιοσύνης, https://e-justice.europa.eu/content_european_arrest_warrant-90-el.do
- Διαδικτυακός τόπος του Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων, http://www.ministryofjustice.gr
- Διαδικτυακός τόπος της Μονάδας Δικαστικής Συνεργασίας της Ευρωπαϊκής Ένωσης (Eurojust), http://www.eurojust.europa.eu
- Διαδικτυακός τόπος της Interpol, https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime