ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

ΣΧΟΛΗ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ, ΕΠΙΚΟΙΝΩΝΙΑΣ &ΠΟΛΙΤΙΣΜΟΥ

ΤΜΗΜΑ ΔΙΕΘΝΩΝ, ΕΥΡΩΠΑΪΚΩΝ & ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΕΘΝΕΣ & ΕΥΡΩΠΑΪΚΟ ΔΙΚΑΙΟ &ΔΙΑΚΥΒΕΡΝΗΣΗ

ΕΙΔΙΚΕΥΣΗ : «ΕΥΡΩΠΑΪΚΟ ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ ΚΑΙ ΠΟΛΙΤΙΚΗ»

«Ζητήματα ανταλλαγής πληροφοριών και συλλογής αποδεικτικών στοιχείων στο πλαίσιο της αστυνομικής συνεργασίας σε ποινικές υποθέσεις στην Ευρωπαϊκή Ένωση: Η σχέση μεταξύ της Ευρωπαϊκής Εντολής Έρευνας και της Ευρωπαϊκής Εντολής Υποβολής και Διατήρησης Ηλεκτρονικών Αποδεικτικών Στοιχείων»

"Intelligence and evidence-gathering issues in police cooperation in criminal cases within the European Union: The relationship between the European Investigation Order and the European Electronic Evidence Production and Preservation Order"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Νικόλαος Γεωργιτσόπουλος

Επιβλέπουσα: Επίκουρη Καθηγήτρια κ. Όλγα Τσόλκα

Αθήνα, 2023

Τριμελής Επιτροπή:

1. Τσόλκα Όλγα, Καθηγήτρια Πάντειου Πανεπιστημίου (Επιβλέπουσα)
2. Πασσάς Αργύριος, Καθηγητής Πάντειου Πανεπιστημίου
3. Πλατιάς Χρήστος, Καθηγητής Πάντειου Πανεπιστημίου

Copyright Νικόλαος Φ. Γεωργιτσόπουλος, 2023

All rights reserved. Με επιφύλαξη παντός δικαιώματος.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας διπλωματικής εργασίας εξ' ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της διπλωματικής εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Η έγκριση της διπλωματικής εργασίας από το Πάντειον Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών δεν δηλώνει αποδοχή των γνωμών του συγγραφέα.

Υπεύθυνη Δήλωση

Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης

Δηλώνω ότι η παρούσα εργασία είναι αποτέλεσμα πρωτότυπης έρευνας και δε χρησιμοποιεί πνευματική ιδιοκτησία τρίτων χωρίς αναφορές. Αναλαμβάνω δε όλες τις προβλεπόμενες νομικές και διοικητικές συνέπειες, σε περίπτωση που η εργασία μου τυχόν αποδειχθεί ότι αποτελεί προϊόν λογοκλοπής.

Ο δηλών

Γεωργιτσόπουλος Φ. Νικόλαος

Αφιερώσεις

Την παρούσα διπλωματική εργασία θα ήθελα να την αφιερώσω στην γιαγιά μου και στον παππού μου που έφυγαν πρόσφατα από τη ζωή σε απόσταση λίγων μηνών μεταξύ τους. Πάντα χαιρόντουσαν και καμάρωναν για τις επιτυχίες μου. Λυπάμαι που δε θα είναι παρόντες για να τους γεμίσω χαρά ακόμα μία φορά.

Συντομογραφίες

ΔΕΕ: Δικαστήριο της Ευρωπαϊκής Ένωσης

ΕΕΕ: Ευρωπαϊκή Εντολή Έρευνας

ΕΕΥποβ.: Ευρωπαϊκή Εντολή Υποβολής ηλεκτρονικών αποδεικτικών στοιχείων

ΕΕΔιατ.: Ευρωπαϊκή Εντολή Διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων

ΠροτΚανονισμού: Πρόταση Κανονισμού

ΠροτΟδηγίας: Πρόταση Οδηγίας

ΧΘΔΕΕ: Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

Ευχαριστίες

Μέσα από τη παρούσα ενότητα της παρούσας διπλωματικής εργασίας θα ήθελα να ευχαριστήσω μία σειρά προσώπων που με το δικό τους τρόπο, άμεσο ή έμμεσο συνέβαλαν στην περάτωση του παρόντος επιστημονικού εγχειρήματος.

Γνωρίζοντας ότι οι διπλωματικές εργασίες παραμένουν εσαεί δημοσιευμένες στην ηλεκτρονική πλατφόρμα του Πάντειου Πανεπιστήμιου «Πάνδημος», η ενότητα των ευχαριστιών είναι πάντοτε μία καλή ευκαιρία για την αποτύπωση σκέψεων και ευχαριστιών που θα μείνουν για πάντα αποτυπωμένες σε ένα επιστημονικό κείμενο στο πέρασμα του χρόνου και μπορεί να ανατρέξει ο κάθε ένας. Κάθε διπλωματική εργασίας διέρχεται από ορισμένα στάδια και εν τέλει ολοκληρώνεται.

Θερμές ευχαριστίες θα ήθελα να αποδώσω σε όλους τους συμφοιτητές μου κατά την διάρκεια του ακαδημαϊκού έτους 2021-22 ήμασταν συνοδοιπόροι στα μαθήματα του παρόντος μεταπτυχιακού προγράμματος σπουδών. Την παράθεση των ευχαριστιών θα ήθελα να ολοκληρώσω εκφράζοντας τις ευχαριστίες μου προς τους διδάσκοντες του μεταπτυχιακού προγράμματος σπουδών για τις γνώσεις και την διδασκαλία που μας προσέφεραν σε αυτό το ταξίδι γνώσης.

Ιδιαίτερες ευχαριστίες θα ήθελα να αποδώσω στην επιβλέπουσα της διπλωματικής μου εργασίας κ. Τσόλκα Όλγα για την αποδοχή μου και την στήριξη της στην παρακολούθηση του εν λόγω προγράμματος μεταπτυχιακών σπουδών στο οποίο διδάσκει αλλά και για τις γνώσεις που μας μετέφερε γύρω από την διαμόρφωση του ευρωπαϊκού ποινικού δικαίου.

Περιεχόμενα

Περίληψη

Στην παρούσα διπλωματική εργασία, γίνεται μία παρουσίαση του πλαισίου μέσα στο οποίο η Ένωση και τα κράτη μέλη καλούνται να αιτηθούν και να συλλέξουν ηλεκτρονικά αποδεικτικά στοιχεία. Το ήδη υφιστάμενο νομικό εργαλείο της Ευρωπαϊκής Εντολής Έρευνας (ΕΕΕ), το οποίο βασίζεται στην αμοιβαία αναγνώριση των δικαστικών αποφάσεων, μπορεί να εφαρμοστεί και για την περίπτωση συλλογής ηλεκτρονικών αποδεικτικών στοιχείων από άλλα κράτη μέλη. Η Επιτροπή στη σχετική πρόταση της για τα ηλεκτρονικά αποδεικτικά στοιχεία, αναφέρει ότι η ΕΕΕ καθώς και η αμοιβαία δικαστική συνδρομή επιφέρουν καθυστερήσεις στην αναζήτηση αυτής της ιδιαίτερης κατηγορίας αποδεικτικών στοιχείων και συνεπώς δεν παρέχουν αποτελεσματικό αίσθημα ασφάλειας στους πολίτες της Ένωσης, για αυτό και προτείνει δύο νέα νομικά εργαλείο για τη συλλογή ηλεκτρονικών αποδεικτικών στοιχείων την Ευρωπαϊκή Εντολή Υποβολής (ΕΕΥποβ.) και την Ευρωπαϊκή Εντολή Διατήρησης (ΕΕΔιατ.) ηλεκτρονικών αποδεικτικών στοιχείων. Όπως διαφαίνεται στο τοπίο η ΕΕΕ, η ΕΕΥποβ. και ΕΕΔιατ. θα συνυπάρξουν στο πεδίο της Ένωσης και θα αποτελούν νομικά εργαλεία που θα επιτρέπουν την ανταλλαγή ηλεκτρονικών αποδεικτικών στοιχείων μεταξύ των κρατών μελών της Ένωσης στο πλαίσιο ποινικών ερευνών. Τα εργαλεία αυτά αποσκοπούν στη διευκόλυνση της διασυνοριακής συνεργασίας στην έρευνα και τη δίωξη των ποινικών αδικημάτων, λαμβάνοντας επίσης υπόψη τα δικαιώματα των ατόμων και την ανάγκη προστασίας προσωπικών δεδομένων. Η ΕΕΕ επιτρέπει στις αρχές σε ένα κράτος μέλος της Ένωσης να ζητήσουν συνδρομή από τις αρχές σε άλλο κράτος μέλος, ακόμα και στη συγκέντρωση ηλεκτρονικών αποδεικτικών στοιχείων για χρήση σε ποινικές διαδικασίες, διασφαλίζοντας πλήρως τα δικαιώματα των υπόπτων και κατηγορουμένων, με την παρέμβαση κρατικών αρχών και στα δύο κράτη μέλη. Από την άλλη πλευρά η προτεινόμενη ΕΕΥποβ. στοχεύει στον εξορθολογισμό της διαδικασίας για την απόκτηση ηλεκτρονικών αποδεικτικών στοιχείων από άλλα κράτη μέλη και να διασφαλίσει ότι τα αιτήματα αυτά αντιμετωπίζονται με έγκαιρο και αποτελεσματικό τρόπο, στερούμενη όμως ορισμένων διασφαλιστικών δικλείδων στην προστασία των θεμελιωδών δικαιωμάτων των υποκείμενων προσώπων σε σχέση με την ΕΕΕ. Παράλληλα η ΕΕΔιατ., επιτρέπει στις αρχές σε ένα κράτος μέλος να ζητήσουν να διατηρηθούν ηλεκτρονικά αποδεικτικά στοιχεία σε έναν πάροχο που βρίσκεται σε άλλο κράτος μέλος για σκοπούς ποινικής διερεύνησης. Η ΕΕΔιατ. αποσκοπεί στην πρόληψη της καταστροφής ή της αλλοίωσης των ηλεκτρονικών αποδεικτικών στοιχείων που μπορεί να απαιτηθούν για ποινική έρευνα. Η Επιτροπή αναφέρει ότι οι δύο νέες εντολές, δημιουργούν ένα σύγχρονο πλαίσιο για την ανταλλαγή ηλεκτρονικών αποδεικτικών στοιχείων μεταξύ των κρατών μελών κατά τρόπο που να είναι σύμφωνο με την Ενωσιακή νομοθεσία και τα θεμελιώδη δικαιώματα των ατόμων. Ωστόσο, συγκρίνοντας τα νομικά εργαλεία αυτά, γίνεται αντιληπτό ότι το επίπεδο προστασίας των δικαιωμάτων ίσως δεν είναι το ίδιο με την χρήση όλων των εντολών και αυτό γιατί με τις προτεινόμενες ρυθμίσεις για την ΕΕΥποβ. και ΕΕΔιατ. δεν είναι βέβαιο αν εξασφαλίζονται επαρκώς και γίνονται σεβαστά τα δικαιώματα των υπόπτων και κατηγορουμένων, συγκρινόμενες πάντα με την ΕΕΕ. Τέλος, διαπιστώνεται ότι η μελλοντική συνύπαρξη αυτών των εντολών (ΕΕΕ, ΕΕΥποβ. και ΕΕΔιατ.) και η σχέση μεταξύ αυτών, δημιουργεί τη δυνατότητα στα κράτη μέλη να επιλέγουν κάθε φορά το κατάλληλο νομικό εργαλείο προκειμένου να διευκολυνθεί η διασυνοριακή συνεργασία σε ποινικές έρευνες, για την συλλογή εκείνων των ηλεκτρονικών αποδεικτικών στοιχείων που κρίνονται αναγκαία, με τις όποιες επιφυλάξεις αναφέρθηκαν προηγουμένως.

Λέξεις Κλειδιά: Ευρωπαϊκή Ένωση, Ασφάλεια, Ηλεκτρονικά αποδεικτικά στοιχεία (e-evidence), Ευρωπαϊκή Εντολή Έρευνας, Ευρωπαϊκή Εντολή Υποβολής Στοιχείων, Ευρωπαϊκή Εντολή Διατήρησης Στοιχείων.

Abstract

This thesis, it is presented the framework in which the Union and the Member States are invited to apply and collect electronic evidence. The European Investigation Order (EIO) is already an existing legal tool based on mutual recognition of judicial decisions that can also be applied to the case of collecting electronic evidence from other Member States. The Commission in its proposal for electronic evidence states that EIO as well as mutual judicial assistance brings delays in the search for this particular category of evidence and therefore does not provide an effective sense of justice to the citizens of the Union, so it proposes two new legal tools. The European Production Order (EPO) and the European Preservation Order (EPSO). As appear in the landscape the EIO, EPO, and EPSO will coexist in the field of Union and will be the legal tools that will allow the exchange of electronic evidence between the Member States within the context of criminal investigations. These tools are intended to facilitate cross-border cooperation in the prosecution and investigation of criminal offenses, also taking into account the rights of individuals and the need to protect personal data. EIO enables the authorities of a Member State of the Union to request the authorities in another Member State, even in the gathering of electronic evidence for use in criminal proceedings, fully ensuring the rights of suspects and accused, but with the intervention of state authorities between the two Member States. On the other hand, the proposed EPO aims to rationalize the process of acquiring electronic evidence from other Member States and to ensure that these requests are treated in a timely and effective way but deprived of certain safeguards in protecting the fundamental rights of the subjects to Relationship with EIO. At the same time, EPSO allows the authorities in one Member State to request that electronic evidence be maintained and not erased in a provider located in another Member State for criminal investigation. The EPSO aims to prevent the destruction or deterioration of electronic evidence that may be required for criminal investigation and is stored in a provider. The Commission states that the two new legal tools will create a modern framework for the exchange of electronic evidence between Member States in a manner by the EU legislation and the fundamental rights of individuals. However, comparing these legal tools, it is understood that the level of protection of rights may not be the same as the use of all orders because of the proposed electronic evidence arrangements. It is not certain whether the rights of suspects and accused are sufficiently secured, always compared to EIO. Finally, it is found that the future coexistence of these orders and the relationship between them creates an ability for the Member States to choose the appropriate legal tool each time to facilitate cross-border cooperation in criminal investigations to collect the electronic evidence that is crucial for each case, having in mind the limitations of each tool in perspective of human rights protection.

Key Words: Intelligence, Security, European Union, e-evidence, electronic evidence, European Investigation Order, European Production Order, European Preservation Order.

Εισαγωγή

Η παρούσα εργασία εκπονήθηκε στα πλαίσια του μεταπτυχιακού Διεθνές Ευρωπαϊκό Δίκαιο και Διακυβέρνηση του Τμήματος Διεθνών και Ευρωπαϊκών Σπουδών του Πάντειου Πανεπιστημίου Κοινωνικών και Πολιτικών Επιστημών στην ειδίκευση με τίτλο «*Ευρωπαϊκό Ποινικό Δίκαιο*» κατά την περίοδο 2021-22.

Ο τίτλος της διπλωματικής εργασίας είναι «*Ζητήματα Ανταλλαγής Πληροφοριών και Συλλογής Αποδεικτικών Στοιχείων στο πλαίσιο της Αστυνομικής Συνεργασίας σε Ποινικές Υποθέσεις στην Ευρωπαϊκή Ένωση: Η Σχέση μεταξύ της Ευρωπαϊκής Εντολής Έρευνας και της Ευρωπαϊκής Εντολής Υποβολής και Διατήρησης Ηλεκτρονικών Αποδεικτικών Στοιχείων*».

Ο στόχος της ανά χείρας διπλωματικής εργασίας είναι να αναλύσει και να συγκρίνει δύο διαφορετικά θεσμικά μοντέλα απόκτησης αποδεικτικών στοιχείων στον χώρο της Ένωσης, που προσφέρουν αυτά τα δύο μέσα, η Ευρωπαϊκή Εντολή Έρευνας (ΕΕΕ) και η προταθείσα Ευρωπαϊκή Εντολή Υποβολής (ΕΕΥποβ.) και Διατήρησης (ΕΕΔιατ.) καθώς και να οριοθετήσει το πεδίο εφαρμογής τους. Επιπλέον μέσα από την παρούσα παρουσιάζονται οι προβληματισμοί σχετικά με την συνύπαρξη αυτών των δύο θεσμικών εργαλείων απόκτησης και πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία και τις συνέπειες που είναι δυνατόν να επιφέρουν στο πεδίο προστασίας των θεμελιωδών ανθρωπίνων δικαιωμάτων, όπως θα αναλυθεί και στη συνέχεια.

Αρχικά στο πρώτο κεφάλαιο οριοθετείται η ανάπτυξη του θέματος και ο αναγνώστης διακρίνει τα όρια μέσα στα οποία κινείται η συγκεκριμένη εργασία, αποσαφηνίζονται όροι και έννοιες, οι οποίες θα αναλυθούν. Την ίδια στιγμή αναδεικνύονται οι προκλήσεις και τα ζητήματα που αντιμετωπίζουν οι Αρχές Επιβολής του Νόμου των κρατών μελών στην αντιμετώπιση του εγκλήματος που διαπράττεται στον κυβερνοχώρο.

Εν συνεχεία στο δεύτερο κεφάλαιο της εργασίας αυτής γίνεται αναφορά στα ηλεκτρονικά αποδεικτικά στοιχεία και αναδεικνύονται οι λόγοι για τους όποιους είναι σημαντικά και αναγκαία όσο ποτέ άλλοτε στην ποινική έρευνα υποθέσεων αλλά και τα ιδιαίτερα χαρακτηριστικά γνωρίσματα που τα διακρίνουν. Ιδιαίτερα τονίζεται η ανάγκη για την συλλογή αυτών, από τους παρόχους όπου αυτά τηρούνται, με τα ήδη

υπάρχοντα νομικά εργαλεία συλλογής αυτών, από τα κράτη μέλη στο πλαίσιο μίας ποινικής έρευνας.

Ακολούθως στο τρίτο κεφάλαιο, περιγράφεται εν συντομία η Ευρωπαϊκή Εντολή Έρευνας (ΕΕΕ) και ορισμένες πτυχές αυτής, καθώς το νομικό αυτό εργαλείο, που ήδη χρησιμοποιείται για τη συλλογή αποδεικτικών στοιχείων από άλλα κράτη μέλη, μπορεί να χρησιμοποιηθεί και ειδικότερα για τη συλλογή ηλεκτρονικών στοιχείων από παρόχους που είναι εγκατεστημένοι σε άλλα κράτη μέλη. Επιπλέον, η αναφορά της ΕΕΕ, αξίζει καθώς αποτελεί τη βάση επάνω στην οποία η Επιτροπή, προχωρεί την ενωσιακή ενοποίηση και χτίζει επάνω σ' αυτήν την πρότασης της για το νέο πακέτο συλλογής ηλεκτρονικών αποδεικτικών στοιχείων με ακόμα δύο νέες εντολές. Η αναφορά στην ΕΕΕ, είναι απαραίτητη, προκειμένου εν συνεχεία με βάση αυτή, να γίνουν οι απαραίτητες συγκρίσεις και να καθοριστεί η σχέση μεταξύ των δύο νέων προτεινόμενων εντολών του επόμενου κεφαλαίου.

Μετέπειτα, στο τέταρτο κεφάλαιο, παρουσιάζονται οι νέες προτάσεις και εξελίξεις στο πεδίο αναφορικά με την συλλογή ηλεκτρονικών αποδείξεων από τους παρόχους ενώ περιγράφονται πως θα λειτουργούν τα δύο νέα νομικά εργαλεία συλλογής ηλεκτρονικών αποδεικτικών στοιχείων, δηλαδή η Ευρωπαϊκή Εντολή Υποβολής ηλεκτρονικών αποδεικτικών στοιχείων (ΕΕΥποβ.) και η Ευρωπαϊκή Εντολή Διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων (ΕΕΔιατ.). καθώς και οι προϋποθέσεις έκδοσης αυτών.

Επιπρόσθετα, στο πέμπτο κεφάλαιο γίνεται η σύγκριση σε διάφορα πεδία, ανάμεσα στην Ευρωπαϊκή Εντολή Έρευνας (ΕΕΕ) και των δύο νέων προτεινόμενων νομικών εργαλείων, δηλαδή την Ευρωπαϊκή Εντολή Υποβολής ηλεκτρονικών αποδεικτικών στοιχείων (ΕΕΥποβ.) και την Ευρωπαϊκή Εντολή Διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων (ΕΕΔιατ.) σε σχέση με την ΕΕΕ και αναδεικνύονται πτυχές ελλιπούς προστασίας των θεμελιωδών δικαιωμάτων υπόπτων και κατηγορουμένων αλλά και άλλες χρήσιμες πληροφορίες που αναδεικνύουν τον τρόπο λειτουργίας και τον σκοπό που θα επιτυγχάνεται με την θεσμοθέτηση αυτών από την Ένωση. Πτυχές από τη σύγκριση αυτή, μπορεί να βρει ο αναγνώστης και στο παράρτημα της παρούσας εργασίας.

Ακολούθως, στο έκτο κεφάλαιο περιγράφεται η μελλοντική υιοθέτηση των προτάσεων της Επιτροπής για τις δύο νέες εντολές όπως τις είδαμε, μέχρι τώρα ενώ

παρουσιάζεται και η πορεία της διαδικασίας ενωσιακής νομοθέτησης επί των προτάσεων της Επιτροπής, για τα ηλεκτρονικά αποδεικτικά στοιχεία.

Καταλήγοντας εξάγονται ορισμένα χρήσιμα συμπεράσματα για την μελλοντική συνύπαρξη αυτών των τριών νομικών εργαλείων που θα έχουν οι αρμόδιες αρχές επιβολής του νόμου και τα κράτη μέλη, ώστε να είναι σε θέση να αιτούνται και συλλέγουν ηλεκτρονικά αποδεικτικά στοιχεία, διασφαλίζοντας την ίδια στιγμή τα δικαιώματα των κατηγορουμένων και των υπόπτων στο πλαίσιο της ποινικής διαδικασίας, σεβόμενοι τον ΧΘΔΕΕ και την προστιθέμενη αξία που δημιουργεί το προστατευτικό πλαίσιο των πολιτών της Ένωσης, διαμέσου του δικαίου.

Κεφάλαιο Πρώτο

1. Η Ευρωπαϊκή Ένωση ως χώρος ελευθερίας, ασφάλειας και δικαιοσύνης

Η παροχή ασφάλειας αποτελεί μία από τις μακροχρόνιες πολιτικές προτεραιότητες της Ένωσης. Άλλωστε το εγχείρημα της ευρωπαϊκής ολοκλήρωσης ξεκίνησε από το βασικό σκοπό της εγγύησης της ασφάλειας στην ευρωπαϊκή ήπειρο για τα κράτη μέλη που μετέχουν σε αυτή και όχι μόνο (EU Global Strategy, 2016).

Η παροχή της ασφάλειας μέσω της Ένωσης περιλαμβάνει την δημιουργία ενός προστατευτικού ιστού μέσω του δικαίου της Ένωσης για την αποτελεσματική αντιμετώπιση εκείνων των απειλών και κινδύνων ενάντια στις αξίες και τα συμφέροντα της ως διεθνή δρώντα στην παγκόσμια σκηνή προασπίζοντας ταυτόχρονα και αυτά των κρατών μελών (European Commission, 2020).

Άλλωστε η ίδια η Ένωση όπως αναφέραμε και προηγουμένως, αποτελεί πρωταρχικό πάροχο ασφάλειας (Drent, Landman, & Zandee, 2014) είτε σε μακροεπίπεδο κρατών είτε με τη δράση που αναπτύσσει στη διεθνή σκηνή, είτε ακόμα και σε ατομικό επίπεδο με την προστασία των θεμελιωδών ανθρωπίνων δικαιωμάτων και την προάσπιση αυτών μέσω πολιτικών και στοχευμένης νομοθέτησης που αναπτύσσει προωθώντας ακόμη περισσότερο το εγχείρημα της ευρωπαϊκής ολοκλήρωσης (Παπακωνσταντής, 2019).

Την ίδια στιγμή, η Ένωση παρέχει αποτελεσματική προστασία όχι μόνο στα κράτη μέλη αλλά και στους πολίτες αυτών μέσα από τις πολιτικές που αναπτύσσει και προωθεί δια του δικαίου καθώς επίσης και μέσα από το σύστημα δικαιοσύνης που έχει εγκαθιδρύσει. Δεν θα πρέπει να ξεχνάμε ότι οι πολίτες των κρατών μελών, πλέον κατέχουν και την ιδιότητα του ευρωπαίου πολίτη διαμέσου της ευρωπαϊκής ιθαγένειας (Παπαγιάννης, 2016).

Το πεδίο της παροχής ασφάλειας είναι πολύ ευρύ και περιλαμβάνει πολλούς και διαφορετικούς τομείς (Stritzel, 2014), ωστόσο οι νέες τεχνολογικές εξελίξεις (εξέλιξη της τεχνολογίας και του διαδικτύου) καθώς και οι υβριδικές απειλές εναντίον κρατών μελών, απαιτούν νέους κανόνες, επιπλέον νομοθετικές ενέργειες και ενισχυμένη συνεργασία μεταξύ των κρατών μελών για την από κοινού αντιμετώπιση αυτών (Darmois & Schméder, 2018).

Όπως αντιλαμβανόμαστε η συνεργασία των κρατών λόγω αυτών των συνθηκών αυξάνεται σε ολοένα περισσότερους τομείς. Ιδιαίτερα η συνεργασία σε ποινικές υποθέσεις, μεταξύ των κρατών-μελών της Ένωσης έχει αποκτήσει θα έλεγε κάποιος μία ιδιαίτερη δυναμική και από τους περισσότερους ειδικούς του χώρου γίνεται λόγος ότι το δε εντεύθεν παραγόμενο δίκαιο από την πλευρά της Ένωσης, είναι δυνατόν να εντάσσεται στον λεγόμενο χώρο του ευρωπαϊκού ποινικού δίκαιου (Αρβανίτης, 2021). Η εξέλιξη αυτή οφείλεται πρωτίστως στην πρόοδο που έχει σημειωθεί στη διαδικασία της ευρωπαϊκής ολοκλήρωσης μετά τη Συνθήκη της Λισσαβόνας. Οι θεσμικές και κανονιστικές ρυθμίσεις της εν λόγω συνεργασίας συνάπτονται με την δημιουργία στην Ένωση ενός Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης (ΧΕΑΔ), (Allegrezza, 2014; Αρβανίτης, 2021).

Άλλωστε η ίδια η Ένωση έχει εγκαθιδρύσει ανάμεσα στα κράτη μέλη έναν Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης (ΧΕΑΔ), προκειμένου να είναι σε θέση όλοι οι ευρωπαίοι πολίτες να απολαμβάνουν εξίσου τις ενωσιακές ελευθερίες σε συνδυασμό με τη προστασία των θεμελιωδών ανθρωπίνων δικαιωμάτων (Tinoco-Pastrana, 2020; Παπαγιάννης, 2016; Παπακωνσταντής, 2019). Μέσα στο χώρο αυτό απαιτείται να διασφαλιστεί η κατοχύρωση της αμοιβαίας αναγνώρισης ως θεμελιακής αρχής για τα κράτη μέλη και τις επιδιώξεις τους και αφετέρου η υποχρέωση σεβασμού των θεμελιωδών δικαιωμάτων της Ένωσης, για την προστασία των πολιτών ως υποκείμενων στην ελεγχόμενη δημοκρατική εξουσία των κρατών μελών.

Το γεγονός αυτό σε συνδυασμό με τις ήδη υπάρχουσες απειλές της τρομοκρατίας, του οργανωμένου εγκλήματος και της ασφάλειας στον κυβερνοχώρο, καθιστούν την δράση της Ένωσης απαραίτητη περισσότερο από ποτέ, προκειμένου να επιτευχθεί ο πρωταρχικός της στόχος, που δεν είναι άλλος από την παροχή προστασίας και ασφάλειας μέσα από την προάσπιση και το σεβασμό των θεμελιωδών ανθρωπίνων δικαιωμάτων (Tinoco-Pastrana, 2020; Παπαγιάννης, 2008).

Ένας συγκεκριμένος τομέας, στον οποίο επιχειρεί η Ένωση να παρέχει αποτελεσματική ασφάλεια και προστασία δια του δικαίου είναι και το πεδίο του κυβερνοχώρου ή αλλιώς του διαδικτύου, το οποίο τείνει να αποτελεί βασικό πεδίο στο οποίο δραστηριοποιούνται ενεργά τόσο πολίτες όσο και κρατικές δομές αλλά και η ίδια η Ένωση (Darmois & Schméder, 2018).

Προκειμένου να πλαισιωθεί καλύτερα η ανά χείρας διπλωματική εργασία, στη συνέχεια του παρόντος κεφαλαίου, γίνεται μία επισκόπηση του πλαισίου εντός του οποίου εντάσσεται η ανάγκη για αποτελεσματική παροχή προστασίας στο πεδίο του κυβερνοχώρου και του διαδικτύου για την εξασφάλιση πρόσβασης και την διασφάλισης των κατάλληλων ηλεκτρονικών αποδείξεων (e-evidence) μέσω κατάλληλων θεσμών και νομικών εργαλείων (Tinoco-Pastrana, 2020), όπως αναλύεται στη συνέχεια.

1.1 Ασφάλεια και έγκλημα στον κυβερνοχώρο

Με την ανάπτυξη της παγκοσμιοποίησης και των νέων τεχνολογιών που τη συνοδεύουν, κάνει την εμφάνιση του ένας νέος χώρος αυτός του διαδικτύου (cyber). Οι σύγχρονες κοινωνίες εξαρτώνται σε μεγάλο βαθμό την σήμερον από τις τεχνολογίες του διαδικτύου και την συνδεσιμότητα που αυτό καταφέρνει. Οι ευρωπαϊκές κοινωνίες έχουν καταφέρει και στηρίζονται σε μεγάλο βαθμό σε πληροφοριακά και επικοινωνιακά δίκτυα, προκειμένου να είναι σε θέση να λειτουργούν κρίσιμες υποδομές όπως της ενέργειας, των μεταφορών, της ύδρευσης, των επικοινωνιών, ώστε να είναι σε θέση να συνεχίσουν να αναπτύσσονται. Ο υψηλός βαθμός εξάρτησης από αυτά τα πληροφοριακά συστήματα, τα καθιστά εξαιρετικά σημαντικά, προκειμένου να διαφυλαχθούν από επιθέσεις ή καταστροφή αυτών (Ilves, 2016; Λιαρόπουλος, 2018).

Ωστόσο στη σήμερον δεν λείπουν οι επιθέσεις σε βάρος αυτών των συστημάτων. Οι κυβερνοεπιθέσεις στοχεύουν να πλήξουν αυτά τα συστήματα με σκοπό να προκαλέσουν διαταραχή στην ομαλή λειτουργία αυτών. Έτσι αυτή η εξάρτηση που προκαλείται στις ευρωπαϊκές κοινωνίες από την συνδεσιμότητα τους με αυτά τα πληροφοριακά συστήματα, τις καθιστά ιδιαίτερα ευάλωτες αν για κάποιο λόγο (για παράδειγμα κυβερνοεπιθέσεις) αυτά τα πληροφοριακά συστήματα παύσουν να λειτουργούν (Ilves, 2016; Russell, 2014). Έτσι πλέον η ασφάλεια στο νέο αυτό πεδίο του κυβερνοχώρου αποκτά άλλες διαστάσεις και δεν περιορίζεται μόνο στο φυσικό χώρο που δρούσε μέχρι τώρα ο άνθρωπος. Τα ζητήματα ασφάλειας στον κυβερνοχώρο είναι ιδιαίτερα σημαντικά, όταν ενδεχόμενες κυβερνοεπιθέσεις σε βάρος αυτών, απειλούν τη λειτουργία ολοκλήρων κρατών ή οργανισμών (Λιαρόπουλος, 2018).

1.2 Η οπτική της ασφάλειας στον κυβερνοχώρο

Είναι πλέον παραδεκτό ότι την σήμερον, όλες οι πολιτικές και στρατιωτικές δραστηριότητες εξαρτώνται σε μεγάλο βαθμό από τον κυβερνοχώρο. Αυτό δημιουργεί νέες ευπάθειες, τόσο σε ατυχήματα όσο και σε εσκεμμένες απειλές. Οι κακόβουλοι δρώντες είτε πρόκειται για άτομα, είτε για οργανωμένες ομάδες είτε ακόμα και για κρατικούς δρώντες που δραστηριοποιούνται στον κυβερνοχώρο μπορούν, χωρίς φυσική παρουσία, να διεισδύσουν σε όλα τα πιθανά δίκτυα, συμπεριλαμβανομένων των πιο ευαίσθητων (Darmois & Schméder, 2018).

Κάθε άτομο, καθώς και οποιοσδήποτε κυβερνητικός ή μη κυβερνητικός οργανισμός ή ακόμα και μία επιχείρηση ή εταιρεία μπορεί να γίνει στόχος μίας τέτοιας επίθεσης μέσω του διαδικτύου (CEPOL, 2017). Εξ' ου και η αυξανόμενη ανησυχία για την ασφάλεια στον κυβερνοχώρο, η οποία αντικατοπτρίζει τις αλλαγές που πραγματοποιούνται στις προσεγγίσεις ασφάλειας, όπως τις αντιλαμβανόμαστε και όπως διέρχονται από την ασφάλεια των κρατών και της εδαφικής ακεραιότητας αυτών έως την ασφάλεια του ατόμου και των κοινωνιών. Δεδομένου της υψηλής συχνότητας με την οποία λαμβάνουν χώρα αλλά και των αξίων που διαταράσσουν οι κυβερνοεπιθέσεις, δύναται αυτές να αντιπροσωπεύουν μια θεμελιώδη επίθεση στα ανθρώπινα δικαιώματα, μεταξύ των οποίων προσβάλλεται η ιδιωτικότητα του ατόμου και τα προσωπικά του δεδομένα. Πέραν αυτών, την σήμερον οι κυβερνοεπιθέσεις έχουν τη δυνατότητα να χειραγωγούν την πορεία μίας δημοκρατικής διαδικασίας, όπως είναι οι εκλογές, θέτοντας με αυτό τον τρόπο σε κίνδυνο την ίδια την ύπαρξη της δημοκρατίας[1] (Darmois & Schméder, 2018).

Από αυτό γίνεται αντιληπτό, πως η ασφάλεια σε αυτό το νέο πεδίο αποκτά νέες διαστάσεις που σχετίζονται με την ίδια την λειτουργία ενός κράτους και κατ' επέκταση με το ίδιο το άτομο, όταν δεν μπορεί να εκπληρώσει βασικές του

[1] Για παράδειγμα τον Απρίλιο του 2007, η Εσθονία είχε δεχθεί κυβερνοεπιθέσεις από τη Ρωσία, που είχαν παραλύσει το μηχανισμό του κράτους της, δεδομένου της υψηλής εξάρτησης του Εσθονικού κράτους, από τη τεχνολογία και τα πληροφοριακά συστήματα, από τα οποία εξυπηρετείται το σύνολο των πολιτών της (Herzog, 2011; Ilves, 2016). Είναι γνωστό ότι η Εσθονία έχει καταφέρει να αναπτύξει από το 2000, παρά πολύ καλές υποδομές σε επίπεδο διαδικτύου και ηλεκτρονικών υπηρεσιών, με παρά πολύ μεγάλη απήχηση από τον πληθυσμό της, με μεγάλο ποσοστό αποδοχής και χρήσης αυτών. Σχεδόν όλες οι τραπεζικές συναλλαγές εξυπηρετούνται από το διαδίκτυο, οι φορολογικές δηλώσεις, οι μεταβιβάσεις ακινήτων, οι συνταγογραφήσεις φαρμάκων ακόμα και η ψηφοφορία των πολιτών. Οι πολίτες της διαθέτουν όλοι τη δυνατότητα ψηφιακής υπογραφής με την ταυτότητα τους, ενώ η ίδια συγκαταλέγεται ως η υπ' αριθμόν ένα χώρα στην ψηφιακή διακυβέρνηση, ανάμεσα στις υπόλοιπες χώρες της Ένωσης. Ωστόσο, αυτή η μοναδικότητα της, την κατέστησε ευάλωτη σε κυβερνοεπιθέσεις που το 2007, παρέλυσαν ολοκληρωτικά τη λειτουργία της (Ilves, 2016).

υποχρεώσεις ή να απολαύσει βασικά δικαιώματα που μέχρι πρότινος εκτελούσε μέσα από την χρήση του διαδικτύου (Hansen & Nissenbaum, 2009).

Θέλοντας να συνδέσουμε την κυβερνοασφάλεια με την θεωρία της Σχολής της Κοπεγχάγης για τις διαφορετικές θεωρήσεις της όψης της ασφάλειας (Balzacq, Léonard, & Ruzicka, 2015; Buzan, Waever, & Jaap De Wilde, 1998), θα λέγαμε ότι «*η ασφάλεια του διαδικτύου*» και η συνέχιση της λειτουργίας του κράτους και η διακινδύνευση της ασφάλειας του ατόμου, αποτελούν τις βασικές αξίες και υποκείμενα που χρήζουν προστασίας σε μία δημοκρατική κοινωνία, ενώ η κατάσταση που είχε δημιουργηθεί το 2007 είχε αναχθεί από τους πολιτικούς της Εσθονίας σε ισοδύναμο «*κυβερνοπόλεμου*» από τη Ρωσία (Hansen & Nissenbaum, 2009). Η Ένωση στα θεσμικά της κείμενα αναφέρει χαρακτηριστικά ότι, αυτές οι κυβερνοεπιθέσεις κατά ιδιωτικών ή κρατικών πληροφορικών συστημάτων στα κράτη μέλη, προσδίδουν μια νέα διάσταση σ' αυτές, αυτή ενός δυνητικού νέου οικονομικού, πολιτικού και στρατιωτικού όπλου (υβριδική απειλή) που στρέφεται ενάντια στα ίδια τα κράτη μέλη και ως εκ τούτου κατά της ίδιας της Ένωσης (EU Global Strategy, 2016).

1.3 Διαδίκτυο και Τρομοκρατία

Με την εξέλιξη της τεχνολογίας και του διαδικτύου προσφέρεται πλέον η δυνατότητα στις τρομοκρατικές οργανώσεις να αναπτύσσουν την δράση τους και στο διαδίκτυο. Έτσι βλέπουμε σε αυτήν την περίπτωση ότι μία από τις κύριες απειλές για την ασφάλεια της Ένωσης, όπως η τρομοκρατία, συνυπάρχει στον κυβερνοχώρο και τον εκμεταλλεύεται (Scrivens, Gill, & Conway, 2020). Στην περίπτωση αυτή, όταν χρησιμοποιούνται τα πληροφοριακά δίκτυα ή ο κυβερνοχώρος, προκειμένου να αναπτυχθεί τρομοκρατική δράση, τότε κάνουμε λόγο για κυβερνοτρομοκρατία (cyberterrorism), (Γέρμανος & Γεωργίου, 2021).

Η χρήση του διαδικτύου και των κοινωνικών μέσων από τους τρομοκράτες, έχει αυξηθεί πάρα πολύ τα τελευταία χρόνια[2]. Η εξέλιξη της τεχνολογίας και του διαδικτύου δίνει τη δυνατότητα να διαδίδεται μέσω αυτού, περιεχόμενο που αφορά την τρομοκρατία ή να χρησιμοποιείται για τρομοκρατικούς σκοπούς ή για την

[2] Ειδικότερα, οι τζιχαντιστικές τρομοκρατικές ομάδες, έχουν δείξει μια εκλεπτυσμένη κατανόηση του τρόπου λειτουργίας των κοινωνικών δικτύων και έχουν ξεκινήσει καλά οργανωμένες και συντονισμένες εκστρατείες στα μέσα κοινωνικής δικτύωσης για την στρατολόγηση οπαδών και για την προώθηση διαδικτυακού υλικού, που περιέχει τρομοκρατικές πράξεις, ενέργειες ή πράξεις βίαιου εξτρεμισμού (Europol, 2021).

στρατολόγηση νέων μελών ή να απευθύνεται κάλεσμα σε μοναχικούς λύκους για την διενέργεια τρομοκρατικών χτυπημάτων ή τέλος για την προσέλκυση χρημάτων για την χρηματοδότηση της (Scrivens et al., 2020).

Κάτι τέτοιο μπορεί να έχει ολέθριες συνέπειες για τις κοινωνίες των ευρωπαϊκών κρατών. Για το λόγο αυτό η έγκαιρη διάγνωση του φαινομένου αυτού άλλα και η πρόληψη του, είναι σημαντική αποστολή του τομέα της πληροφόρησης (intelligence) που διεξάγεται από τα κράτη μέλη και την Ένωση. Σε ενωσιακό επίπεδο, το ρόλο αυτόν τον έχει αναλάβει η Europol και συγκεκριμένα στα πλαίσια του Ευρωπαϊκού Κέντρου Αντιμετώπισης της τρομοκρατίας (European Counter Terrorism Centre-ECTC) όπου έχει δημιουργηθεί η Μονάδα Αναφοράς Διαδικτυακού περιεχομένου (Internet Referral Unit-IRU), που έχει ως σκοπό την αναζήτηση και την συλλογή διαδικτυακού υλικού που αφορά την τρομοκρατία[3] σε συνεργασία με τις αρμόδιες υπηρεσίες αντιμετώπισης της τρομοκρατίας των εθνικών αρχών των κρατών μελών (Γέρμανος & Γεωργίου, 2021; Παπακωνσταντής, 2019). Η διάδοση της τρομοκρατίας μέσω του διαδικτύου είναι μία πολύ σοβαρή απειλή, που τα κράτη χρειάζεται να αντιμετωπίσουν στην σύγχρονη εποχή με τα μέσα που διαθέτουν, προκειμένου να αποτελεί ποινικό αδίκημα αλλά και να αφαιρείται από το διαδίκτυο (Γέρμανος & Γεωργίου, 2021; Παπακωνσταντής, 2019).

1.4 Διαδίκτυο και Έγκλημα

Ωστόσο το διαδίκτυο, χρησιμοποιείται όχι μόνο για να στραφεί ως εργαλείο κατά κρατικών δρώντων αλλά και κατά των ατόμων, προκειμένου κάποιος κακόβουλος χρήστης να διαπράξει κάποιο έγκλημα σε βάρος αυτού. Έτσι οι εγκληματίες, βρίσκουν στο χώρο του διαδικτύου και της τεχνολογίας ένα ακόμα πεδίο δράσης που το εκμεταλλεύονται, προκειμένου να αποκομίσουν παράνομο όφελος οποιαδήποτε μορφής (περιουσιακό κλπ.) σε βάρος απλών πολιτών στα κράτη μέλη. Το έγκλημα στον κυβερνοχώρο, πλέον αποτελεί καθημερινό φαινόμενο ενώ διαβάζουμε και βλέπουμε γι’ αυτό περισσότερο συχνά από ότι παλαιότερα (Γέρμανος & Γεωργίου, 2021).

[3] Χρειάζεται να επισημανθεί ότι οι τεχνικές που χρησιμοποιούνται για την επισήμανση αυτού του περιεχομένου στο διαδίκτυο, συνιστούν τεχνικές συλλογής και ανάλυσης πληροφοριών από ανοικτές πηγές (Open Source Intelligence-OSINT). Επιπλέον για το λόγο αυτό συνεργάζεται με τις ιδιωτικές εταιρείες παρόχους διαδικτυακών υπηρεσιών όπου ειδοποιούνται, προκειμένου να αποσύρουν το σχετικό υλικό στο πλαίσιο των συμβατικών και νομοθετικών τους υποχρεώσεων. Η Μονάδα Αναφοράς Διαδικτυακού περιεχομένου της Europol, δημοσιεύσει το έργο της κάθε χρόνο στην διαδικτυακή ιστοσελίδα (Europol, 2021). Η έκθεση αυτή αποτελεί ένα προϊόν στρατηγικής ανάλυσης πληροφοριών (strategic intelligence) που προέρχεται κυρίως από ανοικτές πηγές (OSINT).

Ορισμένες φορές τα εγκλήματα στον κυβερνοχώρο, μπορεί να λαμβάνουν χώρα περισσότερο συχνά, από ότι στον πραγματικό κόσμο και αυτό γιατί η άνοδος της τεχνολογίας και του διαδικτύου έχουν εισχωρήσει σε πληθώρα δραστηριοτήτων της καθημερινότητας, τόσο των ανθρώπων όσο και των επιχειρήσεων ή άλλων δημόσιων/διεθνών ή ιδιωτικών οργανισμών (Europol SOCTA, 2021).

Το κυβερνοέγκλημα (cybercrime) αποτελεί όρο που προέρχεται επίσημα και από τη Σύμβαση για το έγκλημα στον κυβερνοχώρο του Συμβουλίου της Ευρώπης που θεσπίστηκε το 2001, (Council of Europe, 2001). Ωστόσο στη βιβλιογραφία επικρατούν και άλλοι ορισμοί όπως ψηφιακό έγκλημα ή έγκλημα στο διαδίκτυο ή ηλεκτρονικό έγκλημα. Ωστόσο όταν πολλοί κλάδοι τόσο της νομικής όσο και της πληροφορικής επιχειρούν να αποδώσουν έναν ενιαίο ορισμό για ένα φαινόμενο που μετρά μόνο λίγες δεκαετίες παρουσίας είναι φυσικό να υπάρχει ευρεία χρήση ορισμών και ονομάτων (Γέρμανος & Γεωργίου, 2021).

Ωστόσο το διαδίκτυο μπορεί να υποβοηθά στην τέλεση και άλλων εγκλημάτων που προϋπήρχαν πριν από αυτό ή η τέλεση ορισμένων εξ' αυτών να εξαρτάται αποκλειστικά από το διαδίκτυο και τα πληροφοριακά συστήματα που διασυνδέει μεταξύ τους[4]. Τα εγκλήματα αυτά που η ύπαρξη τους εξαρτάται από το διαδίκτυο χαρακτηρίζονται ως «***γνήσια κυβερνοεγκλήματα***» ενώ τα υπόλοιπα που η χρήση του διαδικτύου απλώς τα υποβοηθά, χαρακτηρίζονται ως «***μη γνήσια κυβερνοεγκλήματα***»[5](Γέρμανος & Γεωργίου, 2021).

Η χρήση του διαδικτύου και των υπηρεσιών που παρέχει αναμφίβολα ωθούν τον κόσμο σε ανάπτυξη και ευημερία ωστόσο μπορούν να χρησιμοποιηθούν και κακόβουλα. Τα εργαλεία και οι υπηρεσίες του διαδικτύου, μπορούν να αποτελέσουν εργαλεία για τη διάπραξη ή τη διευκόλυνση εγκλημάτων, μεταξύ των οποίων και σοβαρά εγκλήματα όπως τρομοκρατικές επιθέσεις (Scrivens et al., 2020). Όταν

[4] Έτσι για παράδειγμα μία προσβολή ή μία δυσφήμηση διαμέσου μίας ανάρτησης σε κάποιο μέσο κοινωνικής δικτύωσης (facebook κλπ), υποβοηθείται από το διαδίκτυο ενώ το ίδιο αδίκημα θα μπορούσε να τελεστεί και διαμέσου ενός έντυπου μέσου ή μέσω τηλεφώνου. Ένα άλλο αδίκημα που υποβοηθείται από την τεχνολογία και το διαδίκτυο θα μπορούσε να αποτελεί η δημιουργία πλαστών εγγράφων ή χαρτονομισμάτων. Ωστόσο από την άλλη πλευρά, υπάρχουν εγκλήματα όπου δε θα μπορούσαν να τελεστούν αν δεν υπήρχε το διαδίκτυο όπως οι επιθέσεις σε βάρος πληροφοριακών συστημάτων, υποκλοπή και αλλοίωση ψηφιακών δεδομένων, διαδικτυακή σεξουαλική κακοποίηση κλπ.

[5] Για την διάκριση ανάμεσα σε γνήσια (stricto-sensu) και μη γνήσια κυβερνοεγκλήματα, καθώς και παραδείγματα τέτοιων εγκλημάτων, μεταξύ άλλων έχει εκδοθεί και η Εγκύκλιος ΕισΑΠ υπ' αριθμό 2 εκδοθ. από 22-5-2019.

συμβαίνει κάτι τέτοιο, οι εν λόγω διαδικτυακές υπηρεσίες ή ηλεκτρονικές εφαρμογές που έχουν χρησιμοποιηθεί από τους δράστες, είναι συχνά το σημείο εκείνο στο οποίο οι αστυνομικές και δικαστικές αρχές, μπορούν να βρουν ενδείξεις για να προσδιορίσουν τον πιθανό δράστη και φυσικά να συλλέξουν αποδεικτικά στοιχεία τα οποία μπορούν να χρησιμοποιηθούν στο δικαστήριο (Ευρωπαϊκή Επιτροπή, 2018a).

1.5 Προκλήσεις και προβλήματα που σχετίζονται με τα ηλεκτρονικά αποδεικτικά στοιχεία

Μελετώντας τη βιβλιογραφία θα παρατηρήσει κανείς ότι το ζήτημα της καταπολέμησης της εγκληματικότητάς στον κυβερνοχώρο συνδέεται σε μεγάλο βαθμό με τη δυνατότητα των αρχών επιβολής του νόμου, να αποκτούν ηλεκτρονικά αποδεικτικά στοιχεία που σχετίζονται με αυτά τα αδικήματα από τους παρόχους υπηρεσιών διαδικτύου ή επικοινωνιών (Rojszczak, 2022). Για το λόγο αυτό, προκειμένου να κατανοηθεί πλήρως το πλαίσιο μέσα στο οποίο εντάσσεται η παρούσα εργασία, στη συνέχεια παρουσιάζονται οι κυριότερες προκλήσεις που προκύπτουν κατά την διερεύνηση υποθέσεων εγκλημάτων στον κυβερνοχώρο τόσο από τη πλευρά των αρχών επιβολής του νόμου άλλα και από την πλευρά των δικαστικών και εισαγγελικών αρχών.

1.5.1 Δυσχέρειες πρόσβασης σε δεδομένα

Όπως ήδη αντιλαμβανόμαστε από τα όσα έχουν αναφερθεί μέχρι στιγμής τα ψηφιακά και ηλεκτρονικά δεδομένα είναι κρίσιμα στοιχεία για την έρευνα μίας υπόθεσης εγκλήματος στον κυβερνοχώρο ή μπορεί να λειτουργήσει συμπληρωματικά για την στοιχειοθέτηση οποιουδήποτε άλλου εγκλήματος αν έχουν χρησιμοποιηθεί ηλεκτρονικά μέσα ή διαδικτυακές υπηρεσίες. Η πρόσβαση στα ψηφιακά αυτά δεδομένα δεν είναι πάντοτε εφικτή και μπορεί να δυσχεραίνει την διερεύνηση μίας υπόθεσης και στην οποία εμπεριέχονται ηλεκτρονικά ή ψηφιακά πειστήρια. Προκειμένου να είναι εφικτή η πρόσβαση στα δεδομένα αυτά, απαιτείται να διατηρούνται από τους παρόχους παροχής υπηρεσιών διαδικτύου ή επικοινωνιών, ώστε εν συνεχεία να μπορούν να αντλούνται από τις αρμόδιες αρχές (Blažič & Klobučar, 2020a).

Για το σκοπό αυτό τέθηκε σε εφαρμογή για μικρό χρονικό διάστημα η 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 διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ. Η Οδηγία αυτή είναι γνωστή ως Οδηγία Διατήρησης Δεδομένων (Data Retention Directive) και ο κύριος στόχος της ήταν η εναρμόνιση των νομοθετικών διατάξεων των κρατών μελών για τη διατήρηση ορισμένων δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία από παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών. Σκοπός αυτής της Οδηγίας ήταν να διασφαλίζεται η διαθεσιμότητα των ψηφιακών δεδομένων που τηρούνται από τους παρόχους για τους σκοπούς της πρόληψης, διερεύνησης και δίωξης σοβαρών ποινικών αδικημάτων, όπως είναι μεταξύ άλλων τα αδικήματα που συνδέονται με το οργανωμένο έγκλημα και την τρομοκρατία. Έτσι, καθόριζε ότι οι προαναφερθέντες Πάροχοι υπηρεσιών διαδικτύου και επικοινωνιών, όφειλαν να διατηρούν τα δεδομένα κίνησης και τοποθεσίας, καθώς και τα συναφή δεδομένα που απαιτούνται για την αναγνώριση του συνδρομητή ή του χρήστη αλλά όχι το περιεχόμενο της επικοινωνίας.

Ωστόσο η Οδηγία 2006/24/ΕΚ καταργήθηκε από το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ) με την απόφαση της 8ης Ιουλίου 2014 στην υπόθεση ΔΕΕ C-293/12. Η εξέλιξη αυτή όπως είναι αναμενόμενο δημιούργησε αβεβαιότητα στις αρχές επιβολής του νόμου αλλά και στις δικαστικές και εισαγγελικές αρχές των διαφόρων κρατών μελών, αναφορικά με την άντληση στοιχείων από ιδιωτικούς φορείς όπως είναι οι Πάροχοι υπηρεσιών διαδικτύου και επικοινωνιών. Πιο συγκεκριμένα στην υπόθεση ΔΕΕ, C-293/12 της 8-07-2017, έκρινε ότι απαιτώντας από τους παρόχους υπηρεσιών τη διατήρηση των δεδομένων που ρυθμίζονται από την Οδηγία και επιτρέποντας την πρόσβαση των αρμόδιων αρχών σε αυτά, η Οδηγία έχει ως αποτέλεσμα να παρεμβαίνει σε τέτοιο βαθμό σε θέματα σεβασμού της ιδιωτικής ζωής του ατόμου και προστασίας προσωπικών δεδομένων που να καθίσταται αντίθετη με τη θεμελιώδη αρχή της αναλογικότητας που απαιτείται να διέπει την ενωσιακή νομοθεσία.

Ωστόσο σε ορισμένα κράτη μέλη εξακολουθεί να υπάρχει νομοθεσία για να διασφαλίζεται ότι οι Πάροχοι υπηρεσιών διαδικτύου διατηρούν δεδομένα για σκοπούς που μπορεί να αφορούν μέτρα για την καταστολή του εγκλήματος ενώ σε άλλα κράτη μέλη η εθνική νομοθεσία αναφορικά με την διατήρηση δεδομένων στους παρόχους, καταργήθηκε μετά την ακύρωση αυτής της Οδηγίας από το ΔΕΕ. Σε

ορισμένα από αυτά τα κράτη μέλη οι Πάροχοι Υπηρεσιών Διαδικτύου ή επικοινωνιών διατηρούν ορισμένα δεδομένα για εμπορικούς ή λογιστικούς σκοπούς άλλα δεν διαθέτουν αυτά τα δεδομένα για την υποστήριξη ποινικών ερευνών. Οι αποκλίσεις αυτές στις εθνικές νομοθεσίες των κρατών μελών, όπως θα αναφερθεί και παρακάτω που είναι σε θέση ορισμένες φορές να οδηγήσουν σε απώλεια ορισμένων δεδομένων ή αποδείξεων και επηρεάζοντας με τον τρόπο αυτό την ικανότητα των αρμόδιων αρχών επιβολής του νόμου για την δίωξη της εγκληματικότητας στο διαδίκτυο και στον κυβερνοχώρο (Γέρμανος & Γεωργίου, 2021).

Το πλαίσιο αυτό ή μάλλον τα διαφορετικά εθνικά πλαίσια που ισχύουν αναφορικά με τη διατήρηση δεδομένων και στοιχείων σε παρόχους, δημιουργούν ένα άνισο πεδίο για τις αρχές επιβολής του νόμου οι οποίες τείνουν να επικεντρώνουν την δραστηριότητα τους σε προθεσμίες ή ασφυκτικά χρονικά πλαίσια, αντί να επικεντρώνονται στην διαλεύκανση σοβαρών υποθέσεων διαδικτυακών εγκλημάτων (Γέρμανος & Γεωργίου, 2021). Χρειάζεται να σημειωθεί ότι στην Ελλάδα οι πάροχοι υπηρεσιών διαδικτύου είναι υποχρεωμένοι να διατηρούν δεδομένα επικοινωνίας για δώδεκα μήνες σύμφωνα με το αρ. 6 του Ν. 3917/2011.

Το υφιστάμενο ήδη προβληματικό πλαίσιο όπως αντιλαμβανόμαστε, εντάθηκε ακόμα περισσότερο μετά τις αποφάσεις της 21ης Δεκεμβρίου 2016 του ΔΕΕ στις υποθέσεις C-203/15 και C-698/15 (υποθέσεις Sverige και Watson) καθώς και τις συνακόλουθες απαιτήσεις για στοχευμένη διατήρηση δεδομένων και κριτήρια πρόσβασης για τις αρμόδιες αρχές των κρατών μελών. Έτσι γίνεται αντιληπτό ότι η έλλειψη ενιαίας πολιτικής για τη διατήρηση των δεδομένων αυτής της φύσεως σε ολόκληρη την Ένωση, μετατρέπεται σε μία από τις κυριότητες προκλήσεις για τη διερεύνηση του διασυνοριακού εγκλήματος στον κυβερνοχώρο όπως επισημαίνουν οι περισσότεροι ειδικοί στο χώρο αυτό (Γέρμανος & Γεωργίου, 2021). Όπως θα εξηγηθεί και στη συνέχεια η διατήρηση των ηλεκτρονικών αποδείξεων είναι κρίσιμης σημασίας, προκειμένου εν συνεχεία να μπορούν να αποκτηθούν και είναι αυτό που στοχεύει και η προταθείσα Ευρωπαϊκή Εντολή Διατήρησης Δεδομένων[6] (όπως θα δούμε και παρακάτω αναφέρεται και ως ΕΕΔιατ.), (Tinoco-Pastrana, 2020).

[6] Η Επιτροπή, με την πρόταση της αυτή, φαίνεται ότι αντιλαμβάνεται τις ανησυχίες των ειδικών που χειρίζονται τέτοιες υποθέσεις διασυνοριακού εγκλήματος στον κυβερνοχώρο και για το λόγο αυτό με τις ήδη κατατεθείσες προτάσεις της, είναι σε θέση να διαμορφώσει σε σημαντικό βαθμό το νομικό πλαίσιο εντός της Ένωσης βάσει του οποίου θα διατηρούνται και θα αποκτάται πρόσβαση κάθε φορά σε πιο γρήγορους χρόνους και πιο αποτελεσματικά, από τις αρμόδιες αρχές των κρατών μελών σε κρίσιμα ηλεκτρονικά αποδεικτικά στοιχεία, τα

1.5.2 Κρυπτογραφία

Η κρυπτογράφηση αποτελεί ένα σύγχρονο στοιχείο της εποχής μας που σχετίζεται με την διακίνηση ηλεκτρονικών δεδομένων και πληροφοριών στο διαδίκτυο και τις επικοινωνίες και είναι σε θέση να εξασφαλίζει και να προστατεύει τα θεμελιώδη ανθρώπινα δικαιώματα αναφορικά με το σεβασμό της ιδιωτικότητας και τα προσωπικά δεδομένα. Εν τούτοις, η τεχνολογία αυτή με τις προοπτικές που προσφέρει για όλους του χρήστες, γίνεται αντικείμενο εκμετάλλευσης και από εγκληματίες του διαδικτύου που σκοπό έχουν να αποκρύψουν και να προστατεύσουν τις όποιες επικοινωνίες τους ή τα όποια δεδομένα διατηρούν, με ισχυρές μορφές κρυπτογράφησης (Γέρμανος & Γεωργίου, 2021). Ενδεικτικά, θα μπορούσαμε να αναφέρουμε την διατήρηση αρχείων παιδικού πορνογραφικού υλικού σε κρυπτογραφημένη μορφή σε έναν σκληρό δίσκο ή πολύ περισσότερο σε ένα διαδικτυακό διακομιστή (server) ενός παρόχου διαδικτύου στο υπολογιστικό νέφος (cloud). Η χρήση εργαλείων κρυπτογράφησης για προσωπική χρήση είναι διαδεδομένη ενώ αρκετοί πάροχοι υπηρεσιών διαδικτύου προσφέρουν την δυνατότητα αυτή στις υπηρεσίες που προσφέρουν, με αποτέλεσμα τα αρχεία που κρυπτογραφούνται να είναι δύσκολα έως και καθόλου αναγνώσιμα και κατανοητά ως προς το περιεχόμενο τους (Pisaric, 2021; Γέρμανος & Γεωργίου, 2021).

Η κρυπτογράφηση των δεδομένων ενός παρόχου, αποτελεί από μόνη της μία πρόκληση, καθώς η ενδεχόμενη πρόσβαση των αρχών στα ψηφιακά κρυπτογραφημένα δεδομένα δεν θα αποτελούσε λύση[7]. Στην περίπτωση αυτή, απαιτείται τα ψηφιακά δεδομένα που τηρούνται σε κάποιο πάροχο υπηρεσιών διαδικτύου και βρίσκονται σε αυτή την κρυπτογραφημένη μορφή, απαιτείται να εξαχθούν με τρόπο που διασφαλίζει την αναγνωσιμότητα τους και την δυνατότητα επεξεργασίας τους για τους σκοπούς αποκάλυψης ενός εγκλήματος ή της τεκμηρίωσης αυτού (Pisaric, 2021; Γέρμανος & Γεωργίου, 2021). Αυτό δεν μπορεί να συμβεί χωρίς την παρέμβαση του ίδιου του παρόχου για την αποκρυπτογράφηση

οποία πολλές φορές μπορεί να αποτελούν το μοναδικό κλειδί για την επιτυχημένη διερεύνηση και δίωξη εγκλημάτων στον κυβερνοχώρο (Rogalski, 2020; Tinoco-Pastrana, 2020).

[7] Η εκτεταμένη χρήση της λειτουργίας αυτής όπως είναι κατανοητό επηρεάζει αρνητικά σε μεγάλο βαθμό τις δυνατότητες των αρχών επιβολής του νόμου για την διερεύνηση εγκλημάτων που σχετίζονται με ηλεκτρονικά αποδεικτικά ενώ ελλοχεύει ο κίνδυνος οι δράστες να κρύψουν κρίσιμα στοιχεία επ' αόριστον χωρίς δυνατότητα αξιοποίησης αυτών (Pisaric, 2021). Ως εκ τούτου η κατάχρηση εργαλείων κρυπτογράφησης και ανωνυμοποιήσης από εγκληματίες για την προστασία των επικοινωνιών ή των δεδομένων που κρατούν ή των οικονομικών συναλλαγών τους και την αποφυγή εντοπισμού αυτών έχει ως αποτέλεσμα να εμποδίζει τις αρμόδιες αρχές στην πρόσβαση σε πληροφορίες ή αποδεικτικά στοιχεία (Γέρμανος & Γεωργίου, 2021).

αυτών και την παροχή τους στις αρχές σε μορφή που είναι αναγνώσιμη ή δυνατή για ψηφιακή εγκληματολογική ανάλυση (Pisaric, 2021).

1.5.3 Προκλήσεις που αφορούν το εθνικό νομικό πλαίσιο των κρατών

Παρά την ύπαρξη διεθνών και ευρωπαϊκών νομοθετικών ρυθμίσεων, ορισμένες διαφορές μεταξύ του εθνικού νομικού πλαισίου ενός κράτους μπορεί να αποδεικνύεται συχνά ως ένα σοβαρό εμπόδιο στη διεθνή ποινική έρευνα και δίωξη του εγκλήματος στον κυβερνοχώρο εν μέρει και λόγω της πλημμελούς μεταφοράς του διεθνούς ή του ευρωπαϊκού νομικού πλαισίου στην εθνική νομοθεσία[8].Οι κύριες διαφορές αυτές εντοπίζονται κυρίως στα εξής σημεία (Blažič & Klobučar, 2020a; Γέρμανος & Γεωργίου, 2021):

- Την πρόβλεψη ενός κράτους για την ποινικοποίηση ή όχι ορισμένης συμπεριφοράς. Έτσι για παράδειγμα όταν τιμωρείται μόνο η αγορά παιδικού πορνογραφικού υλικού και όχι η κατοχή αυτού, τότε πρόκειται για μία διαφοροποιημένη ποινική μεταχείριση ανάμεσα στα εθνικά κράτη που εφαρμόζουν τέτοια ποινική νομοθεσία.
- Την πρόβλεψη κατηγοριοποίησης αυτής της συμπεριφοράς σε διαφορετική βαθμίδα αδικήματος ανάλογα με τη σοβαρότητα αυτού και την επαπειλούμενη ποινή που προβλέπεται από τον ποινικό κώδικα. Έτσι για παράδειγμα μία ποινική συμπεριφορά να τιμωρείται σε βαθμό πλημμελήματος σε ένα κράτος Χ ενώ η ίδια ποινική συμπεριφορά σε βαθμό κακουργήματος σε ένα άλλο κράτος Ψ.
- Την πρόβλεψη για την ύπαρξη επαρκούς επικαιροποιημένου νομικού πλαισίου και εθνικών νομικών διατάξεων για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και την πρόσβαση και απόκτηση ηλεκτρονικών αποδεικτικών στοιχείων.

1.5.4 Απώλεια τοποθεσίας και ζητήματα δικαιοδοσίας

Ο ψηφιακός χώρος του διαδικτύου δεν έχει σύνορα και απλώνεται παντού σε όλον τον κόσμο για όποιον μπορεί να αποκτήσει πρόσβαση σε αυτόν. Όλες οι τελευταίες

[8] Οι διαφορές αυτές, βρίσκουν κυρίως προβληματισμού, όταν απαιτείται από τις ισχύουσες διατάξεις να ισχύει η λεγόμενη «*αρχή του διττού αξιοποίνου*». Η αρχή συναντάται κυρίως κατά την εκτέλεση ενός ευρωπαϊκού εντάλματος σύλληψης, όταν απαιτείται η πράξη να τιμωρείται τόσο στο κράτος έκδοσης όσο και στο κράτος εκτέλεσης αυτού.

τεχνολογικές εξελίξεις στο πεδίο του κυβερνοχώρου όπως είναι η κρυπτογράφηση, η ευρεία διάδοση των κρυπτονομισμάτων, η διάδοση του Σκοτεινού Διαδικτύου (DarkWeb) και αρκετά ακόμη σε συνδυασμό με την κατάχρηση αυτών από τους εγκληματίες του κυβερνοχώρου, δημιουργούν ευκαιρίες για την δραστηριοποίηση τους από οποιοδήποτε μέρος του πλανήτη, υπάρχει πρόσβαση στο διαδίκτυο (Γέρμανος & Γεωργίου, 2021).

Από τη μελέτη της βιβλιογραφίας η παραβατικότητα στον κυβερνοχώρο χαρακτηρίζεται ως ένα έγκλημα που δε γνωρίζει σύνορα (Moraski, 2011). Την ίδια στιγμή, η αυξανόμενη χρήση υπηρεσιών που βασίζονται σε υποδομή διαδικτυακού νέφους (cloud), οριοθετεί πολύ δυσδιάκριτα τα ζητήματα δικαιοδοσίας για την πρόσβαση στα δεδομένα που αποθηκεύονται σ' αυτά. Συνεπώς η φυσική εγγύτητα και η ανάγκη για την παρουσία του δράστη με την τυπική μορφή όπως την γνωρίζουμε στον τόπο τέλεσης του ενός διαδικτυακού εγκλήματος, έχει πλέον χαθεί και δεν υφίσταται[9] (Casino et al., 2022; Γέρμανος & Γεωργίου, 2021).

Το ζήτημα αυτό γεννάται από την προβληματική κατάσταση του δύσκολου προσδιορισμού της ακριβούς τοποθεσίας, καθώς είναι δυσδιάκριτος ο εδαφικός εντοπισμός της υποδομής επί της οποίας είναι αποθηκευμένα τα δεδομένα αυτά, οι οποίες μπορεί να είναι εγκατεστημένες σε διάφορες τοποθεσίες σε διαφορετικές χώρες ή ακόμα και σε ηπείρους. Επομένως κάθε ηλεκτρονικό αποδεικτικό στοιχείο που είναι αποθηκευμένο σε διαφορετική τοποθεσία, τότε από την τελευταία προσδιορίζεται και η δικαιοδοσία και το νομικό καθεστώς που χρειάζεται να εφαρμοστεί για την απόκτηση αυτού[10] (Casino et al., 2022).

Ωστόσο χρειάζεται να λεχθεί ότι η διασυνοριακή διάσταση του εγκλήματος στον κυβερνοχώρο μαζί με άλλες διασυνοριακές απειλές είναι αυτές που έδωσαν την

[9] Έτσι για παράδειγμα, ο δράστης μίας κυβερνοεπίθεσης κατά την προσπάθεια του να εξαπατήσει το θύμα του, μπορεί να βρίσκεται στην Νιγηρία και ο στόχος αυτού σε κάποια ευρωπαϊκή πρωτεύουσα κράτους μέλους της Ένωσης (Βλ. Νιγηριανή απάτη). Ο καθορισμός της φυσικής τοποθεσίας του δράστη και της εγκληματικής υποδομής που αναπτύσσει γίνονται κρίσιμης σημασίας για τον προσδιορισμό του νομικού πλαισίου βάσει του οποίου θα αιτηθούν και θα αποκτήσουν οι αρχές επιβολής του νόμου, τα όποια ηλεκτρονικά αποδεικτικά στοιχεία τυχόν απαιτούνται για την διερεύνηση μιας τέτοιας υπόθεσης. Στις περισσότερες περιπτώσεις δεν είναι δυνατό να καθοριστεί η χώρα στην δικαιοδοσία της οποίας υπάγονται τα ανωτέρω καθώς και το εθνικό νομικό πλαίσιο που μπορεί να ρυθμίζει διαφορετικά ζητήματα από κράτος σε κράτος, αναφορικά με τη συλλογή ηλεκτρονικών αποδεικτικών στοιχείων (Γέρμανος & Γεωργίου, 2021).

[10] Έτσι για παράδειγμα ένα αίτημα για την παροχή στοιχείων μίας αρχής επιβολής του νόμου από ένα κράτος μέλος της Ένωσης προς την πάροχο υπηρεσιών διαδικτύου με την ονομασία «*Facebook ή Meta*» που έχει την ευρωπαϊκή της έδρα στην Ιρλανδία, θα αρκούσε αν η τελευταία συμμετείχε στην Οδηγία για την Ευρωπαϊκή Εντολή Έρευνας. Ωστόσο η Ιρλανδία, δεν συμμετέχει στον ποινικό αυτό θεσμό και για το λόγο αυτό απαιτείται η χρήση του εργαλείου της αμοιβαίας δικαστικής συνδρομής (Mutual Legal Assistance).

ώθηση στα κράτη μέλη και την Ένωση να αναλάβουν από κοινού δράση για να αντιμετωπίσουν απειλές και κινδύνους που εκφεύγουν από τα όρια των κρατών και τα συνήθη νομικά εργαλεία της εθνικής έννομης τάξης, γίνονταν πλέον μη λειτουργικά και αναποτελεσματικά (Foggetti, 2008).

1.5.5 Εμπόδια στη διεθνή συνεργασία

Σε διεθνές επίπεδο, δεν υπάρχει ένα κοινά αποδεκτό νομικό πλαίσιο για την ταχεία ανταλλαγή ηλεκτρονικών αποδεικτικών στοιχείων αλλά και για τη διατήρηση αυτών. Το γεγονός αυτό σημαίνει ότι ένας πάροχος υπηρεσιών διαδικτύου, μπορεί αρχικά να δεχθεί και να εγκρίνει ένα αίτημα διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων που τυχόν τηρεί, ωστόσο μπορεί να παρέλθει μεγάλο χρονικό διάστημα έως ότου τα ηλεκτρονικά αποδεικτικά στοιχεία τελικά διατεθούν στις αρχές επιβολής του νόμου μετά από σχετικό αίτημα που υπέβαλαν. Μεταξύ κρατών που δεν μετέχουν στην Ένωση ή μεταξύ κρατών μελών και τρίτων χωρών μία τέτοια παροχή ηλεκτρονικών αποδεικτικών στοιχείων θα μπορούσε να λάβει χώρα μέσω του θεσμού της αμοιβαίας δικαστικής συνδρομής (Mutual Legal Assistance)[11]. Ωστόσο η διαδικασία αυτή τείνει να θεωρείται πολύ αργή σε χρονικά πλαίσια για την απόκτηση των ηλεκτρονικών αποδεικτικών στοιχείων αλλά και για τη μεταβίβαση αυτών. Έτσι μέσω αυτού του θεσμού αυτού, το χρονικό διάστημα απόκτησης αυτών είναι σημαντικά μεγάλο ενώ τίθεται θέμα και της διαβίβασης αυτών, αφού διέρχεται από όλους τους παραλήπτες και αποδέκτες και όχι κατευθείαν στην αιτούσα αρχή (Ευρωπαϊκή Επιτροπή, 2018a).

Ωστόσο για υποθέσεις που αφορούν την δικαιοδοσία κρατών μελών της Ένωσης, η Ευρωπαϊκή Εντολή Έρευνας[12] (ΕΕΕ) είναι δυνατόν να συμβάλει στη βελτίωση του απαιτούμενου χρόνου για την πλειονότητα των κρατών μελών και όχι για όλα, όπως είδαμε προηγουμένως με το παράδειγμα της Ιρλανδίας. Ωστόσο ο θεσμός της Ευρωπαϊκής Εντολής Έρευνας, παρέχει ευρείες και γενικές διατάξεις που αφορούν όλα τα αποδεικτικά στοιχεία και όχι ειδικότερα τα ηλεκτρονικά αποδεικτικά στοιχεία, πράγμα που σημαίνει ότι απαιτείται να αναπτυχθούν πρόσθετα εργαλεία για

[11] Σύμβαση που καταρτίζεται από το Συμβούλιο βάσει του άρθρου 34 της συνθήκης για την Ευρωπαϊκή Ένωση, για την αμοιβαία δικαστική συνδρομή επί ποινικών υποθέσεων μεταξύ των κρατών μελών της Ευρωπαϊκής Ένωσης - Δήλωση του Συμβουλίου σχετικά με το άρθρο 10 παράγραφος 9 - Δήλωση του Ηνωμένου Βασιλείου σχετικά με το άρθρο 20 (Πηγή: Official Journal 197 , 12/07/2000 P. 0003 - 0023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A42000A0712%2801%29

[12] Στην Αγγλική γλώσσα και ως European Investigation Order (EIO).

τη διευκόλυνση της συλλογής ηλεκτρονικών αποδεικτικών στοιχείων στο πλαίσιο αυτής (Γέρμανος & Γεωργίου, 2021).

Την ίδια στιγμή η υιοθέτηση των Κοινών Ομάδων Έρευνας[13](Terziev, Petkov, & Dragomir, 2021), μπορεί να συνεισφέρει σημαντικά στην ενίσχυση των δυνατοτήτων των κρατών μελών, προκειμένου να είναι σε θέση να συνεργάζονται αποτελεσματικά και να υποβάλλουν κοινά αιτήματα παροχής ηλεκτρονικών αποδεικτικών στοιχείων προς παρόχους και όχι μεμονωμένα από τις αρχές επιβολής του νόμου κάθε κράτους μέλους (Zaharieva, 2017; Γέρμανος & Γεωργίου, 2021). Με τον τρόπο αυτό, οι Πάροχοι υπηρεσιών διαδικτύου και επικοινωνιών θα γίνονται αποδέκτες ενός και μόνο αιτήματος που τυχόν αφορά την ίδια υπόθεση και όχι πολλαπλών αιτημάτων από διαφορετικές Υπηρεσίες και Αρχές επιβολής του νόμου που τυχόν έχουν αποφασίσει να διερευνήσουν μία ποινική υπόθεση εγκλήματος στον κυβερνοχώρο, όπως για παράδειγμα αυτό μεταξύ της Νότιας Κορέας και της Ένωσης (Kim, 2022).

[13]Απόφαση-πλαίσιο 2002/465/ΔΕΥ του Συμβουλίου, της 13ης Ιουνίου 2002, σχετικά με τις κοινές ομάδες έρευνας (ΕΕ L 162 της 20.6.2002, σ. 1).

Κεφάλαιο Δεύτερο

2. Ηλεκτρονικά αποδεικτικά στοιχεία (e-evidence)

Στο προηγούμενο κεφάλαιο αναλύθηκε το πλαίσιο μέσα στο οποίο εντάσσονται τα ζητήματα συλλογής αποδεικτικών στοιχείων στον κυβερνοχώρο και στο διαδίκτυο και είδαμε τις βασικές προκλήσεις που αντιμετωπίζουν οι αρμόδιες αρχές των κρατών μελών στην μάχη κατά των εγκλημάτων που διαπράττονται ηλεκτρονικά. Έγινε αντιληπτό ότι όλες οι σύγχρονες απειλές και κίνδυνοι όπως η τρομοκρατία, το οργανωμένο έγκλημα ακόμα και κρατικοί δρώντες, εκμεταλλεύονται το διαδίκτυο και τις υπηρεσίες που προσφέρει για ίδιους σκοπούς με κακοβουλία.

Όλα τα παραπάνω ζητήματα που είδαμε είτε ως εγκλήματα είτε ως επιθέσεις σε βάρος κρατικών δρώντων, προκειμένου να αποδειχτούν αλλά και να χρησιμοποιηθούν ως απόδειξη στα δικαστήρια ή σε κάποια άλλη διεθνή διαφορά, απαιτείται να αποδειχτούν με χειροπιαστό τρόπο. Η απόδειξη και η στοιχειοθέτηση αυτών των εγκλημάτων όπως και στα εγκλήματα του κοινού ποινικού δίκαιού (κλοπή, ανθρωποκτονία κλπ.) απαιτούν αποδείξεις και αποδεικτικά στοιχεία. Το ίδιο πράγματι συμβαίνει και για τα εγκλήματα που διαπράττονται στον κυβερνοχώρο.

2.1 Η ανάγκη για απόκτηση ηλεκτρονικών αποδεικτικών στοιχείων

Μελετώντας τη βιβλιογραφία θα παρατηρήσει κανείς ότι το ζήτημα της καταπολέμησης της εγκληματικότητάς στον κυβερνοχώρο συνδέεται σε μεγάλο βαθμό με τη δυνατότητα των αρχών επιβολής του νόμου, να αποκτούν αποδεικτικά στοιχεία που σχετίζονται με αυτά τα αδικήματα από παρόχους υπηρεσιών διαδικτύου (Rojszczak, 2022). Το κύριο πρόβλημα των εγκλημάτων αυτών, είναι ότι οι αρχές επιβολής του νόμου, δυσκολεύονται να αποκτήσουν αποδεικτικά στοιχεία για την στοιχειοθέτηση των εγκλημάτων αυτών, που έχουν αναπτυχθεί μόλις τα τελευταία χρόνια και συνδέονται με την ανάπτυξη του διαδικτύου και την ευρεία χρήση συσκευών ή ηλεκτρονικών υπολογιστών που συνδέονται σ’ αυτό, όπως είδαμε και προηγουμένως στην παρούσα.

Όπως γίνεται εύκολα αντιληπτό, απαιτούνται αποδεικτικά στοιχεία που να είναι σε θέση να αποδείξουν ένα γεγονός ή ένα συμβάν για ένα έγκλημα που έχει τελεστεί στον κυβερνοχώρο και ενδεχομένως επιφέρει συνέπειες και στον πραγματικό κόσμο με οποιοδήποτε τρόπο (περιουσιακή απώλεια, απώλεια χρημάτων φήμης κλπ.). Όταν διαπράττεται ένα έγκλημα στον πραγματικό κόσμο, οι

αστυνομικές και δικαστικές αρχές, καλούνται να συλλέξουν αποδείξεις προκειμένου να στοιχειοθετηθεί αυτό το αδίκημα (Blažič & Klobučar, 2020a; Buono, 2019).

Το ίδιο συμβαίνει και με τη διάπραξη ενός κυβερνοεγκλήματος, όταν στο πλαίσιο των ποινικών διαδικασιών, μπορεί να χρειαστεί οι αρχές να βασιστούν επάνω σε πληροφορίες που δημιουργούνται, διανεμήθηκαν ή αποθηκεύονται σε πληθώρα ηλεκτρονικών συσκευών (Buono, 2019). Ορισμένα χαρακτηριστικά παραδείγματα ψηφιακών συσκευών περιλαμβάνουν υπολογιστές, συσκευές αποθήκευσης, κάρτες μνήμης, κινητά (έξυπνα) τηλέφωνα (smartphone), ψηφιακές κάμερες και φορητή τεχνολογία όπως τα έξυπνα ρολόγια. Τέτοιες συσκευές είναι δυνατόν να δημιουργούν πολλές ευκαιρίες για τη διάπραξη εγκλημάτων μεταξύ πολλών άλλων, το phishing, η κλοπή ταυτότητας (id-theft) καθώς επίσης και η απάτη στο διαδίκτυο (Blažič & Klobučar, 2020a).

Οι ηλεκτρονικές πληροφορίες και τα αποδεικτικά στοιχεία, που παράγονται από αυτές τις συσκευές, είναι συχνά σημαντικές για την απόδειξη ή την διάψευση ενός γεγονότος ή κάποιου άλλου στοιχείου, σχετικά με την ενοχή ή την αθωότητα του κατηγορουμένου και ως εκ τούτου όλα τα στοιχεία αυτά, δύναται να αποτελούν μέρος του συνόλου των αποδεικτικών στοιχείων ενώπιον της ακροαματικής διαδικασίας (Buono, 2019). Όλες αυτές τις πληροφορίες μπορούμε να τις χαρακτηρίσουμε γενικά ως ηλεκτρονικά αποδεικτικά στοιχεία (e-evidence), (Ευρωπαϊκή Επιτροπή, 2018a).

2.2 Συλλογή ηλεκτρονικών αποδείξεων στον χώρο της Ένωσης

Τα σύγχρονα ηλεκτρονικά συστήματα πληροφοριών και επικοινωνιών είναι σε θέση να περιέχουν στοιχεία που συμβάλλουν στον εντοπισμό των δραστών εγκλημάτων που διαπράττονται στον πραγματικό κόσμο, είτε στον ψηφιακό κόσμο και έχουν όμως εξίσου επιπτώσεις και στον πραγματικό κόσμο. Στον πραγματικό κόσμο ένας δράστης μίας ανθρωποκτονίας, είναι πολύ πιθανό να αφήσει στον τόπο του εγκλήματος, ίχνη, πειστήρια, ή αποτυπώματα και τα οποία συλλέγουν οι αρχές επιβολής του νόμου, για να αποκαλύψουν την υπόθεση ή για να τεκμηριώσουν το αδίκημα που διαπράχθηκε. Πολλές φορές ένα αδίκημα στον πραγματικό κόσμο, να μπορεί να αποδειχθεί και με συμπληρωματικά αποδεικτικά στοιχεία που παρέχονται από παρόχους διαδικτύου ή άλλων διαδικτυακών υπηρεσιών και σχετίζονται με αυτό. Την ίδια στιγμή, ένας δράστης μίας επίθεσης στον κυβερνοχώρο είναι δυνατόν να

αφήνει στο πέρασμα του μέσα στο διαδίκτυο, ένα ψηφιακό μονοπάτι ιχνών και πειστηρίων από το οποίο διήλθαν για να διαπράξουν ένα αδίκημα στον κυβερνοχώρο (είτε αυτό πλήττει ένα άτομο είτε ένα κράτος ή μία υποδομή). Η διατήρηση αυτών των ψηφιακών ιχνών και πειστηρίων έχει βασική σημασία για τις ποινικές έρευνες των αρχών των κρατών μελών, καθώς επάνω σ' αυτά τα αποδεικτικά στοιχεία είναι δυνατόν να τεκμηριωθεί και να αποδειχθεί στο ακροατήριο το αδίκημα που έχει διαπραχθεί (Commission Staff Working Document, 2018).

Σε ορισμένες περιπτώσεις, τα ψηφιακά στοιχεία δεν είναι μόνο συμπληρωματικά προς άλλα αποδεικτικά στοιχεία που ήδη υπάρχουν αλλά και η βασική πηγή αποδεικτικών στοιχείων, χωρίς την οποία είναι αδύνατο όχι μόνο να προσδιοριστεί ο δράστης αλλά και να ανακατασκευαστεί μια αλυσίδα γεγονότων τα οποία δείχνουν την ροή των πραγμάτων και αναπαριστούν σε χρονική σειρά, το πως διαπράχθηκε ένα αδίκημα στον κυβερνοχώρο (Rojszczak, 2022).

Αρκεί να πούμε ότι η δίωξη ορισμένων τύπων σοβαρών εγκλημάτων για την Ένωση, όπως η νομιμοποίηση εσόδων από παράνομες δραστηριότητες, βασίζεται εκ των πραγμάτων σε αποδεικτικά στοιχεία που εξάγονται τις περισσότερες φορές από ηλεκτρονικά χρηματοπιστωτικά συστήματα που τηρούνται σε τράπεζες ή άλλους χρηματοπιστωτικούς οργανισμούς ή ιδρύματα. Σύμφωνα με την ανάλυση της Ευρωπαϊκής Επιτροπής που είχε πραγματοποιηθεί προκειμένου να προτάξει το νέο πακέτο ευρωπαϊκής νομοθεσίας για τα ηλεκτρονικά αποδεικτικά στοιχεία, δείχνει ότι απαιτούνται ηλεκτρονικά αποδεικτικά στοιχεία σε περίπου 85% από τις ήδη τρέχουσες ποινικές υποθέσεις και στα δύο τρίτα των περιπτώσεων αυτών, τα ηλεκτρονικά αποδεικτικά στοιχεία βρίσκονται σε παρόχους υπηρεσιών διαδικτύου ή επικοινωνιών που εδρεύουν σε άλλη δικαιοδοσία πέραν αυτή των κρατών μελών, από αυτή που ερευνάται το αδίκημα ή μία ποινική υπόθεση (Commission Staff Working Document, 2018; Rojszczak, 2022).

Για τους λόγους αυτούς, οι αρχές των κρατών μελών χρειάζονται πρόσβαση σε δεδομένα που θα μπορούσαν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία και αποθηκεύονται εκτός της χώρας τους σε παρόχους υπηρεσιών σε άλλα κράτη μέλη ή τρίτες χώρες (Ευρωπαϊκή Επιτροπή, 2018a). Έτσι όταν ο πάροχος υπηρεσιών διαδικτύου είναι σε άλλη χώρα από αυτήν που διαπράττεται ένα έγκλημα, τότε οι αρχές αναπτύσσουν δράση, είτε μέσω της αμοιβαίας δικαστικής συνδρομής αν η χώρα αυτή είναι εκτός της Ένωσης, είτε μέσω της Ευρωπαϊκής Εντολής Έρευνας

(European Investigation Order-EIO)[14] αν πρόκειται για κράτη μέλη, (Μιχαηλίδου, 2018).

Η Ευρωπαϊκή Εντολή Έρευνας (ΕΕΕ) όπως έχει υιοθετηθεί, προσέφερε μια ολοκληρωμένη λύση στον τομέα της διασυνοριακής συλλογής όλων των τύπων αποδεικτικών στοιχείων στον ΧΕΑΔ, που θα αντικαθιστούσε τους ήδη υπάρχοντες τρόπους (αμοιβαία δικαστική συνδρομή) για την απόκτηση όλων των τύπων αποδεικτικών στοιχείων. Ωστόσο, αν και δεν είχε παρέλθει ούτε ένας χρόνος από την προθεσμία για την υιοθέτησης της ΕΕΕ, η Επιτροπή πρότεινε ένα νέο πακέτο νομοθετικών ρυθμίσεων αναφορικά με τη συλλογή και την διατήρηση των ηλεκτρονικών αποδεικτικών στοιχείων, γνωστό και ως «***πακέτο e-evidence***», (Buono, 2019).

Αυτή η πρωτοβουλία για την υιοθέτηση νέων κανόνων γύρω από τα ηλεκτρονικά αποδεικτικά στοιχεία, γεννήθηκε από μια αυξανόμενη απογοήτευση στη συγκέντρωση αυτού του είδους αποδεικτικών στοιχείων από τις αρχές επιβολής του νόμου και με βάση τις προκλήσεις που είδαμε προηγουμένως (Commission Staff Working Document, 2018). Ταυτόχρονα δημιουργήθηκε η πεποίθηση ότι η ΕΕΕ, δεν είναι κατάλληλο μέσο για το σκοπό αυτό (Tosza, 2018, 2020). Η ανάγκη για ψηφιακά αποδεικτικά στοιχεία, αποτελεί άμεση συνέπεια της ραγδαίας ανόδου της τεχνολογίας του διαδικτύου και του τρόπου με τον οποίο διευκολύνει την επικοινωνία και άλλες συναλλαγές ή υπηρεσίες στην καθημερινή ζωή των πολιτών (Rojszczak, 2022). Για το λόγο αυτό, η απόκτηση ηλεκτρονικών αποδεικτικών στοιχείων από τις αρμόδιες αρχές για σκοπούς δίωξης και έρευνας των εγκλημάτων, απαιτεί την ίδια ταχύτητα με την οποία δημιουργούνται και διακινούνται αυτά (Depauw, 2018; Mitsilegas, 2018).

Από τον τρόπο με τον οποίο η Επιτροπή επιλέγει να εισάγει ένα νέο πακέτο νομοθετικών ρυθμίσεων αναφορικά με τα ηλεκτρονικά αποδεικτικά στοιχεία, δείχνει ότι διαχωρίζει τα αποδεικτικά στοιχεία ως σύνολο και επιλέγει νέες μορφές νομικών εργαλείων για την συλλογή αυτών. Ωστόσο, η αντίδραση αυτή της Επιτροπής για τον διαχωρισμό των αποδεικτικών στοιχείων, είναι δικαιολογημένη και έχει επαρκή βάση στην οποία στηρίζεται (Commission Staff Working Document, 2018). Τα ηλεκτρονικά αποδεικτικά στοιχεία όπως είδαμε και προηγουμένως χαρακτηρίζονται από τον ευμετάβλητο χαρακτήρα και την παροδικότητα της διατήρησης τους,

[14]Οδηγία 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

εξαιτίας του μεγέθους και της ταχύτητας με την οποία παράγονται (Blažič & Klobučar, 2020b; Chavleski & Galev, 2019). Για το λόγο αυτό, διαφέρουν με διάφορους τρόπους από τα υπόλοιπα αποδεικτικά στοιχεία της «*πραγματικής ζωής*», που καθιστούν το τρέχον νομικό πλαίσιο εξαιρετικά δυσχερές για την επιβολή του νόμου, για εγκλήματα που αφορούν το διαδίκτυο ή τον κυβερνοχώρο ή για τη δίωξη εγκλημάτων όπου τα ηλεκτρονικά αποδεικτικά στοιχεία αποτελούν συμπληρωματικά στοιχεία (Jerman Blažič & Klobučar, 2019).

Ένα από τα σημαντικότερα εμπόδια που αντιμετωπίζουν οι αρχές επιβολής του νόμου είναι το γεγονός ότι τα δεδομένα που χρειάζονται, συχνά αποθηκεύονται στο εξωτερικό ή από έναν πάροχο ξένων υπηρεσιών. Και τα δύο θεσμικά εργαλεία της Ένωσης (ευρωπαϊκή εντολή έρευνας και πακέτο προτάσεων για τα ηλεκτρονικά αποδεικτικά στοιχεία) σχεδιάστηκαν λόγω της ανάγκης να συγκεντρωθούν αποδεικτικά στοιχεία σε υποθέσεις πέρα και έξω από τα σύνορα των κρατών μελών (Biasiotti, Cannataci, Mifsud Bonnici, & Turchi, 2018).

Ωστόσο, το διακρατικό στοιχείο είναι διαφορετικό για κάθε ένα από τα εργαλεία αυτά. Έτσι στην ΕΕΕ, τα απαιτούμενα αποδεικτικά στοιχεία είναι στο εξωτερικό και συγκεκριμένα σε άλλο κράτος μέλος ενώ με τις προταθείσες διατάξεις της ευρωπαϊκής εντολής παραγωγής και διατήρησης δεδομένων τα αποδεικτικά στοιχεία είναι σε κάποιον διακομιστή κάποιου παρόχου που έχει την έδρα του σε άλλο κράτος μέλος ή παρέχει υπηρεσίες σ' αυτό και κατ' επέκταση στον χώρο της Ένωσης (Armada, 2015). Και τα δύο αυτά θεσμικά εργαλεία έχουν ως υποκείμενο ευρωπαίους πολίτες οι οποίοι υπόκεινται στον μηχανισμό ποινικής έρευνας άλλου κράτους μέλους της Ένωσης, ωστόσο, με διαφορετικό τρόπο για κάθε μία περίπτωση, όπως θα αναλυθεί και στη συνέχεια.

Κεφάλαιο Τρίτο

3. Η Ευρωπαϊκή Εντολή Έρευνας

Η Ευρωπαϊκή Εντολή Έρευνας[15] (εφεξής αναφερόμενη και ως ΕΕΕ), η οποία υιοθετήθηκε από την Ένωση με την Οδηγία 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014[16] (ενσωματώθηκε στη χώρα μας με το ν. 4489/2017), είναι σημαντική να περιγραφεί στην παρούσα, καθώς αποτελεί τη βάση και τα θεμέλια επάνω στην οποία αναπτύσσεται η νέα πρόταση της Επιτροπής για τα ηλεκτρονικά αποδεικτικά στοιχεία, όπως θα αναλυθεί και στη συνέχεια.

Γίνεται αντιληπτό ότι μετά την υιοθέτηση της ΕΕΕ στα κράτη μέλη και σε σύντομο χρόνο πριν ακόμα την υιοθέτηση της Οδηγίας αυτής από τα κράτη μέλη, η Επιτροπή πήρε το πράσινο φως, προκειμένου να προωθήσει την ευρωπαϊκή ολοκλήρωση στο πεδίο της συλλογής και απόκτησης των ηλεκτρονικών αποδεικτικών στοιχείων, κατανοώντας την ειδοποιό διαφορά αυτών και το πεδίο στο οποίο αναπτύσσονται, το οποίο όπως είδαμε μπορεί να εκφεύγει από τα όρια των κρατών μελών. Πέραν αυτών χρειάζεται να σημειωθεί ότι την ίδια περίοδο η ανάγκη για την ανεύρεση λύσεων για την απόκτηση ηλεκτρονικών αποδείξεων, ενισχύεται ακόμη περισσότερο και με τις τρομοκρατικές επιθέσεις που σημειώνονται στην Ευρώπη και στις Βρυξέλλες τον Μάρτιο του 2016[17], οι οποίες δρουν καταλυτικά όπως φάνηκε και από την κοινή δήλωση των αρμόδιων Υπουργών της Ένωσης, για την αντιμετώπιση αυτού του περίπλοκου ζητήματος, όπως χαρακτηρίστηκε για την απόκτηση ψηφιακών αποδεικτικών στοιχείων(Tinoco-Pastrana, 2020).

---

[15] Ο όρος που χρησιμοποιείται στην Αγγλική γλώσσα και χρησιμοποιήθηκε κυρίως για την αναζήτηση σχετικής βιβλιογραφίας είναι European Investigation Order (EIO).

[16] Οδηγία 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[17] Η Κοινή δήλωση των Υπουργών Δικαιοσύνης και Εσωτερικών Υποθέσεων της ΕΕ και αντιπροσώπων των θεσμικών οργάνων της Ένωσης για τις τρομοκρατικές επιθέσεις της 22ας Μαρτίου 2016 στις Βρυξέλλες ανέφερε μεταξύ άλλων ότι απαιτείται «*να εξευρεθούν τρόποι, κατά προτεραιότητα, ώστε να εξασφαλίζονται και να λαμβάνονται με τρόπο πιο γρήγορο και αποτελεσματικό ψηφιακά αποδεικτικά στοιχεία, με την ενίσχυση της συνεργασίας με τρίτες χώρες και με παρόχους υπηρεσιών που δραστηριοποιούνται σε ευρωπαϊκό έδαφος, προκειμένου να βελτιωθεί η συμμόρφωση με τη νομοθεσία της ΕΕ και των κρατών μελών και οι άμεσες επαφές με τις αρχές επιβολής του νόμου. Κατά τη σύνοδο του Συμβουλίου τον Ιούνιο θα προσδιοριστούν συγκεκριμένα μέτρα για την αντιμετώπιση αυτού του περίπλοκου ζητήματος.*». Πηγή: https://www.consilium.europa.eu/el/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/.

Θα μπορούσε ίσως να σημειωθεί ότι, μετά το ευρωπαϊκό ένταλμα σύλληψης, η ΕΕΕ αποτελεί το δεύτερο καίριο «*μέτρο εφαρμογής*» της αμοιβαίας αναγνώρισης ποινικών αποφάσεων εντός της Ένωσης ως «*χώρου ελευθερίας, ασφάλειας και δικαιοσύνης*», που κατατείνει στην αποτελεσματική συνεργασία των κρατών μελών στον πεδίο της συλλογής αποδεικτικών στοιχείων σε ποινικές υποθέσεις (Αρβανίτης, 2021).

Η ΕΕΕ, δεν ήταν η μοναδική προσπάθεια για την υιοθέτηση ενός κοινού αποδεκτού μοντέλου για την υποβολή και το παραδεκτό των αποδεικτικών στοιχείων ανάμεσα στα κράτη μέλη[18]. Αφότου εκδόθηκαν οι αποφάσεις-πλαίσια 2003/577/ΔΕΥ και 2008/978/ΔΕΥ διαπιστώθηκε ότι το πλαίσιο για τη συγκέντρωση αποδεικτικών στοιχείων ήταν υπερβολικά κατακερματισμένο και περίπλοκο και για το λόγο αυτό απαιτούνται νέα προσέγγιση[19].

Η ΕΕΕ, αντικαθιστά το συνονθύλευμα των μέσων και νομικών εργαλείων που προβλεπόταν παλαιότερα για την συλλογή αποδεικτικών στοιχείων, με μία μόνο τυποποιημένη εντολή, για όλους τους τύπους αποδεικτικών στοιχείων, με δύο εξαιρέσεις: α) τη δημιουργία ή τη συγκέντρωση αποδεικτικών στοιχείων σε κοινές ομάδες έρευνας (Joint Investigation Teams)[20] και β) τη διασυνοριακή επιτήρηση που προβλέπεται στη σύμβαση που εφαρμόζει τη συμφωνία Schengen[21]. Η ΕΕΕ,

[18] Σκέψη υπ' αριθμό 3 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1): «*Η Απόφαση-πλαίσιο 2003/577/ΔΕΥ του Συμβουλίου, της 22ας Ιουλίου 2003, σχετικά με την εκτέλεση των αποφάσεων δέσμευσης περιουσιακών ή αποδεικτικών στοιχείων στην Ευρωπαϊκή Ένωση (ΕΕ L 196 της 2.8.2003, σ. 45), ανταποκρίθηκε στην ανάγκη άμεσης αμοιβαίας αναγνώρισης των αποφάσεων που επιδιώκουν να προλαμβάνεται η καταστροφή, η παραποίηση, η μετατόπιση, η μεταφορά ή η διάθεση αποδεικτικών στοιχείων. Εντούτοις, επειδή η νομική αυτή πράξη περιορίζεται στη δέσμευση, η απόφαση δέσμευσης πρέπει να συνοδεύεται από χωριστό αίτημα για τη διαβίβαση των αποδεικτικών στοιχείων στο κράτος που εκδίδει την εντολή («κράτος έκδοσης») σύμφωνα με τους κανόνες περί αμοιβαίας συνδρομής επί ποινικών υποθέσεων. Αυτό οδηγεί σε διαδικασία δύο σταδίων, η οποία αποβαίνει σε βάρος της αποδοτικότητας. Επιπλέον, αυτό το καθεστώς συνυπάρχει με τα παραδοσιακά μέσα συνεργασίας και επομένως σπάνια χρησιμοποιείται από τις αρμόδιες αρχές.*»

[19] Σκέψη υπ' αριθμό 5 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[20] Άρθρο 3 της Οδηγίας 2014/41/ΕΕ με τίτλο «Πεδίο Εφαρμογής»: «*Η ΕΕΕ καλύπτει κάθε ερευνητικό μέτρο, εκτός από τη σύσταση κοινής ομάδας έρευνας και τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο κοινής ομάδας έρευνας κατά τα οριζόμενα στο άρθρο 13 της σύμβασης για την αμοιβαία δικαστική συνδρομή επί ποινικών υποθέσεων μεταξύ των κρατών μελών της Ευρωπαϊκής Ένωσης (14) («σύμβαση») και στην απόφαση-πλαίσιο 2002/465/ΔΕΥ του Συμβουλίου (15), πλην των περιπτώσεων εφαρμογής του άρθρου 13 παράγραφος 8 της σύμβασης και του άρθρου 1 παράγραφος 8 της απόφασης-πλαισίου.*»

[21] Σκέψη υπ' αριθμό 9 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της

βασίζεται στην αμοιβαία αναγνώριση των αποφάσεων μεταξύ των κρατών μελών, με εντολές που κυκλοφορούν μεταξύ τους και εκτελούνται από τις αρμόδιες αρχές με διάφορους μη υποχρεωτικούς λόγους άρνησης εκτέλεσης αυτών. Για το λόγο αυτό απαιτείται ένα κράτος μέλος «*έκδοσης*» που εκδίδει την ΕΕΕ, να απευθύνεται στις αρχές ενός άλλου κράτους μέλους «*εκτέλεσης*».

Η οδηγία υιοθετήθηκε μετά από μια σημαντική συζήτηση που επικεντρώθηκε κυρίως σε θέματα θεμελιωδών δικαιωμάτων και στο παραδεκτό των αποδεικτικών στοιχείων που υποβάλλονται στο δικαστήριο (Allegrezza, 2014). Ενώ η ΕΕΕ ως νομικό εργαλείο, προβλέπει ένα ενοποιημένο πλαίσιο, δεν επιχειρεί να ενοποιήσει ή να εναρμονίσει το συνολικό νομικό πλαίσιο των αποδεικτικών στοιχείων που ισχύει στα διάφορα κράτη μέλη, αφήνοντας το πεδίο αυτό ανοικτό στις διάφορες αποφάσεις των κρατών μελών, αναφορικά με τους όρους έκδοσης μίας ΕΕΕ, τις αρμόδιες αρχές που εκδίδουν ΕΕΕ καθώς επίσης και τους συγκεκριμένους τύπους μέτρων που επιθυμεί κάθε κράτος μέλος να λάβει με την ΕΕΕ, όπως τέλος τα ένδικα μέσα κατά της ΕΕΕ, που ρυθμίζονται επίσης από το εθνικό δίκαιο. Τέλος, η περίοδος υιοθέτησης της Οδηγίας για την ΕΕΕ, από τα κράτη μέλη διήρκησε περίπου 3 χρόνια.

Έτσι η ΕΕΕ διαφοροποιείται και αντίθετα με το Ευρωπαϊκό Ένταλμα Σύλληψης όπου το επίκεντρο της απόφασης είναι η λήψη του ίδιου του μέτρου αυτού για τη σύλληψη του ατόμου σε άλλο κράτος και όχι τυχόν αποδεικτικά στοιχεία που συνδέονται με αυτό. Στην περίπτωση της ΕΕΕ, η λήψη του μέτρου είναι η απόκτηση αποδεικτικών στοιχείων, ωστόσο δεν αποκλείεται να συνδέεται και με ήδη αποδεικτικά στοιχεία που τυχόν κατέχουν οι αρμόδιες αρχές. Η ΕΕΕ, είναι δυνατόν να εκδοθεί για κάθε είδους ερευνητικό μέτρο, με τις δύο εξαιρέσεις που αναφέρθηκαν προηγουμένως. Συνεπώς με αυτήν την έννοια μπορεί να χρησιμοποιηθεί για τη λήψη ηλεκτρονικών αποδεικτικών στοιχείων από πάροχο σε άλλο κράτος μέλος, που συμμετέχει στην Οδηγία της ΕΕΕ.

Ωστόσο από το γενικό πλαίσιο εξαιρούνται ορισμένα μέτρα όπως είναι η παρακολούθηση τηλεπικοινωνιών στο κράτος μέλος το οποίο πρέπει να παράσχει την

1.5.2014, σ. 1): «*Η παρούσα οδηγία δεν θα πρέπει να εφαρμόζεται στους διασυνοριακούς ελέγχους βάσει της σύμβασης για την εφαρμογή της συμφωνίας Σένγκεν, η οποία αναφέρεται στην Σύμβαση εφαρμογής της συμφωνίας του Σένγκεν της 14ης Ιουνίου 1985 μεταξύ των κυβερνήσεων των κρατών της Οικονομικής Ένωσης Μπενελούξ, της Ομοσπονδιακής Δημοκρατίας της Γερμανίας και της Γαλλικής Δημοκρατίας, σχετικά με τη σταδιακή κατάργηση των ελέγχων στα κοινά σύνορα (ΕΕ L 239 της 22.9.2000, σ. 19).*»

τεχνική βοήθεια με ορισμένες προϋποθέσεις και για τις οποίες ρυθμίζονται σχετικά (αρ. 30 & 31 της Οδηγίας ΕΕΕ) καθώς επίσης και η συγκέντρωση πληροφοριών σχετικά με τους τραπεζικούς και άλλους χρηματοπιστωτικούς λογαριασμούς ή λειτουργίες, τις ελεγχόμενες παραδόσεις ή τις συγκεκαλυμμένες έρευνες.

Η Ευρωπαϊκή Εντολή Έρευνας (ΕΕΕ) είναι δικαστική απόφαση ή απόφαση την οποία εκδίδει ή επικυρώνει δικαστική αρχή κράτους μέλους της Ένωσης («κράτος έκδοσης») με σκοπό την εκτέλεση ενός ή περισσότερων συγκεκριμένων ερευνητικών μέτρων σε άλλο κράτος μέλος («κράτος εκτέλεσης») για τη λήψη αποδεικτικών στοιχείων.

Η ΕΕΕ εκδίδεται στο πλαίσιο: α) ποινικής διαδικασίας που κινείται από δικαστική αρχή ή μπορεί να κινηθεί ενώπιον της για αξιόποινη πράξη βάσει της νομοθεσίας του κράτους έκδοσης, β) διαδικασίας που κινούν διοικητικές αρχές, όταν αυτή αφορά πράξεις που τιμωρούνται βάσει της νομοθεσίας του κράτους έκδοσης ως παραβάσεις κανόνων δικαίου και όταν η απόφαση της διοικητικής ή δικαστικής αρχής μπορεί να οδηγήσει σε δίκη ενώπιον δικαστηρίου που έχει δικαιοδοσία σε ποινικές υποθέσεις, γ) διαδικασίας που κινούν δικαστικές αρχές, όταν αυτή αφορά πράξεις που τιμωρούνται βάσει της νομοθεσίας του κράτους έκδοσης ως παραβάσεις κανόνων δικαίου και όταν η απόφαση της διοικητικής ή δικαστικής αρχής μπορεί να οδηγήσει σε δίκη ενώπιον δικαστηρίου που έχει δικαιοδοσία σε ποινικές υποθέσεις και δ) διαδικασιών των περιπτώσεων α΄, β΄ και γ΄, οι οποίες αφορούν αξιόποινες πράξεις ή παραβάσεις που μπορούν να στοιχειοθετήσουν την ευθύνη ή να επισύρουν την τιμωρία νομικού προσώπου στο κράτος έκδοσης.

Ωστόσο χρειάζεται να σημειωθεί ότι για τις ανωτέρω περιπτώσεις α) και β) και γ) το κράτος εκτέλεσης μπορεί ενδεχομένως να αρνηθεί να εκτελέσει την ΕΕΕ που έχει εκδοθεί αν το ερευνητικό μέτρο δεν θα επιτρεπόταν από το δίκαιο του κράτους εκτέλεσης σε παρόμοια εγχώρια υπόθεση[22].

Αρμόδιες αρχές για την έκδοση μίας ΕΕΕ είναι οι δικαστικές αρχές του κράτους έκδοσης και η οδηγία ορίζει ποιες μπορεί να είναι αυτές οι αρχές που θα ορίσουν τα κράτη μέλη. Έτσι περιοριστικά ως αρχή έκδοσης μίας ΕΕΕ μπορεί να

[22] Αρ. 11 παρ. 1 περ. γ' της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

είναι ένας δικαστής, το δικαστήριο, ο ανακριτής ή ο εισαγγελέας με αρμοδιότητα στη συγκεκριμένη υπόθεση[23].

Επιπλέον μπορεί να εκδοθεί ΕΕΕ και από κάθε άλλη αρμόδια αρχή ορισθείσα από το κράτος έκδοσης η οποία στη συγκεκριμένη περίπτωση ενεργεί ως ανακριτική αρχή σε ποινικές διαδικασίες, αρμόδια να διατάσσει τη συγκέντρωση αποδεικτικών στοιχείων σύμφωνα με το εθνικό δίκαιο. Επιπλέον, προτού διαβιβαστεί στην αρχή εκτέλεσης, η ΕΕΕ επικυρώνεται, αφού εξεταστεί αν τηρεί τις προϋποθέσεις της παρούσας οδηγίας για την έκδοση ΕΕΕ, ιδίως αυτές του άρθρου 6 παράγραφος 1 της Οδηγίας 2014/41/ΕΕ, από δικαστή, δικαστήριο, ανακριτή ή εισαγγελέα στο κράτος έκδοσης[24]. Αν η ΕΕΕ έχει επικυρωθεί από δικαστική αρχή, η αρχή αυτή μπορεί επίσης να θεωρηθεί αρχή έκδοσης για τους σκοπούς της διαβίβασης της ΕΕΕ.

Παρατηρείται ότι στη δεύτερη περίπτωση όπου η ΕΕΕ εκδίδεται από άλλη αρχή πέραν της δικαστικής, απαιτείται να επικυρωθεί από την αρμόδια δικαστική αρχή του κράτους έκδοσης για το αν πληροί συγκεκριμένες προϋποθέσεις. Στην περίπτωση αυτή η επικύρωση χρειάζεται να έχει ουσιαστικό χαρακτήρα λαμβάνοντας υπόψη ότι η έκδοση της ΕΕΕ είναι απαραίτητη και αναλογική για τους σκοπούς της διαδικασίας του άρθρου 4 της Οδηγίας 2014/41/ΕΕ, λαμβανομένων υπόψη των δικαιωμάτων του υπόπτου ή κατηγορουμένου και το ή τα ερευνητικά μέτρα που προβλέπονται στην ΕΕΕ θα μπορούσαν να είχαν διαταχθεί υπό τις ίδιες προϋποθέσεις σε παρόμοια εγχώρια υπόθεση[25].

Η στάθμιση του ερευνητικού μέτρου υπό τις αρχές της αναγκαιότητας και της αναλογικότητας, είναι σημαντική καθώς χρειάζεται να προβλέπεται και σε παρόμοια υπόθεση που ισχύει και για το κράτος έκδοσης. Έτσι οι συνθήκες αυτές αφήνονται να ρυθμιστούν από κάθε κράτος μέλος ωστόσο η αρχή του διττού αξιόποινου τόσο στο κράτος έκδοσης όσο και στο κράτος εκτέλεσης, δεν περιλαμβάνεται ως προαπαιτούμενο για την έκδοση της ΕΕΕ αλλά περισσότερο αποτελεί προαιρετικό

[23] Αρ. 2 περ. γ) υποπερίπτωση i) της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[24] Μάλιστα η μη επικύρωση από δικαστική αρχή αποτελεί και λόγο επιστροφής της ΕΕΕ από το κράτος εκτέλεσης, σύμφωνα με το αρ. 9 παρ. 3 της της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[25] Αρ. 5 παρ. 1 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

λόγο μη αποδοχής εκτέλεσης της ΕΕΕ από την πλευρά του κράτους εκτέλεσης. Μάλιστα στην περίπτωση της παρακολούθησης τηλεπικοινωνιών με την τεχνική βοήθεια άλλου κράτους μέλους (αρ. 30 της Οδηγίας ΕΕΕ) απαιτείται ειδική αιτιολόγηση και η αρχή έκδοσης αναφέρει διά της ΕΕΕ το λόγο για τον οποίο θεωρεί ότι τα αναφερόμενα εκεί ερευνητικά μέτρα έχουν σημασία για την ποινική διαδικασία[26]. Σημαντικό είναι να σημειωθεί ότι, την έκδοση ΕΕΕ μπορεί να ζητήσει ύποπτος ή κατηγορούμενος (ή δικηγόρος εξ ονόματός του) στο πλαίσιο των δικαιωμάτων υπεράσπισης που προβλέπει το εθνικό δίκαιο και η ποινική δικονομία[27].

Η αρχή εκτέλεσης της ΕΕΕ, οφείλει να αναγνωρίσει την ΕΕΕ και να την εκτελέσει κατά τον ίδιο τρόπο και διαδικασία, ως εάν επρόκειτο για ερευνητικό μέτρο διαταχθέν από αρχή του κράτους εκτέλεσης, εκτός αν η αρχή αυτή αποφασίζει να επικαλεσθεί ένα εκ των λόγων μη αναγνώρισης ή μη εκτέλεσης ή ένα εκ των λόγων αναβολής[28], που περιγράφονται στο αρ. 11 της Οδηγίας ΕΕΕ[29]. Μάλιστα, η αρχή

---

[26] Αρ. 30 παρ. 4 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[27] Αρ. 1 παρ. 3 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[28] Αρ. 9 παρ. 1 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[29] Αρ. 11 παρ. 1 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1): «*Με την επιφύλαξη του άρθρου 1 παράγραφος 4, η αναγνώριση ή η εκτέλεση μιας ΕΕΕ μπορεί να απορριφθεί από την αρχή εκτέλεσης όταν:*

α) υπάρχει ασυλία ή προνόμιο σύμφωνα με το εθνικό δίκαιο του κράτους εκτέλεσης που εμποδίζει την εκτέλεση της ΕΕΕ ή όταν υπάρχουν κανόνες περί ορισμού και περιορισμού της ποινικής ευθύνης σχετικά με την ελευθερία του Τύπου και την ελευθερία της έκφρασης σε άλλα μέσα ενημέρωσης που εμποδίζει την εκτέλεση της ΕΕΕ·

β) στην συγκεκριμένη περίπτωση η εκτέλεση της ΕΕΕ θα έβλαπτε ουσιώδη συμφέροντα εθνικής ασφάλειας, θα έθετε σε κίνδυνο την πηγή των πληροφοριών ή θα απαιτούσε τη χρήση διαβαθμισμένων πληροφοριών σχετικών με συγκεκριμένες δραστηριότητες συλλογής πληροφοριών·

γ) η ΕΕΕ έχει εκδοθεί στο πλαίσιο διαδικασιών που αναφέρονται στο άρθρο 4 στοιχεία β) και γ) και το ερευνητικό μέτρο δεν θα επιτρεπόταν από το δίκαιο του κράτους εκτέλεσης σε παρόμοια εγχώρια υπόθεση·

δ) η εκτέλεση της ΕΕΕ αντίκειται στην αρχή ne bis in idem·

ε) η ΕΕΕ αφορά ποινικό αδίκημα για το οποίο υπάρχουν υπόνοιες ότι διαπράχθηκε εκτός του εδάφους του κράτους έκδοσης και εν μέρει ή εξ ολοκλήρου στο έδαφος του κράτους εκτέλεσης, και η συμπεριφορά για την οποία εκδόθηκε η ΕΕΕ δεν συνιστά αδίκημα στο κράτος εκτέλεσης·

στ) υπάρχουν σοβαροί λόγοι να θεωρηθεί ότι η εκτέλεση του ερευνητικού μέτρου που αναφέρεται στην ΕΕΕ θα ήταν ασύμβατη με τις υποχρεώσεις του κράτους μέλους εκτέλεσης σύμφωνα με το άρθρο 6 ΣΕΕ και το Χάρτη·

εκτέλεσης τηρεί τις διατυπώσεις και τις διαδικασίες που έχει ορίσει ρητώς η αρχή έκδοσης, εκτός εάν προβλέπεται αλλιώς και υπό την προϋπόθεση ότι οι εν λόγω διατυπώσεις και διαδικασίες δεν είναι αντίθετες προς τις θεμελιώδεις αρχές του δικαίου του κράτους εκτέλεσης[30]. Έτσι υπό την έννοια αυτή η εθνική νομοθεσία του κράτους έκδοσης είναι αυτή που διέπει το μέτρο της ΕΕΕ και είναι αυτή που θα εξασφαλίσει το μεταγενέστερο παραδεκτό αυτού στην ποινική διαδικασία (Tosza, 2019).

Αναφορικά με τις προθεσμίες για την αναγνώριση ή την εκτέλεση μίας ΕΕΕ, ισχύει ότι η έκδοση της απόφασης σχετικά με την αναγνώριση ή την εκτέλεση και η εκτέλεση του ερευνητικού μέτρου πραγματοποιούνται από τις αρμόδιες αρχές του κράτους εκτέλεσης με την ταχύτητα και την προτεραιότητα που θα δινόταν για παρόμοια εγχώρια υπόθεση και, εν πάση περιπτώσει, εντός των οριζόμενων προθεσμιών. Η πρώτη σημαντική προθεσμία είναι αυτή των 30 ημερών μετά την παραλαβή της ΕΕΕ, οπότε και η αρμόδια αρχή εκτέλεσης οφείλει να εκδώσει σχετική απόφαση για την αναγνώριση και την εκτέλεση αυτής[31].

Ωστόσο, εάν δεν συντρέχουν λόγοι αναβολής δυνάμει του άρθρου 15 της Οδηγίας ΕΕΕ ή εάν βρίσκονται ήδη στην κατοχή του κράτους εκτέλεσης αποδεικτικά στοιχεία τα οποία αναφέρονται στο ερευνητικό μέτρο που προβλέπει η ΕΕΕ, η αρχή εκτέλεσης εκτελεί αμελλητί το ερευνητικό μέτρο, με την επιφύλαξη της παραγράφου 5, το αργότερο 90 ημέρες μετά τη λήψη της προηγούμενης απόφασης[32] (αναγνώρισης στη συγκεκριμένη περίπτωση). Επιπρόσθετα, όταν σε συγκεκριμένη περίπτωση δεν

ζ) η συμπεριφορά για την οποία έχει εκδοθεί η ΕΕΕ δεν συνιστά αδίκημα κατά τη νομοθεσία του κράτους εκτέλεσης, εκτός αν αφορά αδίκημα περιλαμβανόμενο στις κατηγορίες αδικημάτων του παραρτήματος Δ, όπως αναφέρεται από την αρχή έκδοσης στην ΕΕΕ, αν τιμωρείται στο κράτος έκδοσης με στερητική της ελευθερίας ποινή ή μέτρο στέρησης της ελευθερίας μέγιστης διάρκειας τουλάχιστον τριών ετών· ή

η) η χρήση του ερευνητικού μέτρου που αναφέρεται στην ΕΕΕ περιορίζεται, βάσει της νομοθεσίας του κράτους εκτέλεσης, σε κατάλογο ή σε κατηγορία αδικημάτων ή σε αδικήματα που τιμωρούνται με κύρωση υπερβαίνουσα ένα συγκεκριμένο κατώτατο όριο, που δεν περιλαμβάνει το αδίκημα το οποίο αφορά η ΕΕΕ.

[30] Αρ. 9 παρ. 2 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[31] Αρ. 12 παρ. 3 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[32] Αρ. 12 παρ. 4 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

είναι πρακτικά εφικτό για την αρμόδια αρχή εκτέλεσης να τηρήσει την προθεσμία των 30 ημερών ή την ημερομηνία που έχει θέσει η αρχή έκδοσης (βλ. αρ. 12 παρ. 2 της Οδηγίας ΕΕΕ), τότε η αρχή εκτέλεσης οφείλει να ενημερώνει αμελλητί την αρμόδια αρχή του κράτους έκδοσης με οποιονδήποτε τρόπο, αναφέροντας τους λόγους της καθυστέρησης και τον χρόνο που εκτιμά ότι θα χρειαστεί για την έκδοση της απόφασης. Σε αυτή την περίπτωση, η προθεσμία των 30 ημερών (βλ. αρ. 12 παρ. 3 της Οδηγίας ΕΕΕ), μπορεί να παραταθεί κατά 30 ημέρες κατ' ανώτατο όριο[33] και συνολικά να αγγίξουν τις 60 ημέρες.

Τέλος, όταν σε συγκεκριμένη περίπτωση δεν είναι πρακτικά εφικτό για την αρμόδια αρχή εκτέλεσης να τηρήσει την προθεσμία που ορίζεται στην παράγραφο 4 του αρ. 12 της Οδηγίας ΕΕΕ, (δηλαδή των 90 ημερών), ενημερώνει αμελλητί την αρμόδια αρχή του κράτους έκδοσης με οποιονδήποτε τρόπο, αναφέροντας τους λόγους της καθυστέρησης, και διαβουλεύεται με την αρχή έκδοσης για τον κατάλληλο χρόνο εκτέλεσης του ερευνητικού μέτρου[34].

Επίσης είναι δυνατό να αναβληθεί η αναγνώριση ή η εκτέλεση μίας ΕΕΕ από το κράτος εκτέλεσης όταν η εκτέλεσή της μπορεί να παραβλάψει μια διεξαγόμενη ποινική έρευνα ή δίωξη, για όσο χρονικό διάστημα κρίνει αναγκαίο το κράτος εκτέλεσης ή τα σχετικά αντικείμενα, έγγραφα ή δεδομένα χρησιμοποιούνται ήδη στο πλαίσιο άλλης διαδικασίας, μέχρις ότου αυτά να μην είναι πλέον απαραίτητα προς τούτο[35]. Στην περίπτωση αυτή το κράτος εκτέλεσης είναι αυτό που αποφασίζει πότε θα εκλείψει ο χρόνος αναβολής ενημερώνοντας το κράτος έκδοσης.

Οι λόγοι μη αναγνώρισης ή μη εκτέλεσης μίας ΕΕΕ από το κράτος εκτέλεσης περιγράφονται στο αρ. 11 της Οδηγίας ΕΕΕ. Αξίζει να σημειωθεί η περίπτωση όπου «*η χρήση του ερευνητικού μέτρου που αναφέρεται στην ΕΕΕ περιορίζεται, βάσει της νομοθεσίας του κράτους εκτέλεσης, σε κατάλογο ή σε κατηγορία αδικημάτων ή σε αδικήματα που τιμωρούνται με κύρωση υπερβαίνουσα ένα συγκεκριμένο κατώτατο*

[33] Αρ. 12 παρ. 5 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[34] Αρ. 12 παρ. 6 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[35] Αρ. 15 παρ. 1 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

όριο, που δεν περιλαμβάνει το αδίκημα το οποίο αφορά η ΕΕΕ.», όπου το κράτος εκτέλεσης μπορεί να αρνηθεί κατά βάση την εκτέλεση της ΕΕΕ, καθώς δεν αποτελεί μέτρο για εγχώρια υπόθεση που επιτάσσει και η Οδηγία της ΕΕΕ[36].

Σημαντικό είναι να αναφερθεί ότι το διττό αξιόποινο της συμπεριφορά για την οποία έχει εκδοθεί η ΕΕΕ αποτελεί έναν από τους λόγους για τον οποίους το κράτος εκτέλεσης μπορεί να αρνηθεί να αναγνωρίσει ή να εκτελέσει μία ΕΕΕ. Έτσι το κράτος εκτέλεσης, αντιλαμβανόμενο ότι έχει λάβει μία ΕΕΕ για ένα ερευνητικό μέτρο που δεν είναι τιμωρητέο με τις προϋποθέσεις αυτές στην δική του έννομη τάξη, τότε μπορεί να αρνηθεί να αναγνωρίσει ή να εκτελέσει την ΕΕΕ που έχει λάβει. Μάλιστα στην περίπτωση αυτή, το κράτος εκτέλεσης δεν χρειάζεται καν να ζητήσει συμπληρωματικές πληροφορίες από το κράτος έκδοσης, όπως απαιτείται στις υπόλοιπες περιπτώσεις εξαιρέσεων[37]. Χρειάζεται να σημειώσουμε ότι το διττό αξιόποινο της συμπεριφοράς για την οποία εκδίδεται και το ερευνητικό μέτρο βάσει της ΕΕΕ, αποτελεί πρωταρχική αρμοδιότητα των δικαστικών αρχών του κράτους έκδοσης, αφού αυτές πληρούν και όλα τα εχέγγυα για τη διασφάλιση της διαδικασίας.

Η αρχή εκτέλεσης μπορεί επίσης να προσφεύγει σε ερευνητικό μέτρο διαφορετικό από αυτό που προβλέπεται στην ΕΕΕ όταν το ερευνητικό μέτρο που επιλέγει η αρχή εκτέλεσης σε δύο περιπτώσεις. Πρώτον, όταν το ερευνητικό αυτό μέτρο θα έχει το ίδιο αποτέλεσμα με το ερευνητικό μέτρο που προβλέπεται στην ΕΕΕ αλλά με λιγότερο παρεμβατικό τρόπο[38]. Ουσιαστικά στην περίπτωση αυτή λαμβάνεται υπόψη η εφαρμογή της αρχής της αναλογικότητας κατά την απόκτηση του αποδεικτικού μέσου, σταθμίζοντας το επιδιωκόμενο αποτέλεσμα (πρόσβαση σε αποδείξεις) και το κάθε φορά λαμβανόμενο μέσο (στην περίπτωση μας το λιγότερο

[36] Ο λόγος αυτός έχει εισαχθεί εξαιρετικά για την παρακολούθηση των επικοινωνιών ενός υπόπτου ή κατηγορουμένου αν το συγκεκριμένο μέτρο δεν θα επιτρεπόταν σε παρόμοια εγχώρια υπόθεση. Σε αυτή τη περίπτωση, το κράτος μέλος εκτέλεσης μπορεί να εξαρτήσει τη συγκατάθεσή του από τυχόν όρους, οι οποίοι θα έπρεπε να τηρούνται σε παρόμοια εγχώρια υπόθεσή του, σύμφωνα με το αρ. 30 παρ. 5 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[37] Αρ. 11 παρ. 4 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1): «*Στις περιπτώσεις που αναφέρονται στην παράγραφο 1 στοιχεία α), β), δ), ε) και στ), προτού αποφασίσει να μην αναγνωρίσει ή να μην εκτελέσει, εν όλω ή εν μέρει, μια ΕΕΕ, η αρχή εκτέλεσης συμβουλεύεται την αρχή έκδοσης με κάθε πρόσφορο μέσο και, εάν χρειάζεται, ζητεί από την αρχή έκδοσης να της παράσχει αμελλητί κάθε απαραίτητη πληροφορία.*»

[38] Αρ. 10 παρ. 4 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

παρεμβατικό μέτρο για την εκτέλεση της ΕΕΕ). Δεύτερον όταν το ερευνητικό μέτρο που αναφέρεται στην ΕΕΕ, δεν υφίσταται στη νομοθεσία του κράτους εκτέλεσης, ή δεν θα ήταν διαθέσιμο σε παρόμοια εγχώρια υπόθεση[39].

Ωστόσο ειδικά για τα ηλεκτρονικά αποδεικτικά στοιχεία, ορίζονται, μεταξύ άλλων, ορισμένα ερευνητικά μέτρα, τα οποία πρέπει πάντοτε να είναι διαθέσιμα στο πλαίσιο του εθνικού δικαίου του κράτους εκτέλεσης, όπως για παράδειγμα η αναγνώριση προσώπων που έχουν συνδρομή σε έναν συγκεκριμένο αριθμό τηλεφώνου ή διεύθυνση IP[40] ή ακόμα και πληροφορίες που περιέχονται σε βάσεις δεδομένων τις οποίες τηρούν αστυνομικές ή δικαστικές αρχές και στις οποίες έχει άμεση πρόσβαση η αρχή εκτέλεσης στο πλαίσιο ποινικής διαδικασίας[41].

Στο σημείο αυτό, χρειάζεται να επισημανθεί ξανά, ότι παρά την γενική αρχή της αμοιβαίας αναγνώρισης των δικαστικών αποφάσεων στον χώρο ελευθερίας ασφάλειας και δικαιοσύνης που έχει δημιουργήσει η Ένωση, η κρίση ότι ένα ερευνητικό μέτρο στο κράτος εκτέλεσης θα ήταν λιγότερο επεμβατικό για το άτομο κατά του οποίου στρέφεται ίσως δημιουργεί την ανάγκη επαλήθευσης της αναγκαιότητας και αναλογικότητας του λαμβανόμενου μέτρου, από τις αρμόδιες αρχές του κράτους εκτέλεσης, ώστε να πετύχουν το βέλτιστο αποτέλεσμα σεβόμενοι την αρχή της αναλογικότητας με το λιγότερο παρεμβατικό τρόπο στα θεμελιώδη ανθρώπινα δικαιώματα (Armada, 2015; Tosza, 2019).

Επειδή η θεσμική αρχή επάνω στην οποία στηρίζεται η ΕΕΕ είναι η αρχή της αμοιβαίας αναγνώρισης των δικαστικών αποφάσεων, δεν υπάρχει κάποιος μηχανισμός εξαναγκασμού του κράτους εκτέλεσης να εκτελέσει το ερευνητικό μέτρο της ΕΕΕ, εφόσον φυσικά πληρούνται όλες οι προϋποθέσεις που αναφέρθηκαν και δεν προκύπτουν εξαιρέσεις ή λόγοι μη εκτέλεσης και αναβολής. Σε περίπτωση ενός νόμιμου αιτήματος που το κράτος εκτέλεσης, αρνείται να το εκτελέσει, ίσως η μόνη διαδικασία κατά αυτού είναι η ενεργοποίηση της διαδικασίας για τη μη εφαρμογή

[39] Αρ. 10 παρ. 1 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[40] Αρ. 10 παρ. 2 εδάφ. ε) της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[41] Αρ. 10 παρ. 2 εδάφ. β) της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

μιας οδηγίας[42], η οποία ίσως να έχει ελάχιστη χρησιμότητα για ένα και μόνο συγκεκριμένο αίτημα.

Επιπλέον, είναι δυνατόν ο κατηγορούμενος ή ο ύποπτος να προσφύγει κατά της ΕΕΕ με ένδικα μέσα. Ειδικότερα, τα κράτη μέλη εξασφαλίζουν ότι για τα ερευνητικά μέτρα που προβλέπονται στην ΕΕΕ είναι διαθέσιμα ένδικα μέσα ισοδύναμα με αυτά που προβλέπονται σε παρόμοια εγχώρια υπόθεση στο κράτος έκδοσης[43]. Οι ουσιαστικοί λόγοι για την έκδοση της ΕΕΕ μπορούν να προσβληθούν μόνο με ένδικο μέσο ενώπιον του κράτους έκδοσης, με την επιφύλαξη των διασφαλίσεων των θεμελιωδών δικαιωμάτων στο κράτος εκτέλεσης[44]. Αναφορικά με τα ένδικα μέσα οι εμπλεκόμενες αρχές ενημερώνονται μεταξύ τους[45] ενώ τυχόν άσκηση ένδικου μέσου, δεν αναστέλλει την εκτέλεση της ΕΕΕ, εκτός και αν προβλέπεται σε παρόμοιες εγχώριες υποθέσεις[46].

Τέλος, χρήζει αναφοράς ότι με την ΕΕΕ είναι δυνατόν να δεσμευθούν αποδεικτικά στοιχεία. Οι εντολές δέσμευσης και δήμευσης περιουσιακών στοιχείων που ίσχυαν με τις διατάξεις της απόφασης-πλαισίου 2003/577/ΔΕΥ έχουν ήδη αντικατασταθεί από την Οδηγία για την ΕΕΕ[47], όσον αφορά τη δέσμευση αποδεικτικών στοιχείων για τα κράτη μέλη που δεσμεύονται από την εν λόγω οδηγία. Οι διατάξεις της απόφασης-πλαισίου 2003/577/ΔΕΥ[48] όσον αφορά τη δέσμευση περιουσιακών στοιχείων αντικαθίστανται από τον Κανονισμό (ΕΕ) 2018/1805 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Νοεμβρίου 2018, σχετικά

[42] Βλ. Αρ. 258 και 259 της ΣΛΕΕ.

[43] Αρ. 14 παρ. 1 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[44] Αρ. 14 παρ. 2 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[45] Αρ. 14 παρ. 5 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[46] Αρ. 14 παρ. 6 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[47] Βλ. Αρ. 34 παρ. 2 της Οδηγίας 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις (ΕΕ L 130 της 1.5.2014, σ. 1).

[48] Απόφαση-πλαίσιο 2003/577/ΔΕΥ του Συμβουλίου, της 22ας Ιουλίου 2003, σχετικά με την εκτέλεση των αποφάσεων δέσμευσης περιουσιακών ή αποδεικτικών στοιχείων στην Ευρωπαϊκή Ένωση (ΕΕ L 196 της 2.8.2003, σ. 45).

με την αμοιβαία αναγνώριση των αποφάσεων δέσμευσης και δήμευσης, μεταξύ των κρατών μελών που δεσμεύονται από αυτόν[49]. Η απόφαση δέσμευσης εκδίδεται ή επικυρώνεται από αρχή έκδοσης για την αποτροπή της καταστροφής, μετατροπής, μετακίνησης, μεταφοράς ή διάθεσης περιουσιακών στοιχείων, με σκοπό τη δήμευσή τους. Με βάση τον Κανονισμό είναι δυνατή η δέσμευση περιουσιακών στοιχείων που συνδέονται με ορισμένα αδικήματα εντός χρονικού ορίου 48 ωρών. Παρόμοια λειτουργία επιτελεί και η Ευρωπαϊκή Εντολή Διατήρησης Ηλεκτρονικών αποδεικτικών στοιχείων (ΕΕΔιατ.), όπως θα παρουσιαστεί και στη συνέχεια.

Κεφάλαιο Τέταρτο

4. Οι εξελίξεις για τα ηλεκτρονικά αποδεικτικά στοιχεία (e-evidence) στον χώρο της Ευρωπαϊκής Ένωσης

Η Ένωση διαθέτει την εξουσία να νομοθετήσει στο πεδίο της προστασίας του κυβερνοεγκλήματος βάσει του αρ. 83 παρ. 1 ΣΛΕΕ καθώς αναφέρεται στους εν λόγω τομείς εγκληματικότητας όπου το Κοινοβούλιο μαζί με το Συμβούλιο μπορούν με τη συνήθη νομοθετική διαδικασία μέσω Οδηγιών, να θεσπίζουν ελάχιστους κανόνες για τον ορισμό ποινικών αδικημάτων και των κυρώσεων στους τομείς της ιδιαιτέρως σοβαρής εγκληματικότητας, η οποία απορρέει κυρίως από τη φύση ή τις επιπτώσεις του αδικήματος της «*εγκληματικότητας στο χώρο της πληροφορικής*» ή λόγω της ειδικής ανάγκης να καταπολεμηθεί σε κοινή βάση με ομοιόμορφο τρόπο από τα κράτη μέλη. Πέραν αυτού σημαντική πτυχή είναι η αμοιβαία αναγνώριση των δικαστικών αποφάσεων και διαταγών των κρατών μελών όπως προβλέπεται από το αρ. 82 παρ. 1 ΣΛΕΕ, για τους ίδιους τομείς εγκληματικότητας και συνεπώς για το κυβερνοέγκλημα. Η αμοιβαία αναγνώριση των δικαστικών αποφάσεων αποτελεί και

[49] Προβλέπεται επίσης ότι η απόφαση-πλαίσιο 2006/783/ΔΕΥ θα πρέπει επίσης να αντικατασταθεί από τον Κανονισμό (ΕΕ) 2018/1805 μεταξύ των κρατών μελών που δεσμεύονται από αυτόν. Οι διατάξεις της απόφασης-πλαισίου 2003/577/ΔΕΥ όσον αφορά τη δέσμευση περιουσιακών στοιχείων καθώς και οι διατάξεις της απόφασης-πλαισίου 2006/783/ΔΕΥ του Συμβουλίου, της 6ης Οκτωβρίου 2006, σχετικά με την εφαρμογή της αρχής της αμοιβαίας αναγνώρισης στις αποφάσεις δήμευσης (ΕΕ L 328 της 24.11.2006, σ. 59), θα πρέπει ως εκ τούτου να συνεχίσουν να εφαρμόζονται όχι μόνο μεταξύ των κρατών μελών που δεν δεσμεύονται από τον Κανονισμό (ΕΕ) 2018/1805 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Νοεμβρίου 2018, σχετικά με την αμοιβαία αναγνώριση των αποφάσεων δέσμευσης και δήμευσης, αλλά και μεταξύ κάθε κράτους μέλους που δεν δεσμεύεται από τον ίδιο κανονισμό και κάθε κράτους μέλους που δεσμεύεται από αυτόν.

τη νομική βάση της σχετικής πρότασης της Επιτροπής για τα ηλεκτρονικά αποδεικτικά στοιχεία (Ευρωπαϊκή Επιτροπή, 2018a), όπως θα παρουσιαστεί και στη συνέχεια.

Ωστόσο η Επιτροπή στην σχετική ΠροτΚανονισμού, επισημαίνει ότι «*παρά τις τακτικές μεταρρυθμίσεις, οι εν λόγω μηχανισμοί συνεργασίας υφίστανται εντεινόμενη πίεση από την αυξανόμενη ανάγκη έγκαιρης διασυνοριακής πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία. Για να ανταποκριθούν στο φαινόμενο αυτό, ορισμένα κράτη μέλη και τρίτες χώρες έχουν καταφύγει στην επέκταση των εθνικών τους εργαλείων. Ο κατακερματισμός που προκύπτει δημιουργεί ανασφάλεια δικαίου και συγκρουόμενες υποχρεώσεις και εγείρει ερωτήματα ως προς την προστασία των θεμελιωδών δικαιωμάτων και των δικονομικών εγγυήσεων για τα πρόσωπα που θίγονται από τα σχετικά αιτήματα*», (Ευρωπαϊκή Επιτροπή, 2018a).

Η πρόταση της Επιτροπής για την υιοθέτηση του Κανονισμού (ΠροτΚανονισμού) για τα ηλεκτρονικά αποδεικτικά στοιχεία, εστιάζεται στο ειδικό πρόβλημα που δημιουργείται από τον ευμετάβλητο χαρακτήρα[50] των ηλεκτρονικών αποδεικτικών στοιχείων και τη διεθνή διάστασή του (Blažič & Klobučar, 2020a). Αυτό που επιδιώκει είναι η προσαρμογή των μηχανισμών συνεργασίας στην ψηφιακή εποχή, δίνοντας στη δικαστική εξουσία και στις αρχές επιβολής του νόμου τα εργαλεία να ανταπεξέλθουν στον τρόπο με τον οποίο επικοινωνούν σήμερα οι εγκληματίες και να καταπολεμήσουν τις σύγχρονες μορφές εγκληματικότητας στο χώρο του διαδικτύου (Mitsilegas, 2018).

Παράλληλα, η Επιτροπή στην σχετική πρότασης της, επισημαίνει ότι, τα εργαλεία αυτά θα πρέπει να υπόκεινται σε ισχυρούς μηχανισμούς προστασίας των θεμελιωδών δικαιωμάτων. Την ίδια στιγμή, με την πρόταση αυτή η Επιτροπή, αποσκοπεί στη βελτίωση της ασφάλειας δικαίου για τις αρχές, τους παρόχους υπηρεσιών και τα θιγόμενα πρόσωπα, και στη συμμόρφωση με υψηλά πρότυπα σε ότι αφορά τα αιτήματα των αρχών επιβολής του νόμου, διασφαλίζοντας με τον τρόπο αυτό, την προστασία των θεμελιωδών δικαιωμάτων, τη διαφάνεια και τη λογοδοσία. Τέλος, αποσκοπεί στην επιτάχυνση της διαδικασίας διατήρησης και συλλογής

[50] Τα ηλεκτρονικά αποδεικτικά στοιχεία, διατηρούνται για περιορισμένο χρονικό διάστημα στους παρόχους, μετά την πάροδο του οποίου διαγράφονται αυτόματα. Το πακέτο προτάσεων της Επιτροπής, περιλαμβάνει και την ΕΕΔιατ. όπου με αυτό τον τρόπο, οι εθνικές αρχές θα είναι σε θέση να ζητούν την διατήρηση αυτών στον πάροχο, προκειμένου να τα αιτηθεί στη συνέχεια, είτε μέσω της ήδη υπάρχουσας ΕΕΕ είτε μέσω της προτεινόμενης ΕΕΥποβ.

ηλεκτρονικών αποδεικτικών στοιχείων που αποθηκεύονται ή/και τηρούνται από παρόχους υπηρεσιών που είναι εγκατεστημένοι σε άλλη έννομη τάξη πέρα από την εθνική σε άλλο κράτος μέλος (Ευρωπαϊκή Επιτροπή, 2018a).

4.1 Το πακέτο προτάσεων για τα ηλεκτρονικά αποδεικτικά στοιχεία

Το πακέτο προτάσεων, για τα ηλεκτρονικά αποδεικτικά στοιχεία (e-evidence proposal) αποτελείται αντιστοίχως από μία πρόταση κανονισμού (ΠροτΚανονισμού) σχετικά με την Ευρωπαϊκή Εντολή Υποβολής[51] (ΕΕΥποβ.) και την Ευρωπαϊκή Εντολή Διατήρησης[52] (ΕΕΔιατ.) ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις (Ευρωπαϊκή Επιτροπή, 2018a), αλλά και μία πρόταση οδηγίας (ΠροτΟδηγίας) σχετικά με την θέσπιση εναρμονισμένων κανόνων για τον ορισμό νομικών εκπροσώπων και αντίστοιχων υπευθύνων παραλαβής και εκτέλεσης (legal representatives) ορισμένων παρόχων υπηρεσιών με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών (Ευρωπαϊκή Επιτροπή, 2018b). Με τις προτάσεις αυτές, η Επιτροπή φιλοδοξεί να ξεπεράσει τις πρακτικές και νομικές δυσχέρειες λόγω της φύσης των ηλεκτρονικών δεδομένων, όπως τις είδαμε, προκειμένου τα κράτη μέλη να αποκτήσουν νομικά εργαλεία που θα τους εξυπηρετούν με ταχύτητα (Τσιλίκης, 2021).

4.1.1 Η νομική βάση

Η νομική βάση της πρότασης του Κανονισμού, είναι το άρθρο 82 παρ. 1 ΣΛΕΕ. Στην περίπτωση αυτή, μπορούν να λαμβάνονται μέτρα με τη συνήθη νομοθετική διαδικασία για τον καθορισμό κανόνων και διαδικασιών για να εξασφαλίζεται η αναγνώριση, σε ολόκληρη την Ένωση, όλων των τύπων δικαστικών αποφάσεων και διαταγών. Μπορούν επίσης να λαμβάνονται μέτρα για τη διευκόλυνση της συνεργασίας μεταξύ των δικαστικών ή άλλων ισοδύναμων αρχών των κρατών μελών κατά την άσκηση ποινικών διώξεων και την εκτέλεση των αποφάσεων (ΣΛΕΕ, 2012). Αυτή η νομική βάση ισχύει για τα προτεινόμενα μέτρα των δύο νέων ευρωπαϊκών εντολών για τη διατήρηση και συλλογή ηλεκτρονικών αποδεικτικών στοιχείων με την πρόταση Κανονισμού της Επιτροπής (ΠροτΚανονισμού).

[51] Στο Αγγλικό κείμενο της ΠροτΚανονισμού αναφέρεται ως *European Production Order*.

[52] Στο Αγγλικό κείμενο της ΠροτΚανονισμού αναφέρεται ως *European Preservation Order*.

Το άρθρο 82 παρ. 1 ΣΛΕΕ, διασφαλίζει την αμοιβαία αναγνώριση των δικαστικών αποφάσεων με τις οποίες μία δικαστική αρχή στο κράτος έκδοσης απευθύνεται σε νομικό πρόσωπο σε άλλο κράτος μέλος, επιβάλλοντάς του μέχρι και υποχρεώσεις, χωρίς την προηγούμενη παρέμβαση δικαστικής αρχής σ' αυτό, δηλαδή στο άλλο κράτος μέλος στο οποίο θα απευθύνεται η ευρωπαϊκή εντολή διατήρησης ή υποβολής ηλεκτρονικών αποδεικτικών στοιχείων. Η ευρωπαϊκή εντολή υποβολής ή διατήρησης στοιχείων, μπορεί να έχει ως αποτέλεσμα την παρέμβαση δικαστικής αρχής του κράτους εκτέλεσης, όταν αυτό είναι απαραίτητο για την εκτέλεση της απόφασης κατά τις περιπτώσεις που προκύπτουν αμφιβολίες ως προς την εκτέλεση από τον πάροχο που είναι εγκατεστημένος σε άλλο κράτος μέλος.

Το άρθρο 82 παρ. 1 ΣΛΕΕ, παρέχει τη δυνατότητα στον νομοθέτη της Ένωσης να εκδίδει Κανονισμούς και Οδηγίες. Η Επιτροπή, στην πρόταση της αναφέρει ότι επειδή το πλαίσιο μέσα στο οποίο εντάσσονται τα ηλεκτρονικά αποδεικτικά στοιχεία, αφορά κυρίως διασυνοριακές διαδικασίες, στις οποίες απαιτούνται ενιαίοι κανόνες, δεν είναι απαραίτητο να δοθεί στα κράτη μέλη το περιθώριο να μεταφέρουν τους εν λόγω κανόνες στο εθνικό τους δίκαιο με Οδηγία και γι' αυτό επιλέγει ως καλύτερη λύση να προτείνει Κανονισμό. Η λογική είναι ότι ο Κανονισμός ισχύει άμεσα, παρέχει σαφήνεια και μεγαλύτερη ασφάλεια δικαίου και επιτρέπει να αποφεύγονται οι αποκλίνουσες ερμηνείες στα κράτη μέλη και άλλα προβλήματα μεταφοράς στο εθνικό τους δίκαιο, τα οποία έχουν δημιουργηθεί κατά το παρελθόν, σε σχέση με τις αποφάσεις-πλαίσια για την αμοιβαία αναγνώριση δικαστικών αποφάσεων και διαταγών. Επιπλέον, ο κανονισμός επιτρέπει την επιβολή της ίδιας υποχρέωσης με ομοιόμορφο τρόπο σε όλα τα κράτη μέλη. Η Επιτροπή τονίζει ότι γι' αυτούς τους λόγους, ο προτεινόμενος κανονισμός για τα ηλεκτρονικά αποδεικτικά στοιχεία, θεωρείται η καταλληλότερη μορφή νομικής πράξης, για αυτήν την περίπτωση αμοιβαίας αναγνώρισης δικαστικών αποφάσεων (Ευρωπαϊκή Επιτροπή, 2018a).

Καταλήγοντας, χρειάζεται να παρατηρηθεί ότι στη περίπτωση αυτή, ο θεσμός της αμοιβαίας αναγνώρισης των δικαστικών αποφάσεων μεταξύ δύο αρχών που συνήθως ήταν δικαστικές, αυτή τη φορά χρησιμοποιείται για την υποβολή αιτημάτων με την επικύρωση της δικαστικής αρχής (από το κράτος έκδοσης) προς έναν ιδιώτη πάροχο που είναι εγκατεστημένος σε ένα άλλο κράτος (εκτέλεσης), χωρίς να παρεμβάλλεται άλλη δικαστική αρχή (Φαρμακίδης, 2021).

4.1.2 Σκοποί που εξυπηρετούνται

Την σήμερον με την ανάπτυξη της τεχνολογίας, διαπιστώνουμε ολοένα και περισσότερο ότι ο μεγαλύτερος όγκος των χρήσιμων πληροφοριών που χρειάζονται για τη διερεύνηση ποινικών αδικημάτων και την άσκηση διώξεων είναι αποθηκευμένος σε υπηρεσίες υπολογιστικού νέφους (cloud), σε κάποιον εξυπηρετητή (server) σε άλλη χώρα ή μπορεί να τηρείται από παρόχους υπηρεσιών που είναι εγκατεστημένοι σε άλλες χώρες (Tosza, 2018).

Η Επιτροπή έχει αντιληφθεί ότι το υφιστάμενο νομικό πλαίσιο συνεργασίας στο πεδίο των ηλεκτρονικών αποδείξεων για την καταπολέμηση του κυβερνοεγκλήματος αλλά και των άλλων απειλών στο διαδίκτυο, πάσχει ενώ χαρακτηρίζεται από κατακερματισμό, απουσία υποχρεωτικότητας από την πλευρά του παρόχου για παροχή αυτών αλλά και διαφορετική νομική δικαιοδοσία ανάλογα με το που τηρούνται αυτά τα ηλεκτρόνια αποδεικτά στοιχεία (Rogalski, 2020).

Στην σχετική πρόταση της, η Επιτροπή επισημαίνει ότι, το υφιστάμενο νομοθετικό πλαίσιο αποτελείται από ενωσιακά εργαλεία συνεργασίας σε ποινικές υποθέσεις, όπως η οδηγία 2014/41/ΕΕ περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις[53], η σύμβαση για την αμοιβαία δικαστική συνδρομή επί ποινικών υποθέσεων μεταξύ των κρατών μελών της Ευρωπαϊκής Ένωσης[54], η απόφαση 2002/187/ΔΕΥ του Συμβουλίου σχετικά με τη σύσταση της Eurojust[55], ο κανονισμός (ΕΕ) 2016/794 για την Europol[56], η απόφαση-πλαίσιο 2002/465/ΔΕΥ του Συμβουλίου σχετικά με τις κοινές ομάδες έρευνας[57], καθώς και διμερείς συμφωνίες

[53] Οδηγία 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 3ης Απριλίου 2014 περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις, (ΕΕ L 130, 1.5.2014, σελ.1).

[54] Πράξη του Συμβουλίου της 29ης Μάϊου 2000 για κατάρτιση, σύμφωνα με το άρθρο 34 της συνθήκης για την Ευρωπαϊκή Ένωση, της σύμβασης για την αμοιβαία δικαστική συνδρομή επί ποινικών υποθέσεων μεταξύ των κρατών μελών της Ευρωπαϊκής Ένωσης.

[55] Απόφαση 2002/187/ΔΕΥ του Συμβουλίου της 28ης Φεβρουαρίου 2002, σχετικά με τη σύσταση της Eurojust προκειμένου να ενισχυθεί η καταπολέμηση των σοβαρών μορφών εγκλήματος.

[56] Κανονισμός (ΕΕ) 2016/794 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαΐου 2016, για τον Οργανισμό της Ευρωπαϊκής Ένωσης για τη Συνεργασία στον Τομέα της Επιβολής του Νόμου (Europol) και την αντικατάσταση και κατάργηση των αποφάσεων του Συμβουλίου 2009/371/ΔΕΥ, 2009/934/ΔΕΥ, 2009/935/ΔΕΥ, 2009/936/ΔΕΥ και 2009/968/ΔΕΥ.

[57] Απόφαση πλαίσιο 2002/465/ΔΕΥ του Συμβουλίου, της 13ης Ιουνίου 2002, σχετικά με τις κοινές ομάδες έρευνας.

μεταξύ της Ένωσης και τρίτων χωρών, όπως η συμφωνία αμοιβαίας δικαστικής συνδρομής μεταξύ ΕΕ και ΗΠΑ[58], είναι κατακερματισμένο.

Βασικός στόχος των προτάσεων αυτών, είναι η ευελιξία και η ταχύτητα των ερευνών των αρμόδιων εθνικών αρχών των κρατών, προκειμένου να διαθέτουν επαρκή νομικά εργαλεία για την γρήγορη άντληση και την διαβίβαση σε αυτούς, ηλεκτρονικών αποδεικτικών στοιχείων. Σε αντίθεση με τα υπάρχοντα μέσα συνεργασίας, όπως η Ευρωπαϊκή Εντολή Έρευνας (ΕΕΕ), που απαιτούν τη συμμετοχή Αρχών τόσο του Κράτους Έκδοσης όσο και του Κράτους Εκτέλεσης, η απευθείας επικοινωνία των Αρχών με τους Παρόχους Υπηρεσιών, χωρίς δηλαδή τη μεσολάβηση των Αρχών του Κράτους Εκτέλεσης, σε συνδυασμό με τις εξαιρετικά σύντομες, σε σχέση με τους ισχύοντες σήμερα θεσμούς δικαστικής συνεργασίας προθεσμίες, αναμένεται ότι θα επιταχύνουν τις έρευνες (Φαρμακίδης, 2021), αλλά και την αποτελεσματική παροχή αισθήματος δικαιοσύνης.

4.1.3 Η Ευρωπαϊκή Εντολή Διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων

Με την εντολή αυτή (ΕΕΔιατ.) σκοπός είναι η αποφυγή της διαγραφής των ηλεκτρονικών αποδεικτικών στοιχείων που βρίσκονται αποθηκευμένα στον πάροχο. Η ΕΕΔιατ. εκδίδεται μόνο για ποινικές διαδικασίες, τόσο κατά το στάδιο της προδικασίας όσο και κατά τη διάρκεια της δίκης. Η ΕΕΔιατ. εκδίδεται επίσης στο πλαίσιο διαδικασίας που σχετίζεται με ποινικό αδίκημα που μπορεί να καταλογιστεί σε νομικό πρόσωπο στο κράτος έκδοσης ή για το οποίο μπορεί να τιμωρηθεί νομικό πρόσωπο στο κράτος αυτό.

Με την παραλαβή της εντολής αυτής, ο πάροχος οφείλει να συμμορφώνεται και να διατηρεί χωρίς να διαγράψει τα απαιτούμενα στοιχεία που τηρεί, προκειμένου στη συνέχεια είτε με την εντολή υποβολής στοιχείων είτε με την έκδοση ευρωπαϊκής εντολής έρευνας να αποκτήσει μία αρχή ορισμένα στοιχεία που αιτείται για μία υπόθεση.

Η εντολή εκδίδεται όταν είναι απαραίτητη και αναλογική ώστε να αποτραπεί η αφαίρεση, η διαγραφή ή η αλλοίωση των δεδομένων ενόψει επακόλουθου

[58] Απόφαση 2009/820/ΚΕΠΠΑ του Συμβουλίου , της 23ης Οκτωβρίου 2009, σχετικά με τη σύναψη, εξ ονόματος της Ευρωπαϊκής Ένωσης, της συμφωνίας σχετικά με την έκδοση μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής και της συμφωνίας σχετικά με την αμοιβαία δικαστική συνδρομή μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής.

αιτήματος υποβολής των εν λόγω δεδομένων μέσω αμοιβαίας δικαστικής συνδρομής, ευρωπαϊκής εντολής έρευνας ή ευρωπαϊκής εντολής υποβολής στοιχείων. Ευρωπαϊκές εντολές διατήρησης στοιχείων με τις οποίες ζητείται η διατήρηση δεδομένων εκδίδονται για οποιοδήποτε ποινικό αδίκημα, χωρίς διάκριση των δεδομένων που ζητούνται να διατηρηθούν[59].

Θα μπορούσαμε να πούμε ότι σε μια ενδεχόμενη περίπτωση ποινικής έρευνας στο εσωτερικό ενός κράτους μέλους όπου όλα τα εμπλεκόμενα μέρη είναι υπήκοοι του ίδιου κράτους μέλους αλλά απαιτούνται ηλεκτρονικά αποδεικτικά στοιχεία που τηρούνται σε πάροχο σε άλλο κράτος μέλος, θα είναι δυνατή η υποβολή μίας τέτοιας εντολής για την διατήρηση αυτών και την μετέπειτα απόκτηση τους, με την επόμενη εντολή που θα δούμε στη συνέχεια.

4.1.4 Η Ευρωπαϊκή Εντολή Υποβολής ηλεκτρονικών αποδεικτικών στοιχείων

Με την εντολή αυτή (ΕΕΥποβ.), εξασφαλίζεται ότι η υποβολή των στοιχείων ανάλογα με τα δεδομένα που ζητούνται κάθε φορά γίνεται κατευθείαν από τον πάροχο στο κράτος έκδοσης χωρίς να μεσολαβεί κάποια άλλη δικαστική αρχή πέραν από αυτή του κράτους έκδοσης της. Με αυτόν τον τρόπο, η αμοιβαία αναγνώριση των δικαστικών αποφάσεων ιδιωτικοποιείται και οι αποφάσεις αυτές απευθύνονται πλέον όχι σε δικαστικές αρχές που έχουν την εξουσία δικαστικού ελέγχου αυτών αλλά απευθείας σε ιδιώτες που ίσως έχουν ελάχιστες νομικές γνώσεις ή περιορισμένα περιθώρια ανταπόκρισης αναφορικά με την προστασία των δικαιωμάτων των υπόπτων (Φαρμακίδης, 2021).

Η ΕΕΥποβ. είναι αναγκαία και αναλογική για τον σκοπό που επιφέρει, δηλαδή την απόκτηση των ηλεκτρονικών αποδεικτικών στοιχείων τηρούμενων ορισμένων προϋποθέσεων καθώς, η ευρωπαϊκή εντολή υποβολής στοιχείων όπως και η ευρωπαϊκή εντολή διατήρησης στοιχείων, εκδίδονται μόνο για ποινικές διαδικασίες, τόσο κατά το στάδιο της προδικασίας όσο και κατά τη διάρκεια της δίκης. Οι εντολές εκδίδονται επίσης στο πλαίσιο διαδικασίας που σχετίζεται με ποινικό αδίκημα που

[59] Η αιτιολογική έκθεση της ΠροτΚανονισμού, για το σημείο αυτό αναφέρει ότι «*Δεδομένου, για παράδειγμα, ότι η ΕΕΕ εν γένει μπορεί να εκδοθεί για οποιοδήποτε αδίκημα χωρίς να περιορίζεται σε συγκεκριμένα όρια, δεν θα περιορίζεται ούτε η ευρωπαϊκή εντολή διατήρησης στοιχείων. Ειδάλλως, το εν λόγω μέσο δεν θα είναι αποτελεσματικό. Για να δίνεται η δυνατότητα στις αρμόδιες για την έρευνα αρχές να ενεργούν γρήγορα και δεδομένου ότι θα επακολουθεί το σχετικό αίτημα υποβολής των δεδομένων, στο πλαίσιο του οποίου θα εξετάζονται και πάλι ενδελεχώς όλες οι προϋποθέσεις, οι ευρωπαϊκές εντολές διατήρησης στοιχείων θα μπορούν επίσης να εκδίδονται ή να εγκρίνονται από εισαγγελέα*» (Commission Staff Working Document, 2018).

μπορεί να καταλογιστεί σε νομικό πρόσωπο στο κράτος έκδοσης ή για το οποίο μπορεί να τιμωρηθεί νομικό πρόσωπο στο κράτος αυτό. Η ΕΕΥποβ. εκδίδεται μόνο αν είναι διαθέσιμο παρόμοιο μέτρο για το ίδιο ποινικό αδίκημα σε συγκρίσιμη εγχώρια κατάσταση στο κράτος έκδοσης.

Έτσι, η έκδοση ΕΕΥποβ. με την οποία ζητείται η υποβολή δεδομένων συνδρομητή ή πρόσβασης εκδίδονται για οποιοδήποτε ποινικό αδίκημα. Επίσης, ΕΕΥποβ. με τις οποίες ζητείται η υποβολή δεδομένων συναλλαγών ή περιεχομένου εκδίδονται μόνο: α) για ποινικά αδικήματα που επισύρουν, στο κράτος έκδοσης, στερητική της ελευθερίας ποινή με ανώτατο όριο τουλάχιστον τριών ετών, ή β) για τα ακόλουθα αδικήματα, αν διαπράχθηκαν εν όλω ή εν μέρει μέσω πληροφοριακού συστήματος:

i. απάτη και πλαστογραφία που αφορούν τα μέσα πληρωμής πλην των μετρητών[60]
ii. σεξουαλική κακοποίηση και σεξουαλική εκμετάλλευση παιδιών και παιδική πορνογραφία[61]
iii. επιθέσεις κατά συστημάτων πληροφοριών[62]
iv. αδικήματα που σχετίζονται με την τρομοκρατία[63]

[60] Τα αδικήματα του άρθρου 3, 4 και 5 της απόφασης-πλαισίου 2001/413/ΔΕΥ του Συμβουλίου.

[61] Τα αδικήματα των άρθρων 3 έως 7 της οδηγίας 2011/93/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

[62] Τα αδικήματα των άρθρων 3 έως 8 της οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

[63] Τα εγκλήματα των άρθρων 3 έως 12 και του άρθρου 14 της οδηγίας (ΕΕ) 2017/541 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Κεφάλαιο Πέμπτο

5. Η Σχέση μεταξύ της Ευρωπαϊκής Εντολής Έρευνας και της Ευρωπαϊκής Εντολής Υποβολής και Διατήρησης Ηλεκτρονικών Αποδεικτικών Στοιχείων

Είναι σημαντικό να αναφερθεί στο σημείο αυτό ότι η ΠροτΚανονισμού αναφέρει ότι δεν θα εμποδίζονται οι αρχές των κρατών μελών να εκδίδουν ευρωπαϊκές εντολές έρευνας σύμφωνα με την οδηγία 2014/41/ΕΕ για τη λήψη ηλεκτρονικών αποδεικτικών στοιχείων[64]. Από την πρόταση αυτή, γίνεται κατανοητό ότι στην Ένωση, με την ΠροτΚανονισμού, θα δημιουργηθούν ακόμη δύο νέα νομικά εργαλεία για την απόκτηση αποδεικτικών στοιχείων, τα οποία θα εξειδικεύονται στα ηλεκτρονικά αποδεικτικά στοιχεία που κατέχουν οι πάροχοι υπηρεσιών διαδικτύου και επικοινωνίας. Εν προκειμένω, γίνεται άμεσα αντιληπτό ότι τα νέα αυτά νομικά εργαλεία σε συνδυασμό με την ΕΕΕ, θα λειτουργούν παράλληλα, ενώ πολλές φορές θα μπορούν να χρησιμοποιούνται και συνδυαστικά όπως θα δούμε και στη συνέχεια. Ακολούθως στα επόμενα σημεία της ανά χείρας διπλωματικής εργασίας, θα συγκρίνουμε τις δύο αυτές εντολές (ΕΕΥποβ. και ΕΕΔιατ.) και τα χαρακτηριστικά τους γνωρίσματα με την ΕΕΕ, όπως την είδαμε προηγουμένως.

5.1 Διάκριση δεδομένων ανάλογα με τη δικαστική προστασία που παρέχεται

Από την προηγούμενη διάκριση που είδαμε προηγουμένως αναφορικά με την ΕΕΥποβ. και την ΕΕΔιατ. ανάλογα με τις προϋποθέσεις που χρειάζεται να ισχύουν προκειμένου να εκδοθούν, παρατηρούμε ότι τα ηλεκτρονικά αποδεικτικά στοιχεία χαρακτηρίζονται σε δύο μεγάλες κατηγορίες, η μία εκ των οποίων χαρακτηρίζεται από αυξημένη δικαστική προστασία, όπως θα εξηγηθεί.

Χρειάζεται να επισημανθεί ότι τα «*δεδομένα συνδρομητή*», τα «*δεδομένα πρόσβασης*» και τα «*δεδομένα συναλλαγών*», συνήθως αναφέρονται από κοινού ως «*δεδομένα που δεν αφορούν το περιεχόμενο*». Τέλος, ως «*δεδομένα περιεχομένου*» ορίζονται οποιαδήποτε δεδομένα αποθηκεύονται σε ψηφιακή μορφή, όπως κείμενο, φωνή, βίντεο, εικόνες και ήχος, άλλα από τα δεδομένα συνδρομητή, πρόσβασης ή συναλλαγών. Έτσι, ως αυξημένης δικαστικής προστασίας (αρ. 4 παρ. 2 και αρ. 5 παρ. 4 της ΠροτΚανονισμού) δεδομένα χαρακτηρίζονται τα δεδομένα συναλλαγών[65] και

[64] Βλ. Αρ. 23 της ΠροτΚανονισμού.

[65] «**δεδομένα συναλλαγών**»: δεδομένα που σχετίζονται με την παροχή μιας υπηρεσίας από πάροχο υπηρεσιών, τα οποία χρησιμεύουν για την παροχή γενικότερου πλαισίου ή πρόσθετων πληροφοριών

περιεχομένου[66] και αυτό γιατί απαιτείται να συντρέχουν ορισμένες προϋποθέσεις τέλεσης αξιόποινων αδικημάτων όπως τα είδαμε προηγουμένως, προκειμένου να αιτηθούν από μία δικαστική αρχή και όχι απλά από μια εθνική αρχή με επικυρωμένη εντολή όπως γίνεται για τις υπόλοιπες δύο κατηγορίες δεδομένων (Tosza, 2019).

Έτσι θα μπορούσε να ειπωθεί ότι στα δεδομένα συναλλαγών και περιεχομένου η παρεμβατικότητα των αρχών μπορεί να είναι μεγαλύτερη (Φαρμακίδης, 2021), αλλά γίνεται υπό τη συνδρομή ειδικότερων προϋποθέσεων[67]. Κατ' αναλογία, οι τελευταίες κατηγορίες χαρακτηρίζονται ως μειωμένης δικαστικής προστασίας (αρ. 4 παρ. 1 και αρ. 5 παρ. 3 της ΠροτΚανονισμού) και αποτελούν τα δεδομένα συνδρομητή[68] αλλά και τα δεδομένα πρόσβασης[69], όπου γι' αυτά η ΕΕΥποβ., θα μπορεί να εκδίδεται για οποιοδήποτε ποινικό αδίκημα.

για την εν λόγω υπηρεσία, και τα οποία παράγονται ή υποβάλλονται σε επεξεργασία από πληροφοριακό σύστημα του παρόχου υπηρεσιών, όπως η πηγή και ο προορισμός μηνύματος ή άλλου είδους αλληλεπίδρασης, δεδομένα σχετικά με την τοποθεσία της συσκευής, η ημερομηνία, η ώρα, η διάρκεια, το μέγεθος, η δρομολόγηση, η μορφή, το χρησιμοποιούμενο πρωτόκολλο και το είδος της συμπίεσης, εκτός αν αυτά τα δεδομένα αποτελούν δεδομένα πρόσβασης.

[66] «**δεδομένα περιεχομένου**»: οποιαδήποτε δεδομένα αποθηκεύονται σε ψηφιακή μορφή, όπως κείμενο, φωνή, βίντεο, εικόνες και ήχος, άλλα από δεδομένα συνδρομητή, πρόσβασης ή συναλλαγών.

[67] Η αιτιολογική έκθεση της ΠροτΚανονισμού στο σημείο αυτό επισημαίνει ότι «*Τα δεδομένα συναλλαγών και περιεχομένου θα πρέπει να υπόκεινται σε αυστηρότερες απαιτήσεις ούτως ώστε να αντικατοπτρίζεται ο πιο ευαίσθητος χαρακτήρας των δεδομένων αυτών και ο αντίστοιχα υψηλότερος βαθμός παρεμβατικότητας των εντολών γι' αυτά τα δεδομένα, σε σύγκριση με τα δεδομένα συνδρομητή και πρόσβασης. Επομένως, οι εντολές μπορούν να εκδοθούν μόνο για αδικήματα που επισύρουν στερητική της ελευθερίας ποινή με ανώτατο όριο τουλάχιστον 3 ετών ή και περισσότερο. Η θέσπιση ορίου με βάση το ανώτατο όριο της στερητικής της ελευθερίας ποινής επιτρέπει μια πιο αναλογική προσέγγιση, μαζί με μια σειρά άλλων εκ των προτέρων και εκ των υστέρων προϋποθέσεων και εγγυήσεων ώστε να διασφαλίζεται ο σεβασμός της αναλογικότητας και των δικαιωμάτων των θιγόμενων προσώπων*» (Commission Staff Working Document, 2018).

[68] «**δεδομένα συνδρομητή**»: οποιαδήποτε δεδομένα αφορούν: α) την ταυτότητα συνδρομητή ή πελάτη, όπως το όνομα, η ημερομηνία γέννησης, η ταχυδρομική ή η γεωγραφική διεύθυνση, δεδομένα τιμολόγησης και πληρωμών, τηλέφωνο ή ηλεκτρονικό ταχυδρομείο, που έχουν παρασχεθεί, β) το είδος της υπηρεσίας και τη διάρκειά της, συμπεριλαμβανομένων των τεχνικών δεδομένων και των δεδομένων που ταυτοποιούν σχετικά τεχνικά μέτρα ή διεπαφές που χρησιμοποιούνται από ή παρέχονται προς τον συνδρομητή ή τον χρήστη, και δεδομένα που σχετίζονται με την επικύρωση της χρήσης της υπηρεσίας, εξαιρουμένων κωδικών πρόσβασης ή άλλων μέσων επαλήθευσης ταυτότητας που χρησιμοποιούνται αντί του κωδικού πρόσβασης και που παρέχονται από τον χρήστη ή δημιουργούνται κατόπιν αιτήματός του.

[69] «**δεδομένα πρόσβασης**»: δεδομένα που σχετίζονται με την έναρξη και τη λήξη της περιόδου πρόσβασης ενός χρήστη σε μια υπηρεσία, τα οποία είναι απολύτως απαραίτητα αποκλειστικά για τον σκοπό της ταυτοποίησης του χρήστη μιας υπηρεσίας, όπως η ημερομηνία και η ώρα χρήσης, ή η σύνδεση και αποσύνδεση από την υπηρεσία, μαζί με τη διεύθυνση IP που έχει χορηγηθεί από τον πάροχο υπηρεσιών πρόσβασης στο διαδίκτυο στον χρήστη της υπηρεσίας, δεδομένα που ταυτοποιούν τη χρησιμοποιούμενη διεπαφή και το αναγνωριστικό χρήστη.

5.2 Σκοπός έκδοσης των εντολών

Όπως είδαμε, η ΕΕΕ εκδίδεται για την απόκτηση οποιοδήποτε είδους αποδεικτικού στοιχείου σε ένα άλλο κράτος μέλος. Η ανάγκη για την δημιουργία της προέρχεται από την ελεύθερη μετακίνηση των πολιτών εντός του ΧΕΑΔ και την απαλοιφή των εσωτερικών συνόρων. Ουσιαστικά αποτελεί το νομικό εργαλείο, το οποίο χρησιμοποιώντας το θεσμό της αμοιβαίας αναγνώρισης των δικαστικών αποφάσεων στο πεδίο της Ένωσης εισχωρεί και στην έννομη τάξη άλλου κράτους μέλους. Από την άλλη πλευρά, η ΕΕΥποβ. και η ΕΕΔιατ., χρησιμοποιούνται αποκλειστικά στο πεδίο της συλλογής ηλεκτρονικών αποδεικτικών από τους παρόχους. Η ανάγκη για την δημιουργία τους προέρχεται από το defacto καθεστώς που δημιουργείται στο πεδίο του διαδικτύου και των επικοινωνιών με τους παρόχους αυτών των υπηρεσιών, να αποτελούν κομβικό σημείο ακόμα και για την λειτουργία θεσμών όπως η δικαιοσύνη και η παροχής ασφάλειας. Επιπλέον θα μπορούσε να ειπωθεί ότι στα νέα δεδομένα, η παροχή των υπηρεσιών μέσω του διαδικτύου είναι αυτές που διακινούνται και προσφέρονται ελευθέρα και όχι οι χρήστες αυτών.

Επιπλέον οι δύο αυτές εντολές (ΕΕΥποβ. και ΕΕΔιατ.), εκδίδονται μόνο στο πλαίσιο ποινικής διαδικασίας τόσο κατά την προδικασία όσο και κατά τη διάρκεια της δίκης[70] και όχι για άλλο σκοπό, όπως μπορεί να συμβαίνει με την ΕΕΕ, όπου μπορεί να εκδίδεται και για διαδικασία που κινείται από διοικητική αρχή για παραβάσεις νομοθεσίας που μπορούν να οδηγήσουν σε δίκη (βλ. αρ. 4 περ. β’ και γ’ της Οδηγίας ΕΕΕ).

Έτσι στην περίπτωση αυτή, αντιλαμβανόμαστε ότι ο σκοπός έκδοσης της ΕΕΕ, περιλαμβάνει περισσότερες περιπτώσεις από ότι οι δύο νέες προτεινόμενες εντολές. Ωστόσο στην περίπτωση που απαιτούνται ηλεκτρονικά αποδεικτικά στοιχεία σε διοικητικές διαδικασίες, τότε αυτά θα είναι δυνατόν να αποκτηθούν μέσω ΕΕΕ και όχι με τη χρήση ΕΕΥποβ..

5.3 Αρμόδιοι για την έκδοση των εντολών

Όπως με την ΕΕΕ όπου με την Οδηγία 2014/41/ΕΕ τα κράτη μέλη είναι αρμόδια να ορίζουν τις αρχές οι οποίες θα εκδίδουν την ΕΕΕ, έτσι και με την

[70] Βλ. Αρ. 3 παρ. της ΠροτΚανονισμού για τα ηλεκτρονικά αποδεικτικά στοιχεία (Πρόταση ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις (No. 2018/0108 (COD)). Στρασβούργο: COM(2018) 225 final.)

ΠροτΚανονισμού αρμόδιες αρχές για την έκδοση ΕΕΥποβ. και ΕΕΔιατ. είναι κατ' αρχήν δικαστικές αρχές[71]. Επιπλέον παρέχεται η δυνατότητα έκδοσης αυτών των εντολών και σε κάθε άλλη αρμόδια αρχή ορισθείσα από το κράτος έκδοσης η οποία, στη συγκεκριμένη υπόθεση, ενεργεί ως ανακριτική αρχή σε ποινική διαδικασία, με αρμοδιότητα να διατάσσει τη συγκέντρωση αποδεικτικών στοιχείων σύμφωνα με το εθνικό δίκαιο[72]. Ωστόσο, στην περίπτωση αυτή που μία αρμόδια αρχή επιβολής του νόμου, αποφασίζει να εκδώσει μία ΕΕΥποβ. ή μία ΕΕΔιατ. απαιτείται προηγουμένως να εξεταστεί η συμμόρφωσή της με τις προϋποθέσεις για την έκδοση της και ακολούθως εγκρίνεται από δικαστή, δικαστήριο, ανακριτή ή εισαγγελέα στο κράτος έκδοσης[73].

Η διαδικασία της επικύρωσης και του ελέγχου των εντολών αυτών, χρειάζεται να είναι ουσιαστική από την πλευρά της αρμόδιας δικαστικής αρχής ελέγχοντας τους λόγους της αναγκαιότητας και την αναλογικότητας για την έκδοση τους και να μην λαμβάνει τον χαρακτήρα μίας τυπικής επικύρωσης, με την τοποθέτηση μίας απλής υπογραφής (Tosza, 2018).

5.4 Αποδέκτες των εντολών

Οι ΕΕΥποβ. και οι ΕΕΔιατ. θα πρέπει να απευθύνονται στον νόμιμο εκπρόσωπο που έχει οριστεί από τον πάροχο υπηρεσιών για τον σκοπό της συλλογής αποδεικτικών στοιχείων σε ποινικές διαδικασίες σύμφωνα με την οδηγία σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον διορισμό νόμιμων εκπροσώπων με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών. Η διαβίβαση αυτή θα έχει τη μορφή πιστοποιητικού σαφώς οριζόμενο ως προς τα πεδία που χρειάζεται να περιλαμβάνει από την ΠροτΚανονισμού[74]. Αυτός ο νόμιμος εκπρόσωπος είναι υπεύθυνος για την παραλαβή τους και την έγκαιρη και πλήρη εκτέλεσή τους. Αυτό αφήνει στους παρόχους υπηρεσιών την επιλογή ως προς τον

[71] Βλ. Αρ. 4 της ΠροτΚανονισμού, δηλαδή από δικαστή, δικαστήριο, ανακριτή ή εισαγγελέα με αρμοδιότητα στη συγκεκριμένη ποινική υπόθεση.

[72] Στην αιτιολογική έκθεση της ΠροτΚανονισμού, επ' αυτού σημειώνεται ότι «*Στην έκδοση ευρωπαϊκής εντολής υποβολής στοιχείων ή ευρωπαϊκής εντολής διατήρησης στοιχείων πρέπει πάντα να συμμετέχει δικαστική αρχή, είτε ως αρχή έκδοσης είτε ως αρχή έγκρισης. Για τις εντολές υποβολής δεδομένων συναλλαγών και περιεχομένου, η δικαστική αρχή μπορεί να είναι δικαστής ή δικαστήριο. Για τα δεδομένα συνδρομητή ή πρόσβασης, η εν λόγω αρχή μπορεί να είναι και εισαγγελέας*.» (Commission Staff Working Document, 2018)

[73] Βλ. Αρ. 4 της ΠροτΚανονισμού.

[74] Βλ. Αρ. 8 της ΠροτΚανονισμού.

τρόπο με τον οποίο θα οργανωθούν για να υποβάλουν τα δεδομένα που έχουν ζητήσει οι αρχές των κρατών μελών[75]. Επιπλέον, παρέχονται και διευκρινίσεις αναφορικά με τον ορισμό μη εκπροσώπου, κατά το μεταβατικό στάδιο μεταφοράς της ΠροτΟδηγίας, με την οποία θεσπίζεται αυτή η υποχρέωση στα κράτη μέλη[76].

Έτσι ενώ είδαμε ότι στην ΕΕΕ, αποδέκτης είναι μία αρχή στο κράτος εκτέλεσης, ενώ στην ΕΕΥποβ. και ΕΕΔιατ. αποδέκτης είναι ένας πάροχος υπηρεσιών που προσφέρει υπηρεσίες διαδικτύου στην Ένωση και ο οποίος έχει εγκαθιδρύσει ένα αντιπρόσωπο σε κάποιο κράτος μέλος και ζητούνται αποδεικτικά στοιχεία που σχετίζονται με τα δεδομένα που είδαμε παραπάνω. Χρειάζεται να σημειωθεί ότι οι εντολές αυτές (ΕΕΥποβ. και ΕΕΔιατ.) είναι διαθέσιμες μόνο αν υπάρχει κάποιος αντιπρόσωπος από τον πάροχο που ζητούνται τα ηλεκτρονικά αποδεικτικά στοιχεία, ειδάλλως, θα απαιτείται η έκδοση ΕΕΕ, προκειμένου να αποκτηθούν τα εν λόγω στοιχεία.

Με την ΠροτΚανονισμού και την ΠροτΟδηγίας, ρυθμίζεται ουσιαστικά το πεδίο των σχέσεων μεταξύ των αρχών και των παρόχων στο πεδίο υποβολής στοιχείων που κατέχουν οι τελευταίοι, και απαιτούνται στην ποινική έρευνα. Εν προκειμένω, οι πάροχοι καθίστανται σημαντικό κομμάτι της ποινικής διαδικασίας στην Ένωση, καθώς με τις προτάσεις αυτές τους επιβάλλονται υποχρεώσεις που

[75] Έτσι για παράδειγμα ο πάροχος Meta ή Facebook είναι σε θέση να παρέχει δικό του δίαυλο επικοινωνίας των αρχών επιβολής του νόμου, σε αντίθεση με άλλους παρόχους όπου απαιτείται υποβολή αυτών των εντολών με πιο συνήθη μέσα ηλεκτρονικής επικοινωνίας (email κλπ). Επιπλέον, στην αιτιολογική έκθεση της ΠροτΚανονισμού, επ' αυτού σημειώνεται ότι «*Ορισμένοι πάροχοι υπηρεσιών έχουν ήδη δημιουργήσει πλατφόρμες για την υποβολή αιτημάτων από τις αρχές επιβολής του νόμου. Η χρήση αυτών των πλατφορμών δεν θα εμποδίζεται από τον κανονισμό, καθώς προσφέρει πολλά πλεονεκτήματα, συμπεριλαμβανομένης της δυνατότητας εύκολου ελέγχου της ταυτότητας των δεδομένων και της ασφαλούς διαβίβασής τους. Ωστόσο, αυτές οι πλατφόρμες πρέπει να επιτρέπουν την υποβολή του πιστοποιητικού ΕΕΥ και του πιστοποιητικού ΕΕΔ στη μορφή που προβλέπεται στα παραρτήματα Ι και ΙΙ, χωρίς να ζητούνται περισσότερα στοιχεία σχετικά με την εντολή. Οι πλατφόρμες που έχουν δημιουργηθεί από κράτη μέλη ή όργανα της Ένωσης μπορεί να προβλέπουν επίσης ασφαλή μέσα διαβίβασης και να διευκολύνουν τον έλεγχο της ταυτότητας των εντολών και τη συλλογή στατιστικών στοιχείων. Θα πρέπει να εξεταστεί μια ενδεχόμενη επέκταση των πλατφορμών eCodex και SIRIUS ώστε να συμπεριλαμβάνουν ασφαλή σύνδεση με τους παρόχους υπηρεσιών για τους σκοπούς της διαβίβασης του πιστοποιητικού ΕΕΥ και του πιστοποιητικού ΕΕΔ και, ανάλογα με την περίπτωση, απαντήσεις από τους παρόχους υπηρεσιών.*», (Commission Staff Working Document, 2018).

[76] Στην αιτιολογική έκθεση της ΠροτΚανονισμού, επ' αυτού σημειώνεται ότι «*Αν δεν έχει οριστεί νόμιμος εκπρόσωπος, οι εντολές μπορούν να απευθύνονται σε οποιαδήποτε εγκατάσταση του παρόχου υπηρεσιών στην Ένωση. Η εν λόγω εφεδρική επιλογή αποσκοπεί στη διασφάλιση της αποτελεσματικότητας του συστήματος σε περίπτωση που ο πάροχος υπηρεσιών δεν έχει (ακόμα) ορίσει ειδικό εκπρόσωπο, για παράδειγμα όταν δεν υπάρχει η υποχρέωση διορισμού νόμιμου εκπροσώπου σύμφωνα με την οδηγία, επειδή οι πάροχοι υπηρεσιών είναι εγκατεστημένοι και δραστηριοποιούνται μόνο σε ένα κράτος μέλος ή σε περιπτώσεις όπου η υποχρέωση διορισμού νόμιμου εκπροσώπου δεν έχει τεθεί ακόμη σε ισχύ, πριν από τη λήξη της προθεσμίας για τη μεταφορά της οδηγίας στο εθνικό δίκαιο.*», (Commission Staff Working Document, 2018).

απαιτείται να συμμορφωθούν με αυτές αναφορικά με τη συνεργασία τους με τις αρχές επιβολής του νόμου και τις άλλες αρμόδιες αρχές των κρατών μελών. Ουσιαστικά η Επιτροπή, υπενθυμίζει στον ιδιωτικό τομέα και τους αντίστοιχους παρόχους ότι η κερδοφορία στο πεδίο της Ένωσης από την παροχή των τεχνολογικών υπηρεσιών τους, συνοδεύεται από υποχρεώσεις απέναντι στα κράτη μέλη στο τομέα αυτό (Tosza, 2020).

Όπως είδαμε, αποδέκτες και των δύο αυτών εντολών(ΕΕΥποβ. και ΕΕΔιατ.), καθίστανται οι ίδιοι οι Πάροχοι Υπηρεσιών και όχι οι δικαστικές αρχές εκτέλεσης στο κράτος εκτέλεσης. Με αυτόν τον τρόπο ο έλεγχος των εντολών αυτών από μία δικαστική αρχή στο κράτος εκτέλεσης, δεν πραγματοποιείται όπως στην ΕΕΕ, αλλά παρακάμπτεται χάριν ταχύτητας και του σκοπού που εξυπηρετεί σύμφωνα με τις προτάσεις της Επιτροπής.

Πέραν αυτού, μία από τις σημαντικές αλλαγές που επιφέρουν οι προτάσεις της Επιτροπής (Κανονισμός και Οδηγία) είναι η κατάργηση των κριτηρίων τοποθεσίας σε ποινικές υποθέσεις μέσω της υποχρέωσης για ορισμό νόμιμου εκπροσώπου για Παρόχους Υπηρεσιών που δεν είναι εγκατεστημένοι σε κράτη μέλη της Ένωσης, αλλά προσφέρουν υπηρεσίες στην Ένωση. Με αυτόν τον τρόπο ενισχύεται η δυνατότητα των εθνικών αρχών να ζητούν τη διατήρηση και την υποβολή δεδομένων από τους Παρόχους, ανεξάρτητα από την ακριβή τοποθεσία αποθήκευσης των εν λόγω δεδομένων(Φαρμακίδης, 2021). Ωστόσο, παρότι η κατάργηση των κριτηρίων τοποθεσίας μπορεί να συνιστά νέο στοιχείο στον τομέα του Ποινικού Δικαίου, δεν πρόκειται για στοιχείο ξένο σε σχέση με την ενωσιακή νομοθεσία, καθώς η κατάργηση των κριτηρίων τοποθεσίας, είχε προηγηθεί ήδη στον τομέα προστασίας των δεδομένων με τον ΓΚΠΔ.

Ωστόσο για χάριν εξυπηρέτησης της ταχύτητας απόκρισης των διωκτικών αρχών, οι δύο νέες αυτές εντολές θα αποτελούν μία «***λεωφόρο***» παροχής στοιχείων ή εναλλακτικά μία γρήγορη οδό, ενώ την ίδια στιγμή η ΕΕΕ, διατηρείται παράλληλα σε ισχύ με τις δύο νέες εντολές υποβολής και διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων, ακόμα και για τα ίδια δεδομένα (αρ. 23 της ΠροτΚανονισμού).

Επομένως στο πλαίσιο που θα δημιουργηθεί με τις προτάσεις αυτές, θα είναι δυνατόν να εκδοθεί στην αρχή μία ΕΕΔιατ., προκειμένου στη συνέχεια να αντληθούν ηλεκτρονικά αποδεικτικά στοιχεία με την χρήση μίας ΕΕΕ (αρ. 6, παρ. 2 της

ΠροτΚανονισμού). Τα κράτη έκδοσης ανάλογα με την περίπτωση θα έχουν το δικαίωμα να υποβάλλουν αντίστοιχο αίτημα. Μπορεί να προτιμήσουν να χρησιμοποιήσουν την ΕΕΕ, όταν ζητούν ένα σύνολο ερευνητικών μέτρων διαφορετικών ειδών, συμπεριλαμβανομένης, ενδεικτικά, της υποβολής ηλεκτρονικών αποδεικτικών στοιχείων από ένα άλλο κράτος μέλος.

Περιπτώσεις κατά τις οποίες τα ζητούμενα δεδομένα αποθηκεύονται ή υποβάλλονται σε επεξεργασία στο πλαίσιο υποδομής που παρέχεται από πάροχο υπηρεσιών σε εταιρεία, κατά κανόνα σε υπηρεσίες φιλοξενίας ή λογισμικού, η ίδια η εταιρεία θα πρέπει να είναι ο βασικός αποδέκτης του αιτήματος από τις αρμόδιες για την έρευνα αρχές. Αυτό ενδέχεται να απαιτεί διαδικασία έκδοσης ΕΕΕ ή αμοιβαίας δικαστικής συνεργασίας σε περίπτωση που η εταιρεία δεν είναι πάροχος υπηρεσιών που υπάγεται στο πεδίο εφαρμογής της ΠροτΚανονισμού.

Στην περίπτωση αυτή, μία ΕΕΥποβ, μπορεί να απευθυνθεί στον πάροχο υπηρεσιών μόνο αν δεν θα ήταν σκόπιμο να απευθυνθεί το αίτημα στην εταιρεία, ιδίως σε περίπτωση που κάτι τέτοιο θα συνεπαγόταν κίνδυνο υπονόμευσης της έρευνας, για παράδειγμα όταν η ίδια η εταιρεία αποτελεί αντικείμενο της έρευνας. Ωστόσο χρειάζεται να σημειωθεί ότι αν υιοθετηθεί η πρόταση του Κανονισμού και της Οδηγίας για την Ευρωπαϊκή Εντολής Υποβολής και Διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων, η Δανία, (ίσως και η Ιρλανδία) δε θα δεσμεύεται από αυτόν και συνεπώς δε θα είναι δυνατή η έκδοση αυτών, αλλά θα οι ίδιοι σκοποί θα εξυπηρετούνται με την διαδικασία της ΕΕΕ.

5.5 Προϋποθέσεις έκδοσης εντολών

Αρχικά θα λέγαμε ότι τα πρώτα δύο κριτήρια που απαιτείται να συντρέχουν για την έκδοση των δύο νέων αυτών προτεινόμενων εντολών, προσομοιάζουν με αυτά της ΕΕΕ. Έτσι στην περίπτωση της ΕΕΥποβ. απαιτείται για την έκδοση της να υπάρχει ένα παρόμοιο διαθέσιμο μέτρο για το ίδιο ποινικό αδίκημα σε συγκρίσιμη εγχώρια κατάσταση στο κράτος έκδοσης στο πλαίσιο ποινικής διαδικασίας[77] και η έκδοση αυτών των εντολών να πληροί τα κριτήρια της αναγκαιότητας και της αναλογικότητας. Πέραν αυτού για την έκδοση ΕΕΥποβ. που αφορά δεδομένα

[77] Αρ. 5 παρ. 2 της ΠροτΚανονισμού: *«Η ευρωπαϊκή εντολή υποβολής στοιχείων είναι αναγκαία και αναλογική για τον σκοπό των διαδικασιών του άρθρου 3 παράγραφος 2 και εκδίδεται μόνο αν είναι διαθέσιμο παρόμοιο μέτρο για το ίδιο ποινικό αδίκημα σε συγκρίσιμη εγχώρια κατάσταση στο κράτος έκδοσης.»*

συναλλαγών και περιεχομένου, απαιτείται να συντρέχουν προϋποθέσεις ποινικής έρευνας συγκεκριμένων αδικημάτων.

Η τρίτη αυτή ειδικότερη προϋπόθεση που απαιτείται να συντρέχει για την έκδοση ΕΕΥποβ. παρουσιάστηκε παραπάνω κάνοντας την διάκριση των δεδομένων που ζητούνται με αυτήν βάση της δικαστικής προστασίας που τους παρέχεται. Έτσι είδαμε τον διαφορετικό βαθμό κριτήριών που απαιτείται για τα δεδομένα περιεχομένου, διότι η απόκτηση αυτών αποτελεί τον μέγιστο βαθμό παρεμβατικότητας στην ιδιωτική ζωή κάποιου από την πλευρά των διωκτικών αρχών και εξ' ου και η αυξημένη προστασία που χρειάζεται να παρέχεται σε αυτά (δεδομένα περιεχομένου). Από την άλλη πλευρά, η έκδοση ΕΕΥποβ. για την υποβολή δεδομένων συνδρομητή και πρόσβασης μπορούν να εκδοθούν για οποιοδήποτε ποινικό αδίκημα.

Αναφορικά με την τρίτη προϋπόθεση που απαιτείται να συντρέχει αναφορικά με τον χαρακτηρισμό ορισμένων αδικημάτων, χρειάζεται να επισημανθεί ότι ο διττός έλεγχος των ΕΕΥποβ. και ΕΕΔιατ. από μία δικαστική αρχή στο κράτος εκτέλεσης, απαλείφεται και δεν διενεργείται, όπως γίνεται στην ΕΕΕ. Εξαιτίας αυτού, ο διττός έλεγχος του αξιόποινου τόσο στο κράτος έκδοσης όσο και στο κράτος εκτέλεσης, παύει να ισχύει για την περίπτωση των ΕΕΥποβ. και ΕΕΔιατ.. Αυτό θα συμβαίνει γιατί πλέον με την διαβίβαση των δύο νέων εντολών το κράτος εκτέλεσης, δεν έχει αρμοδιότητα για τον έλεγχο αυτών παρά μόνο σε ορισμένες περιπτώσεις μη συμμόρφωσης του παρόχου, όπου θα ζητείται η συνδρομή του, για την διασφάλιση της εκτέλεσης των ΕΕΥποβ. και ΕΕΔιατ.. Σε μία τέτοια περίπτωση μία ΕΕΥποβ. είναι σαν να μετατρέπεται στην ουσία σε ΕΕΕ, χωρίς ωστόσο να υπάρχουν οι ίδιοι λόγοι απόρριψης ή άρνησης εκτέλεσης αυτής, όπως θα δούμε.

Επιπλέον, η απαίτηση για την ύπαρξη ίδιου διαθέσιμου μέτρου στην εγχώρια τάξη δεν το θέτει ως προαπαιτούμενο για την έκδοση της ΕΕΔιατ. ωστόσο διατηρείται το κριτήριο της αναγκαιότητας και της αναλογικότητας. Εν προκειμένω, παρατηρείται το παράδοξο να είναι δυνατή η έκδοση ΕΕΔιατ. από ένα κράτος έκδοσης, προκειμένου να διατηρηθούν ηλεκτρονικά αποδεικτικά, ακόμα και αν δεν παρέχεται τέτοια δυνατότητα από την εθνική νομοθεσία του κράτους έκδοσης για τις εγχώριες υποθέσεις του άλλα ίσως μία τέτοια πρόβλεψη απαιτείται να ρυθμιστεί εκ

των υστέρων, με βάση την αρχή της καλόπιστης συνεργασίας[78]. Ωστόσο δεν θα πρέπει, να αθετούμε τον κύριο σκοπό με τον οποίο εισάγεται αυτή η νέα εντολή στην ευρωπαϊκή ποινική δικαιοταξία, δηλαδή την αποτροπή της αφαίρεσης, η διαγραφής ή της αλλοίωσης των ηλεκτρονικών δεδομένων που τηρούνται σε έναν πάροχο, (λόγω του ευμετάβλητου που τα χαρακτηρίζει όπως είδαμε) ενόψει επακόλουθου αιτήματος υποβολής των εν λόγω δεδομένων μέσω αμοιβαίας δικαστικής συνδρομής, ΕΕΕ ή ΕΕΥποβ.[79].

Από την άλλη πλευρά, βλέπουμε ότι ΕΕΔιατ. μπορεί να υποβληθεί για οποιοδήποτε αδίκημα. Αυτό σημαίνει ότι ακόμα για ένα αδίκημα όπως η εξύβριση, οι αρμόδιες αρχές έχουν το δικαίωμα να υποβάλλουν αντίστοιχο αίτημα προς τον πάροχο για την διατήρηση ηλεκτρονικών αποδεικτικών στοιχείων που πιθανόν να σχετίζονται με μία συσκευή, ένα όνομα χρήστη (username) ένα email, μία ηλεκτρονική διεύθυνση IPή έναν αριθμό τηλεφώνου. Στην περίπτωση αυτή, όπου ακόμα μία υπόθεση βρίσκεται στο στάδιο της προδικασίας, ίσως θεωρείται ιδιαίτερα επεμβατικό στην προστασία των δικαιωμάτων ενός ατόμου, η υποβολή μίας τέτοιας εντολής, ωστόσο δε θα πρέπει να ξεχνάμε ότι σκοπός αυτής, είναι να ειδοποιηθεί ο πάροχος, να διατηρήσει τα ηλεκτρονικά στοιχεία που τηρεί και να μην τα διαγράψει και όχι να τα διαθέσει στις αρμόδιες αρχές του κράτους έκδοσης. Έτσι θα λέγαμε ότι ακόμα και να εκδοθεί μία ΕΕΔιατ. μπορεί σε μετέπειτα στάδιο της ποινικής διαδικασίας να μην ζητηθούν τα ηλεκτρονικά στοιχεία που ζητήθηκαν να διατηρηθούν από τον πάροχο.

Άλλωστε με την έκδοση της ΕΕΔιατ., από πλευράς προσβολής της ιδιωτικότητας του ατόμου, δεν υπάρχει τέτοια στο βαθμό κατά τον οποίο, τα δεδομένα απλώς δεσμεύονται στην διαθεσιμότητα του παρόχου, προκειμένου ο τελευταίος να είναι έτοιμος να τα διαβιβάσει, οποτεδήποτε χρειαστεί στην αρμόδια αρχή, όταν του ζητηθεί με τον νομότυπο τρόπο (υποβολή ΕΕΕ, αιτήματος αμοιβαίας δικαστικής συνδρομής ή ΕΕΥποβ.). Η ΕΕΔιατ. λειτουργεί εξασφαλιστικά ως τις αρμόδιες αρχές επιβολής του νόμου, προκειμένου να μπορούν να αξιοποιήσουν κατά

[78] Βλ. ΔΕΕ, υπόθεση C-852/19, Απόφαση της 11ης Νοεμβρίου 2021 (υπόθεση Gavanozov), Πηγή: ECLI:EU:C:2021:902, σύμφωνα με την σκέψη 57, ότι «*Εξάλλου, πρέπει να υπομνησθεί ότι εναπόκειται στα κράτη μέλη, βάσει ιδίως της αρχής της καλόπιστης συνεργασίας κατά το άρθρο 4, παράγραφος 3, πρώτο εδάφιο, ΣΕΕ, να διασφαλίζουν, το καθένα στο έδαφός του, την εφαρμογή και την τήρηση του δικαίου της Ένωσης και να λαμβάνουν, προς τον σκοπό αυτό, κάθε γενικό ή ειδικό μέτρο που δύναται να διασφαλίσει την εκπλήρωση των υποχρεώσεων που απορρέουν από τις Συνθήκες ή από τις πράξεις των θεσμικών οργάνων της Ένωσης (πρβλ. απόφαση της 6ης Μαρτίου 2018, Achmea, C-284/16, EU:C:2018:158, σκέψη 34 και εκεί μνημονευόμενη νομολογία).*»

[79] Βλ. Αρ. 6 παρ. 2 της ΠροτΚανονισμού.

την πορεία έρευνας μίας ποινικής υπόθεσης, τυχόν ηλεκτρονικά αποδεικτικά στοιχεία, μη επηρεαζόμενη από τον ευμετάβλητο χαρακτήρα τους (Eurojust, 2020).

5.6 Έκδοση εντολής με πρωτοβουλία του κατηγορουμένου ή του υπόπτου

Σημαντικό είναι να σημειωθεί σε αντίθεση με την έκδοση ΕΕΕ που μπορεί να ζητήσει κάποιος ύποπτος ή κατηγορούμενος (ή δικηγόρος εξ ονόματός του) να εκδοθεί στο πλαίσιο των δικαιωμάτων υπεράσπισης που προβλέπει το εθνικό δίκαιο και η ποινική δικονομία, στις περιπτώσεις της ΕΕΥποβ. και της ΕΕΔιατ. αποδεικτικών στοιχείων δεν παρατηρούμε αντίστοιχη πρόβλεψη. Ίσως απαιτείται αντίστοιχη πρόβλεψη να υιοθετηθεί και στην σχετική πρόταση της Επιτροπής, προκειμένου τα δικαιώματα κατηγορουμένων και υπόπτων να διασφαλίζονται καλύτερα, καθώς όπως παρατηρείται στο πεδίο της συλλογής στοιχείων για την ενίσχυση της κατηγορίας, συντελείται σημαντική πρόοδος με αυτές τις δύο εντολές (ΕΕΥποβ. και ΕΕΔιατ.). Ωστόσο απαιτείται να έχουμε υπόψιν και την έκδοση αυτών των εντολών για υπερασπιστικούς λόγους επίσης, προς υποβοήθηση της αθώωσης αυτών των προσώπων, αν οι περιστάσεις και οι συνθήκες το απαιτούν. Στην περίπτωση αυτή, παρόλο που δεν προβλέπεται θα είναι δυνατόν, ο κατηγορούμενος σε μία ποινική διαδικασία να ζητήσει από τον εισαγγελέα ή το δικαστήριο ή τον ανακριτή την έκδοση τέτοιας εντολής (ΕΕΥποβ. και ΕΕΔιατ.), αν πρόκειται με αυτόν τον τρόπο να προσκομιστούν στοιχεία στην διαδικασία που θα δύναται να ενισχύσουν την υπερασπιστική του γραμμή.

5.7 Ένδικα μέσα κατά αυτών των εντολών

Κατ' αρχήν το δικαίωμα αποτελεσματικής προσφυγής κατά οποιουδήποτε ποινικού μέτρου, κατοχυρώνεται στο άρθρο 47 του ΧΘΔΕΕ. Είδαμε ότι κατά της ΕΕΕ, μπορούν να προβληθούν ένδικα μέσα αντίστοιχα με αυτά που προβλέπονται για το ίδιο ερευνητικό μέτρο και στο κράτος έκδοσης[80] και με βάση επίσης ορισμένους ουσιαστικούς λόγους [81]. Επομένως, οι ουσιαστικοί λόγοι για την έκδοση μίας ΕΕΕ, μπορούν να προσβληθούν μόνο με ένδικο μέσο ασκούμενο εντός του κράτους μέλους εκδόσεως. Έτσι στην υπόθεση C-852/19 με την απόφαση της 11ης Νοεμβρίου 2021 το ΔΕΕ (υπόθεση Gavanozov II), έκρινε ότι, «*εναπόκειται στο κράτος μέλος εκδόσεως να μεριμνά ώστε κάθε πρόσωπο στο οποίο επιβλήθηκε υποχρέωση να παρουσιαστεί να*

[80] Βλ. Αρ. 14 της Οδηγίας ΕΕΕ.

[81] Βλ. Αρ. 11 της Οδηγίας ΕΕΕ

καταθέσει ως μάρτυρας ή να απαντήσει στις ερωτήσεις που θα του τεθούν κατά τη διάρκεια μιας τέτοιας εξέτασης στο πλαίσιο εκτελέσεως ευρωπαϊκής εντολής έρευνας να διαθέτει δικαίωμα προσφυγής ενώπιον δικαστηρίου του κράτους μέλους αυτού που να του παρέχει τη δυνατότητα να αμφισβητήσει, τουλάχιστον, τους ουσιαστικούς λόγους στους οποίους στηρίζεται η έκδοση της ευρωπαϊκής εντολής έρευνας[82].».

Αντίθετα, η ΠροτΚανονισμού, δεν αναφέρει συγκεκριμένους λόγους προσφυγής ή απόρριψης των εντολών ΕΕΥποβ. ή ΕΕΔιατ.. Σε αντίθεση με ότι προβλέπεται για τους παρόχους υπηρεσιών όπως είδαμε, η ΠροτΚανονισμού, δεν περιορίζει τους πιθανούς λόγους με βάση τους οποίους όλα αυτά τα πρόσωπα μπορούν να αμφισβητήσουν τη νομιμότητα της εντολής. Οι λόγοι αυτοί περιλαμβάνουν την αναγκαιότητα και την αναλογικότητα της εντολής (Commission Staff Working Document, 2018). Επιπλέον, το πλήρες σκεπτικό με τους λόγους της αναγκαιότητας και της αναλογικότητας ή περισσότερες λεπτομέρειες για την υπόθεση δεν θα πρέπει να περιλαμβάνονται στο πιστοποιητικό ΕΕΥποβ., ώστε να αποτρέπεται ο κίνδυνος υπονόμευσης της έρευνας. Ως εκ τούτου, είναι απαραίτητο μόνο ως μέρος της ίδιας της εντολής, ώστε να επιτραπεί αργότερα στον ύποπτο ή τον κατηγορούμενο, να την αμφισβητήσει κατά τη διάρκεια της ποινικής διαδικασίας στο κράτος έκδοσης αυτής (Commission Staff Working Document, 2018).

Η δυνατότητα υποβολής ένδικων μέσων παρέχεται σύμφωνα με την διαδικασία του κράτους έκδοσης. Ωστόσο, για να ασκηθούν αυτά από το ενδιαφερόμενο πρόσωπο απαιτείται προηγουμένως να έχει ενημερωθεί επαρκώς ότι κινείται σε βάρος του ορισμένη διαδικασία. Όπως θα δούμε και εν συνεχεία, η ενημέρωση του υποκείμενου προσώπου, τα δεδομένα του οποίου ζητούνται, καθίσταται προβληματική επίσης, αφού εναπόκειται τις περισσότερες φορές στο κράτος έκδοσης, η δυνατότητα να ασκήσει αυτήν την ενημέρωση, παρέχοντας και τα μέσα έννομης προστασίας στο κράτος έκδοσης της ΕΕΥποβ..

Από την άλλη πλευρά, η υποβολή ένδικων μέσων κατά της ΕΕΔιατ. δεν προβλέπεται καθώς όπως αναφέραμε είναι πρόδρομο εργαλείο που μπορεί να προηγείται της ΕΕΥποβ., οπότε ένδικο μέσο ασκείται τελικά κατά της εντολής με την οποία διαβιβάζονται τα εν λόγω στοιχεία (ΕΕΥποβ.) και όχι κατά της εντολής με την

[82] ΔΕΕ, υπόθεση C-852/19, Απόφαση της 11ης Νοεμβρίου 2021 (υπόθεση Gavanozov), Πηγή: ECLI:EU:C:2021:902

οποία τα στοιχεία δεσμεύονται στον πάροχο (ΕΕΔιατ.) και μπορεί να μην αποκτηθούν πότε από την αρχή έκδοσης.

Το υποκείμενο των δεδομένων που ζητούνται με την ΕΕΥποβ. διατηρεί το δικαίωμα χρήσης μέσου αποτελεσματικής έννομης προστασίας ασκείται ενώπιον δικαστηρίου στο κράτος έκδοσης σύμφωνα με το εθνικό του δίκαιο και συμπεριλαμβάνει τη δυνατότητα αμφισβήτησης της νομιμότητας του μέτρου, καθώς και της αναγκαιότητας και της αναλογικότητάς του[83].

Επιπλέον, είναι καινοφανές ότι στην ΠροτΚανονισμού, προτείνεται διάκριση των προσώπων που έχουν δικαίωμα υποβολής ένδικων μέσων κατά της ΕΕΥποβ. σε κατηγορούμενους και ύποπτούς για τους οποίους ζητήθηκαν δεδομένα και σε πρόσωπα των οποίων τα δεδομένα συλλέχθηκαν και δεν είναι ύποπτοι ή κατηγορούμενοι στην ποινική διαδικασία για την οποία εκδόθηκε η ΕΕΥποβ.[84] Πάντως και στις δύο αυτές κατηγορίες προσώπων παρέχεται η ίδια προστασία[85] υποβολής ένδικων μέσων στο κράτος έκδοσης της ΕΕΥποβ.. Τέλος, όπως και στην περίπτωση εντολών που εκτελούνται μέσω άλλων μορφών δικαστικής συνεργασίας, τα δικαστήρια του κράτους έκδοσης είναι τα πλέον αρμόδια για να ελέγχουν τη νομιμότητα των ΕΕΥποβ. τις οποίες εκδίδουν οι αρχές του εν λόγω κράτους και να αξιολογούν τη συμβατότητά τους με το οικείο εθνικό δίκαιο (Commission Staff Working Document, 2018). Επιπλέον, κατά το στάδιο της εκτέλεσης, οι αποδέκτες μπορούν να αντιταχθούν μεμονωμένα στην εκτέλεση ΕΕΥποβ. και ΕΕΔιατ. στο κράτος μέλος που εκδίδει αυτές και το δικαστήριο του οποίου είναι αρμόδιο για την παροχή δικαστικής προστασίας (Commission Staff Working Document, 2018).

5.8 Λόγοι απόρριψης, αναβολής ή άρνησης εκτέλεσης αυτών των εντολών

Οι λόγοι για τους οποίους δεν εκτελείται μία ΕΕΕ, είναι σαφείς και συγκεκριμένοι στην Οδηγία που την μεταφέρει στο εθνικό δίκαιο των κρατών μελών και αναφέρονται στο αρ. 11 της Οδηγίας και περιλαμβάνουν αρκετές εξασφαλιστικές δικλείδες όπως η αρχή ne bis in idem, ο έλεγχος του διττού αξιόποινου και στα δύο κράτη, δηλ. έκδοσης και εκτέλεσης της ΕΕΕ, σε ορισμένες περιπτώσεις καθώς και

[83] Βλ. Αρ. 17 παρ. 3 της ΠροτΚανονισμού.

[84] Όλα αυτά τα δικαιώματα έννομης προστασίας στο κράτος έκδοσης, ισχύουν υπό την επιφύλαξη των διαθέσιμων μέσων έννομης προστασίας που προβλέπονται στην Οδηγία για την προστασία των δεδομένων προσωπικού χαρακτήρα από τις αρχές επιβολής του νόμου και τον ΓΚΠΔ.

[85] Βλ. Αρ. 17 παρ1 και 2 της ΠροτΚανονισμού, δηλαδή δικαίωμα χρήσης μέσων αποτελεσματικής έννομης προστασίας κατά της ευρωπαϊκής εντολής υποβολής στοιχείων στο κράτος έκδοσης, με την επιφύλαξη των μέσων έννομης προστασίας που είναι διαθέσιμα σύμφωνα με την οδηγία (ΕΕ) 2016/680 και τον κανονισμό (ΕΕ) 2016/679.

σοβαροί λόγοι ότι ένα πιθανό ερευνητικό μέτρο είναι ασύμβατο με τον ΧΘΔΕΕ και τις υποχρεώσεις του κράτους μέλους προς αυτόν. Από την άλλη πλευρά, οι λόγοι για τους οποίους μπορεί να εναντιωθεί κάποιος κατά μίας ΕΕΥποβ. και ΕΕΔιατ. είναι μόνο ορισμένοι λόγοι αναφορικά με την αναγκαιότητα και την αναλογικότητα του μέτρου και όχι καν η ύπαρξη του διττού αξιόποινου.

Επιπλέον είναι χαρακτηριστικό ότι στις δύο νέες αυτές εντολές (ΕΕΥποβ. και ΕΕΔιατ.) οι λόγοι αναβολής ή άρνησης ή αδυναμίας εκτέλεσης περιορίζονται να αναφερθούν από τον πάροχο (παραδείγματος χάριν, λάθη των εντολών ή παραλείψεις, τα δεδομένα πλέον δεν βρίσκονται στην κατοχή του παρόχου, το υποκείμενο των δεδομένων δεν είναι πελάτης του παρόχου κλπ.), αφού αυτός είναι που τις εκτελεί και μπορεί ακόμα να έχουν σχέση με παραβιάσεις δικαίου τρίτου κράτους τις περισσότερες φορές, όπου με την υποβολή τυχόν ηλεκτρονικών αποδεικτικών στοιχείων, θα μπορούσε να έχει ως αποτέλεσμα την παραβίαση της νομοθεσίας τρίτης χώρας η οποία απαγορεύει τη γνωστοποίηση των δεδομένων, για το λόγο ότι αυτό είναι απαραίτητο είτε για την προστασία των θεμελιωδών δικαιωμάτων των εμπλεκόμενων προσώπων ή των θεμελιωδών συμφερόντων της τρίτης χώρας, τα οποία συνδέονται με την εθνική ασφάλεια ή άμυνα.

Επιπλέον, διαπιστώνουμε ότι με βάση τις ασφαλιστικές δικλείδες που προσφέρονται ανάλογα με τα εργαλεία που θα χρησιμοποιήσουν οι αρμόδιες αρχές ενός κράτους μέλους για την απόκτηση αποδεικτικών στοιχείων, η ΕΕΥποβ. και ΕΕΔιατ. μπορεί να φαίνεται πιο επιβλαβής για την ιδιωτικότητα ενός ατόμου αναφορικά με την διαδικασία έκδοσης αυτών και τις εγγυήσεις που παρέχονται παρά για την απόκτηση εγγράφων που τηρούνται στο φυσικό αρχείο μίας εταιρείας ενός κράτους μέλους με την διαδικασία που ισχύει για την ΕΕΕ και την παρεμβολή της ασφαλιστικής δικλείδας του κράτους εκτέλεσης. Έτσι, γίνεται αντιληπτό ότι λιγότερο παρεμβατικά μέτρα στην ιδιωτικότητα του ατόμου (απόκτηση εγγράφων μέσω της ΕΕΕ σε σύγκριση με την απόκτηση στοιχείων ενός προσωπικού email), είναι αντικείμενα υψηλότερης προστασίας από άποψη προστασίας θεμελιωδών δικαιωμάτων και ασφαλιστικών δικλείδων σε επίπεδο διαδικαστικών κανόνων (ποινική δικονομία) που εφαρμόζονται στην ποινική δικαιοσύνη ανάμεσα στα κράτη μέλη.

5.9 Διαβίβαση αποδεικτικών στοιχείων με τις εντολές

Όπως συμβαίνει με την ΕΕΕ, όπου ζητούμενο είναι η απόκτηση και η διαβίβαση στοιχείων από το κράτος εκτέλεσης με την παρεμβολή του τελευταίου, έτσι και με τις εντολές αυτές (ΕΕΥποβ. και ΕΕΔιατ.), ζητούνται στοιχεία από τον πάροχο που βρίσκεται εγκατεστημένος στην περιφέρεια κράτους μέλους ή προσφέρει τις υπηρεσίες του σ' αυτό, χωρίς την σύμπραξη του κράτους εκτέλεσης. Το μόνο χαρακτηριστικό που διαφέρει με την ΕΕΥποβ. είναι ότι οι πάροχοι, είναι δυνατόν ακόμα και να διαβιβάζουν τα αιτούμενα στοιχεία απευθείας στην αρμόδια αρχή έκδοσης[86], χωρίς την παρεμβολή άλλης αρχής στο κράτος εκτέλεσης, όπως συμβαίνει με την ΕΕΕ.

Στο ιδανικό σενάριο που συμβαίνει τις περισσότερες φορές είναι οι εντολές αυτές να εκτελούνται. Ωστόσο μπορεί να συμβούν και περιπτώσεις μη εκτέλεσης αυτών. Στην περίπτωση της ΕΕΕ, όταν συντρέχει κάποιος λόγος από αυτούς που αναφέρονται στην επίμαχη Οδηγία για την ΕΕΕ, τότε το κράτος έκδοσης μπορεί ακόμα και να ανακαλέσει την ΕΕΕ, καθώς όπως είδαμε ο θεσμός επάνω στον οποίο βασίζεται είναι η αμοιβαία αναγνώριση των δικαστικών αποφάσεων.

Πάντως είναι δυνατό αν ο αποδέκτης πάροχος δεν μπορεί να συμμορφωθεί με την υποχρέωσή του για λόγους ανωτέρας βίας ή πραγματικής αδυναμίας που δεν οφείλονται σε υπαιτιότητα του ιδίου ή, αν πρόκειται περί διαφορετικών προσώπων, σε υπαιτιότητα του παρόχου υπηρεσιών, ιδίως επειδή το πρόσωπο του οποίου ζητούνται τα δεδομένα δεν είναι πελάτης τους ή τα δεδομένα διαγράφηκαν πριν από τη λήψη της ΕΕΥποβ. ή ΕΕΔιατ., τότε ο πάροχος ενημερώνει χωρίς αδικαιολόγητη καθυστέρηση την αρχή έκδοσης και εξηγεί τους λόγους. Πάντως είναι δυνατόν, αν πληρούνται οι σχετικές προϋποθέσεις που αναφέρθηκαν προηγουμένως, η αρχή έκδοσης να ανακαλεί την ΕΕΥποβ. ή την ΕΕΔιατ.

Αναφορικά με την ΠροτΚανονισμού, προβλέπεται ξεχωριστή διαδικασία για την εκτέλεση των εντολών σε περίπτωση μη συμμόρφωσης, με τη συνδρομή του κράτους μέλους στο οποίο βρίσκεται ο αποδέκτης της εντολής (ΕΕΥποβ. και ΕΕΔιατ). Έτσι, ανάλογα με το ποιος είναι ο αρχικός αποδέκτης της εν διαβιβαζόμενης εντολής, το εν λόγω κράτος μέλος μπορεί να είναι είτε το κράτος μέλος του παρόχου υπηρεσιών είτε το κράτος μέλος του νόμιμου εκπροσώπου του

[86] Χαρακτηριστικά στην περίπτωση της Ελλάδας, μπορεί να είναι η Διεύθυνση Πρόληψης και Δίωξης Ηλεκτρονικού Εγκλήματος του Αρχηγείου της Ελληνικής Αστυνομίας.

παρόχου. Στην περίπτωση αυτή μη συμμόρφωσης του παρόχου, η αρχή έκδοσης θα διαβιβάζει στην αρμόδια αρχή του κράτους εκτέλεσης την πλήρη ΕΕΥποβ. ή ΕΕΔιατ., συμπεριλαμβανομένου του σκεπτικού ως προς την αναγκαιότητα και την αναλογικότητα τους και η εν λόγω αρμόδια αρχή στο κράτος εκτέλεσης των εντολών, θα τα εκτελεί σύμφωνα με το εθνικό της δίκαιο καταφεύγοντας, αν χρειαστεί, στις επ' απειλούμενες κυρώσεις κατά των παρόχων με την ΠροτΚανονισμού.

Αν η εντολή διαβιβάζεται προς εκτέλεση στο κράτος εκτέλεσης, η αρχή εκτέλεσης μπορεί να αποφασίσει να μην αναγνωρίσει και να μην εκτελέσει την εντολή αν, κατά την παραλαβή της, θεωρεί ότι συντρέχει οποιοσδήποτε από τους περιορισμένους λόγους ένστασης, και κατόπιν διαβούλευσης με την αρχή έκδοσης. Ειδάλλως, αναφέρεται ότι η ΕΕΥποβ. ή ΕΕΔιατ. αναγνωρίζεται από το κράτος εκτέλεσης, χωρίς καθυστέρηση, αποδεικνύοντας εν τοις πράγμασι ακόμα μία φορά το θεμέλιο αυτής της συνεργασίας, που δεν είναι άλλο από την αρχή της αμοιβαίας αναγνώρισης.

Επιπλέον, αν κινηθεί η διαδικασία εκτέλεσης, ο ίδιος ο αποδέκτης θα πρέπει να είναι σε θέση να ανακόψει την εντολή ενώπιον της αρχής εκτέλεσης. Το άρθρο 14 της ΠροτΚανονισμού, παρέχει ορισμένους λόγους για τους οποίους ο αποδέκτης ή το κράτος εκτέλεσης είναι δυνατόν να αντιταχθούν στην εκτέλεση μίας ΕΕΥποβ.[87] ή ΕΕΔιατ.[88]. Ο αποδέκτης θα μπορεί να προβεί στην εν λόγω ενέργεια βάσει οποιουδήποτε εξ αυτών των λόγων, με την εξαίρεση ασυλιών και προνομίων,

---

[87] Βλ. Αρ. 14 παρ. 4 της ΠροτΚανονισμού, σύμφωνα με την οποία: "*Ο αποδέκτης μπορεί να αντιταχθεί στην εκτέλεση της ΕΕΥποβ. μόνο για τους ακόλουθους λόγους:*
α) η ευρωπαϊκή εντολή υποβολής στοιχείων δεν έχει εκδοθεί ή εγκριθεί από την αρμόδια αρχή έκδοσης του άρθρου 4 της ΠροτΚανονισμού.
β) η ευρωπαϊκή εντολή υποβολής στοιχείων δεν έχει εκδοθεί για αδίκημα του άρθρου 5 παράγραφος 4 της ΠροτΚανονισμού.
γ) ο αποδέκτης δεν ήταν σε θέση να συμμορφωθεί με το πιστοποιητικό ΕΕΥ για λόγους ανωτέρας βίας ή πραγματικής αδυναμίας ή επειδή το πιστοποιητικό ΕΕΥποβ. περιέχει πρόδηλα σφάλματα·
δ) η ευρωπαϊκή εντολή υποβολής στοιχείων δεν αφορά δεδομένα που είναι αποθηκευμένα από τον πάροχο υπηρεσιών ή για λογαριασμό του κατά τον χρόνο παραλαβής του πιστοποιητικού ΕΕΥποβ.
ε) η υπηρεσία δεν καλύπτεται από την παρούσα ΠροτΚανονισμού.
στ) με βάση αποκλειστικά τις πληροφορίες που περιέχονται στο πιστοποιητικό ΕΕΥποβ., είναι προφανές ότι το πιστοποιητικό παραβιάζει προδήλως τον Χάρτη ή ότι είναι προδήλως καταχρηστικό.

[88] Βλ. Αρ. 14 παρ. 5 της ΠροτΚανονισμού, σύμφωνα με την οποία: «*Ο αποδέκτης μπορεί να αντιταχθεί στην εκτέλεση της ΕΕΔιατ. μόνο για τους ακόλουθους λόγους:*
α) η ευρωπαϊκή εντολή διατήρησης στοιχείων δεν έχει εκδοθεί ή εγκριθεί από αρχή έκδοσης του άρθρου 4 της ΠροτΚανονισμού,
β) ο πάροχος υπηρεσιών δεν ήταν σε θέση να συμμορφωθεί με το πιστοποιητικό ΕΕΔιατ. για λόγους ανωτέρας βίας ή πραγματικής αδυναμίας ή επειδή το πιστοποιητικό ΕΕΔιατ. περιέχει πρόδηλα σφάλματα,
γ) η ευρωπαϊκή εντολή διατήρησης στοιχείων δεν αφορά δεδομένα που είναι αποθηκευμένα από τον πάροχο υπηρεσιών ή για λογαριασμό του κατά τον χρόνο του πιστοποιητικού ΕΕΔιατ.,
δ) η υπηρεσία δεν καλύπτεται από το πεδίο εφαρμογής της ΠροτΚανονισμού,
ε) με βάση αποκλειστικά τις πληροφορίες που περιέχονται στο πιστοποιητικό ΕΕΔιατ., είναι προφανές ότι το πιστοποιητικό ΕΕΔ παραβιάζει προδήλως τον Χάρτη ή ότι είναι προδήλως καταχρηστικό.»

συμπεριλαμβανομένων όμως περιπτώσεων στις οποίες η εντολή προδήλως δεν εκδόθηκε ή εγκρίθηκε από αρμόδια αρχή ή η συμμόρφωση μ' αυτήν θα παραβίαζε προδήλως τον ΧΘΔΕΕ ή θα ήταν προδήλως καταχρηστική[89].

Βλέπουμε ότι με τη διάταξη αυτή του αρ. 14 της ΠροτΚανονισμού, η Επιτροπή καταφεύγει στην γνωστή λύση της επέμβασης του κράτους εκτέλεσης όπως γίνεται ήδη και με την ΕΕΕ, που με την ΠροτΚανονισμού, προσπαθεί υπό κανονικές συνθήκες συμμόρφωσης να αποφύγει την εμπλοκή αυτού, για χάριν εξυπηρέτησης ταχύτητας και υποβολής των στοιχείων. Καταληκτικά, στην περίπτωση μη συμμόρφωσης ενός παρόχου με μία ΕΕΥποβ. αυτή μετατρέπεται σε ένα είδος ΕΕΕ, αφού πλέον για την συμμόρφωση του παρόχου και την παροχή των ηλεκτρονικών αποδεικτικών στοιχείων, απαιτείται επέμβαση αυτού και της δύναμης επιβολής των κυρώσεων που απειλούνται. Την ίδια στιγμή, όπως συμβαίνει και με την ΕΕΕ για τους λόγους αναβολής εκτέλεσης ή ενστάσεων κατά αυτής ξεκινάει μία διαδικασία διαβούλευσης ανάμεσα στο κράτος έκδοσης και στο κράτος εκτέλεσης, έτσι και στην ίδια περίπτωση για τις δύο νέες αυτές εντολές εκκινείτε αντίστοιχη διαδικασία διαβούλευσης η οποία μπορεί αρχικά να ξεκινάει με τον πάροχο και εν συνεχεία να περιλαμβάνει και το κράτος εκτέλεσης μίας ΕΕΥποβ. σε περίπτωση μη συμμόρφωσης του παρόχου να την εκτελέσει.

5.10 Χρονικά όρια απόκρισης στις εντολές

Είδαμε ότι τα χρονικά όρια απόκρισης του κράτους εκτέλεσης στην περίπτωση της διαδικασίας μίας ΕΕΕ, διαφέρουν σημαντικά και μπορεί να είναι από 30 έως 90 ημέρες ανάλογα με διάφορες προϋποθέσεις ή παράγοντες που μπορεί να προκύψουν. Ωστόσο στην περίπτωση της ΕΕΥποβ. τα χρονικά όρια συντομεύουν κατά πολύ περισσότερο και οι πάροχοι είναι υποχρεωμένοι να παρέξουν σχετικά στοιχεία ενός 10 ημερών από την παραλαβή του αιτήματος, εκτός αν η αρχή έκδοσης αναφέρει λόγους που απαιτείται να πραγματοποιηθεί νωρίτερα η γνωστοποίηση

[89] Για παράδειγμα, εντολή με την οποία θα ζητούνταν η υποβολή δεδομένων περιεχομένου που αφορούν απροσδιόριστη κατηγορία προσώπων εντός μιας γεωγραφικής περιοχής ή η οποία δεν θα συνδεόταν με συγκεκριμένη ποινική διαδικασία θα παρέβλεπε προδήλως τους όρους έκδοσης ευρωπαϊκής εντολής υποβολής στοιχείων οι οποίοι προβλέπονται στον παρόντα κανονισμό, κάτι που θα ήταν καταφανές ήδη από το περιεχόμενο του ίδιου του πιστοποιητικού. Το πρόσωπο του οποίου ζητούνται τα δεδομένα θα μπορεί να επικαλεστεί άλλους λόγους μόνο στο πλαίσιο των διαθέσιμων σ' αυτό μέσων έννομης προστασίας στο κράτος έκδοσης (βλ. άρθρο 17 της ΠροτΚανονισμού). Επιπλέον, οι πάροχοι υπηρεσιών θα πρέπει να έχουν στη διάθεσή τους ένα μέσο έννομης προστασίας κατά της απόφασης της αρχής εκτέλεσης με την οποία θα τους επιβάλλεται ποινή, (Commission Staff Working Document, 2018).

αυτών[90]. Μάλιστα, προβλέπεται ότι σε περιπτώσεις έκτακτης ανάγκης, ο αποδέκτης πάροχος απαιτείται να διαβιβάζει τα ζητούμενα δεδομένα χωρίς αδικαιολόγητη καθυστέρηση το αργότερο 6 ώρες από την παραλαβή του αιτήματος[91].Από την άλλη πλευρά, κατά την παραλαβή του μίας ΕΕΔιατ. ο αποδέκτης διατηρεί τα ζητούμενα δεδομένα χωρίς αδικαιολόγητη καθυστέρηση. Η διατήρηση αυτή παύει μετά από 60 ημέρες, εκτός αν η αρχή έκδοσης επιβεβαιώσει ότι έχει δρομολογηθεί το επακόλουθο αίτημα υποβολής αυτών των στοιχείων[92]. Αν η αρχή έκδοσης επιβεβαιώσει, εντός της προηγούμενης προθεσμίας των 60 ημερών, ότι έχει δρομολογηθεί το επακόλουθο αίτημα υποβολής[93], ο αποδέκτης πάροχος διατηρεί τα δεδομένα για όσο διάστημα απαιτείται για την υποβολή τους, μετά την επίδοση του επακόλουθου αιτήματος υποβολής[94]. Παρατηρούμε ότι τα χρονικά όρια απόκρισης στις περιπτώσεις ΕΕΥποβ. είναι σαφώς γρηγορότερα και θα επιτυγχάνουν ουσιαστική προστασία των δικαιωμάτων των θυμάτων για ταχεία και αποτελεσματική απονομή της δικαιοσύνης στο χώρο της Ένωσης, ωστόσο μπορεί να έχουν ως κόστος την ελλειμματική προστασία των δικαιωμάτων των κατηγορουμένων και των υπόπτων στην περίπτωση ΕΕΥποβ. όπως παρατηρούμε από τις ασφαλιστικές δικλίδες έννομης προστασίας κατ' αυτών.

5.11 Απόρρητο και ενημέρωση χρήστη

Όπως είναι φυσικό οι αποδέκτες αυτών των εντολών (ΕΕΥποβ. και ΕΕΔιατ.) και, αν πρόκειται περί διαφορετικών προσώπων, οι πάροχοι υπηρεσιών λαμβάνουν τα αναγκαία μέτρα ώστε να διασφαλίζουν το απόρρητο των αιτημάτων ΕΕΥποβ. και ΕΕΔιατ. και των υποβαλλόμενων ή διατηρούμενων δεδομένων και, αν αυτό ζητηθεί από την αρχή έκδοσης, δεν ενημερώνουν το πρόσωπο του οποίου τα δεδομένα ζητούνται προκειμένου να μην παρακωλύεται η σχετική ποινική διαδικασία. Την ίδια στιγμή αν η αρχή έκδοσης ζητήσει από τον αποδέκτη να μην ενημερώσει το πρόσωπο του οποίου τα δεδομένα ζητούνται, η αρχή έκδοσης ενημερώνει ως προς την υποβολή των δεδομένων, χωρίς αδικαιολόγητη καθυστέρηση, το πρόσωπο του οποίου τα δεδομένα ζητούνται με την ΕΕΥποβ. Η ενημέρωση αυτή μπορεί να καθυστερήσει για

[90] Βλ. Αρ. 9 παρ. 1 της ΠροτΚανονισμού.

[91] Βλ. Αρ. 9 παρ. 2 της ΠροτΚανονισμού.

[92] Βλ. Αρ. 10 παρ. 1 της ΠροτΚανονισμού.

[93] Δηλαδή, μπορεί να είναι ΕΕΥποβ. ή ΕΕΕ ή Αίτημα αμοιβαίας δικαστικής συνδρομής.

[94] Βλ. Αρ. 10 παρ. 2 της ΠροτΚανονισμού.

όσο διάστημα είναι αναγκαίο και αναλογικό ώστε να αποτραπεί η παρακώλυση της σχετικής ποινικής διαδικασίας. Τέλος, κατά την ενημέρωση του προσώπου, η αρχή έκδοσης παρέχει πληροφορίες σχετικά με τυχόν διαθέσιμα μέσα έννομης προστασίας (ένδικα μέσα), στο κράτος έκδοσης της εντολής[95].

Στο σημείο αυτό, παρατηρούμε ότι αν η αρχή έκδοσης δεν ζητήσει την μη ενημέρωση του προσώπου του οποίου τα δεδομένα ζητούνται, προκειμένου να μην παρακωλύεται η σχετική ποινική διαδικασία, τότε ο πάροχος ανάλογα με τους όρους που παρέχει τις υπηρεσίες του στο πεδίο της Ένωσης, ίσως οφείλει να ενημερώσει ο ίδιος το πρόσωπο αυτό. Ορισμένοι πάροχοι, στους όρους χρήσης των υπηρεσιών τους αναφέρουν σχετικές διατάξεις αναφορικά με τη συνεργασία τους με τις αρχές επιβολής του νόμου. Αντίθετα, αν η αρχή έκδοσης ζητήσει την μη ενημέρωση του προσώπου του οποίου τα δεδομένα ζητούνται, υποχρεούνται να το πράξει η ίδια όμως σε χρόνο κατά τον οποίο δεν ορίζεται ρητά σε ημέρες αλλά μπορεί να γίνει καθυστερημένα ακόμα και σε χρόνο (δηλ. μέσα σε χρονικό διάστημα είναι αναγκαίο και αναλογικό) πολύ μεταγενέστερο αυτού της υποβολής της ΕΕΥποβ. ώστε να διασφαλιστεί η μη παρακώλυση της σχετικής ποινικής διαδικασίας.

Από την άποψη παρεμβατικότητας των μέτρων, το πρόσωπο του οποίου τα δεδομένα ζητούνται δεν ειδοποιείται καθόλου στην περίπτωση υποβολής μίας ΕΕΔιατ. αλλά αντίθετα ειδοποιείται στην περίπτωση υποβολής ΕΕΥποβ. αλλά σε χρόνο που επιλέγει η αρχή έκδοσης, για λόγους προστασίας της έρευνας της υπόθεσης. Εν μέρει αυτό είναι αναγκαίο, προκειμένου αρχικά να μην γνωρίζει το πρόσωπο αυτό ότι ερευνάται και τυχόν προβεί σε ενέργειες που ίσως εξαφανίσουν ή αλλοιώσουν τα ηλεκτρονικά αποδεικτικά στοιχεία που τηρούνται στον πάροχο.

[95] Στην αιτιολογική έκθεση της ΠροτΚανονισμού, επ' αυτού σημειώνεται ότι «*Το απόρρητο της υπό εξέλιξη έρευνας, συμπεριλαμβανομένου του γεγονότος ότι έχει εκδοθεί εντολή για τη συλλογή σχετικών δεδομένων, θα πρέπει να προστατεύεται. Το εν λόγω άρθρο είναι εμπνευσμένο από το άρθρο 19 της οδηγίας ΕΕΕ. Προβλέπει την υποχρέωση του αποδέκτη και, σε περίπτωση που είναι διαφορετικά πρόσωπα, του παρόχου υπηρεσιών, να σέβονται το απόρρητο του πιστοποιητικού ΕΕΥ ή του πιστοποιητικού ΕΕΔ, ιδίως αποφεύγοντας να ενημερώσουν το πρόσωπο του οποίου τα δεδομένα ζητούνται, εφόσον διατυπώσει σχετικό αίτημα η αρχή έκδοσης, με στόχο να διασφαλιστεί η έρευνα των ποινικών αδικημάτων, σε συμμόρφωση με το άρθρο 23 του ΓΚΠΔ. Από την άλλη πλευρά, είναι σημαντικό να ενημερώνεται το πρόσωπο του οποίου ζητούνται τα δεδομένα, μεταξύ άλλων και για την άσκηση μέσων έννομης προστασίας. Αν ο πάροχος υπηρεσιών δεν προβεί στην αντίστοιχη ενέργεια κατόπιν αιτήματος της αρχής έκδοσης, η αρχή έκδοσης θα ενημερώνει το πρόσωπο σύμφωνα με το άρθρο 13 της οδηγίας για την προστασία των δεδομένων προσωπικού χαρακτήρα από τις αρχές επιβολής του νόμου, όταν δεν θα υφίσταται πλέον κίνδυνος υπονόμευσης της έρευνας, συμπεριλαμβάνοντας πληροφορίες σχετικά με τα διαθέσιμα μέσα έννομης προστασίας. Δεδομένου του λιγότερο παρεμβατικού τους χαρακτήρα ως προς τα οικεία δικαιώματα, δεν προβλέπεται η παροχή των εν λόγω πληροφοριών στην περίπτωση ευρωπαϊκής εντολής διατήρησης στοιχείων, αλλά μόνο στην περίπτωση ευρωπαϊκής εντολής υποβολής στοιχείων.*», (Commission Staff Working Document, 2018).

Καταλήγοντας είναι σημαντικό να αναφερθεί ότι με το δικαίωμα αυτό στην ενημέρωση του υποκειμένου των δεδομένων, είναι δυνατόν να εκκινήσει από αυτό και η παροχή έννομης προστασίας κατά αυτής της εντολής (ΕΕΥποβ.) κάτι που αποτελεί και την ουσία του δικαιώματος του αρ. 47 του ΧΘΔΕΕ, όπως είδαμε παραπάνω.

Κεφάλαιο Έκτο

6. Η υιοθέτηση των νομοθετικών προτάσεων από τα κράτη-μέλη

Στον ενωσιακό χώρο είναι ξεκάθαρο, ότι η Ένωση δια μέσου των κρατών μελών, μπορεί και χαράσσει την πολιτική της με βάση το δίκαιο και την δύναμη επιβολής αυτού απέναντι στην εθνική έννομη τάξη (Chalmers & Barroso, 2014). Μέσα από την αρχή της υπεροχής του Ενωσιακού δικαίου, αντιλαμβανόμαστε ότι οι δυνατότητες των κρατών μελών να αντιδράσουν απέναντι στις επιταγές του ενωσιακού νομοθέτη είναι μηδαμινές (Trstenjak, 2013), αφού συμμετέχοντας στο ενωσιακό οικοδόμημα, τα ίδια είναι που παράγουν από κοινού την ενωσιακή νομοθεσία, μέσα από τη συνήθη νομοθετική διαδικασία τις περισσότερες φορές, οπότε όποιες ενστάσεις ή προβληματισμούς διαθέτουν, οφείλουν να τους αμβλύνουν κατά το στάδιο των διαπραγματεύσεων της σχετικής νομοθέτησης, όταν ακόμη η υπό συζήτηση νομοθεσία διαπραγματεύεται σε ενωσιακό επίπεδο (Kwiecień, 2005).

Ωστόσο μπορεί να διαπιστώνεται και το αντίθετο. Εάν ένα κράτος μέλος ή ορισμένα κράτη μέλη αντιμετωπίζουν δυσχέρειες για τη ρύθμιση έντονα αμφιλεγόμενων θεμάτων στο εσωτερικό τους, για τα οποία έχει εξουσία η Ένωση να αναλάβει δράση σχετικά, τότε ίσως προσπαθήσουν να υπερκεράσουν τις δυσκολίες στο εσωτερικό, μέσω της ενωσιακής οδού αναζητώντας να ρυθμιστεί σχετικά το θέμα σε ενωσιακό πλέον επίπεδο (Παπαγιάννης, 2008).

Αν αυτό εν τέλει επιτευχθεί, τότε ο εθνικός νομοθέτης μεταβάλλεται στη συνέχεια σχεδόν σε «*εκτελεστικό νομοθέτη*», αφού πλέον θα είναι υποχρεωμένα τα κράτη μέλη να μεταφέρουν στην εθνική έννομη τάξη, την ενωσιακή ρύθμιση χωρίς κανέναν σχεδόν περιθώριο, διακριτικής ευχέρειας, αν μάλιστα πρόκειται και για κανονισμό. Η πρακτική αυτή, εφόσον τηρούνται όλες οι ενωσιακές διαδικαστικές ρυθμίσεις και καλύπτεται η ρυθμιστέα ύλη από τον ενωσιακό νομοθέτη για την άσκηση αρμοδιότητας από την Ένωση, δε θα πρέπει να θεωρείται καταδικαστέα. Η διαδικασία αυτή είναι ανεκτή αν πληρείται πρώτα από όλα και η αρχή της επικουρικότητας (Παπαγιάννης, 2008).

Έτσι με αυτό τον τρόπο, βλέπουμε ότι η δύναμη της Ένωσης να κυβερνά μέσω του δικαίου (Chalmers & Barroso, 2014), μπορεί να προέρχεται είτε με πρωτοβουλία που προέρχεται από την ίδια Ένωση και μετέπειτα αποδοχή από τα κράτη μέλη με την συνήθη νομοθετική διαδικασία, είτε με την ανάδειξη των θεμάτων

από τα κράτη μέλη με σκοπό να αναλάβει ξανά ρόλο η Ένωση για την προώθηση αυτών. Η διαδικασία αυτή, είναι συνεχής και θα μπορούσε να ειπωθεί ότι δεν είναι επ' ουδενί κατακριτέα άλλα αντίθετα, προωθείται με αυτόν τον τρόπο, η ευρωπαϊκή ολοκλήρωση (Saurugger & Terpan, 2021).

Έτσι και στην περίπτωση της πρότασης του Κανονισμού και της Οδηγίας για τα ηλεκτρονικά αποδεικτικά στοιχεία η Επιτροπή όπως είδαμε στηρίζεται στις επιτυχημένες επιλογές της Ευρωπαϊκής Εντολής Έρευνας αλλά και εν μέρει στα στοιχεία ορισμού υπευθύνων στους παρόχους υπηρεσιών διαδικτύου στην πρόταση της Οδηγίας, όπως πετυχημένα έπραξε με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων[96], προκειμένου να μπορεί να εξασφαλίσει την αποτελεσματική λειτουργία των δικαστικών εντολών που θεσπίζονται με την ΠροτΚανονισμού και αφορούν τις δύο εντολές όπως τις είδαμε, προηγουμένως.

Στην περίπτωση της Ελλάδας και ειδικότερα στον ΚΠΔ έχουν προβλεφθεί αντίστοιχες ρυθμίσεις για την κατάσχεση και συνεπώς την αξιοποίηση των ψηφιακών δεδομένων ως αποδεικτικών στοιχείων στο αρ. 265 ΚΠΔ[97]. Επιπλέον στην έννοια του

---

[96] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων), (ΕΕ L 119 της 4.5.2016, σ. 1).

[97] Ειδικότερα αναφέρεται στο αρ. 265 ΚΠΔ αναφέρεται ότι «*1. Η κατάσχεση ψηφιακών δεδομένων μπορεί να επιβληθεί: α) Σε ένα σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτόν, στα οποία έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση, β) σε ένα μέσο αποθήκευσης δεδομένων υπολογιστή στο οποίο υπάρχουν αποθηκευμένα δεδομένα υπολογιστή και έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση, γ) σε ένα απομακρυσμένο σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτόν ή σε ένα απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτό, τα οποία είναι διασυνδεδεμένα στο σύστημα υπολογιστή στο οποίο έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση. Στην τελευταία περίπτωση, τα ψηφιακά δεδομένα που είναι αποθηκευμένα και προσβάσιμα μέσω συστήματος και υπηρεσιών νεφοϋπολογιστικής (cloudservices) δεν θεωρούνται αποθηκευμένα σε απομακρυσμένο σύστημα υπολογιστή ή σε απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή τα οποία είναι διασυνδεδεμένα στο σύστημα υπολογιστή στο οποίο έχουν φυσική πρόσβαση οι αρχές.2. Η κατά τα ανωτέρω κατάσχεση πραγματοποιείται αποκλειστικά με τη χρήση κατάλληλου εξοπλισμού που επιτρέπει σε εκείνον που τη διεξάγει:α) Την αφαίρεση και την κατάσχεση του υλικού φορέα των υπό στοιχείων α-γ της παρ. 1, στο οποίο βρίσκονται αποθηκευμένα τα δεδομένα και/ήβ) την αντιγραφή και την αφαίρεση των αποθηκευμένων ψηφιακών δεδομένων των υπό στοιχείων α-γ της παρ. 1 σε μέσο αποθήκευσης δεδομένων καιγ) την αναπαραγωγή και την επαλήθευση της αυθεντικότητας και της ακεραιότητας των κατασχεθέντων δεδομένων. 3. Η κατάσχεση που διενεργείται κατά τις παρ. 1 και 2, βεβαιώνεται με ειδική έκθεση, η οποία αναφέρει ειδικώς τις ενέργειες της παρ. 2 που πραγματοποιεί εκείνος που διεξάγει την ανάκριση. 4. Τα ψηφιακά δεδομένα που κατάσχονται διατηρούνται αποθηκευμένα καθ' όλη τη διάρκεια της ποινικής διαδικασίας σε ένα και μόνο υλικό μέσο αποθήκευσης που περιέχεται στη δικογραφία. Ασφαλές αντίγραφο αυτού ώστε να διασφαλίζεται η δυνατότητα ανάκτησης των δεδομένων που έχουν κατασχεθεί, σε περίπτωση απώλειας ή καταστροφής, σχηματίζεται κατά την κατάσχεσή τους και διατηρείται στο γραφείο πειστηρίων του πρωτοδικείου στο οποίο υποβάλλεται η δικογραφία και το οποίο παρέχει τις κατάλληλες εγγυήσεις φυσικής ασφάλειας και πρόσβασης σε εκείνους μόνο που ασκούν καθήκοντα στην υπόθεση. Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία. 5. Η πρόσβαση και η δυνατότητα αναπαραγωγής των ψηφιακών δεδομένων που κατάσχονται επιτρέπεται μόνο σε όσους ασκούν δικαστικά, εισαγγελικά και ανακριτικά καθήκοντα στην υπόθεση ή τους γραμματείς. Προς το σκοπό αυτό χρησιμοποιούνται τα κατάλληλα τεχνικά μέσα. Τέτοια μέσα είναι η κρυπτογράφηση και η χρήση κωδικών ασφαλείας για την πρόσβαση και αναπαραγωγή των κατασχεμένων ψηφιακών δεδομένων από το υλικό μέσο αποθήκευσης στο οποίο βρίσκονται αποθηκευμένα. Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας*

αρ. 13 ΠΚ στοιχείο ζ) ορίζονται τα πληροφοριακά συστήματα[98] και τα ψηφιακά δεδομένα[99].

Στην περίπτωση που οι προτάσεις υιοθετηθούν στην τελική τους μορφή όπως θα διαμορφωθούν μετά το τέλος της νομοθετικής διαδικασίας (συμφωνία Συμβουλίου και Ευρωπαϊκού Κοινοβουλίου[100]) τότε ο εθνικός νομοθέτης στην περίπτωση της ΠροτΚανονισμού, θα εκδώσει έναν εκτελεστικό νόμο προκειμένου να προσαρμοστούν οι απαιτήσεις του Κανονισμού στην ελληνική έννομή τάξη και να οριστούν τυχόν οι δικαστικές αρχές που θα είναι αρμόδιες επί του θέματος όπως έγινε και στην περίπτωση της ΕΕΕ ενώ στην περίπτωση της ΠροτΟδηγίας, θα μεταφερθεί πάλι με το πρόσφορο νομοθετικό μέσο (νόμος ή προεδρικό διάταγμα) στην ελληνική έννομη τάξη οι ρυθμίσεις που επιβάλλονται να ρυθμιστούν στους παρόχους υπηρεσιών διαδικτύου, προκειμένου να μπορούν να παραλαμβάνουν τις αντίστοιχες εντολές ΕΕΥποβ. και ΕΕΔιατ., προκειμένου το όλο εγχείρημα να ξεκινήσει να λειτουργεί με επιτυχία.

Στην περίπτωση αυτή και μεταφερόμενοι στην ελληνική πραγματικότητα οι αρμόδιες αρχές της Ελλάδας, ως κράτους μέλους, θα έχουν στη διάθεση τους τρία νομικά εργαλεία, για την απόκτηση αποδεικτικών στοιχείων από άλλο κράτος μέλος, μία ΕΕΕ, μία ΕΕΥποβ. και μία ΕΕΔιατ. Ωστόσο έχοντας αυτά στη διάθεση τους, οι αρμόδιες αρχές επιβολής του νόμου, ίσως είναι πιο εύκολο για αυτές να επιλέγουν τις εντολές για την απόκτηση ηλεκτρονικών αποδεικτικών στοιχείων και ίσως λιγότερο την ΕΕΕ και αυτό γιατί η διαδικασία όπως φαίνεται με τις ΕΕΥποβ. και ΕΕΔιατ. θα είναι πολύ πιο απλή και δεν θα παρεμβάλλεται μία αρχή στο κράτος εκτέλεσης των εντολών, τα στοιχεία θα περιέρχονται στην κατοχή τους σε συντομότερο χρόνο αλλά

που περιλαμβάνονται στη δικογραφία. 6. Απαγορεύεται η δημιουργία και η διατήρηση αντιγράφων των ψηφιακών δεδομένων για οποιονδήποτε άλλον λόγο εκτός αν ο αρμόδιος εισαγγελέας ή ανακριτής ή συμβούλιο ή το δικαστήριο κρίνουν ότι τα κατασχεμένα ψηφιακά δεδομένα είναι αναγκαίο να περιληφθούν σε άλλη δικογραφία. Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία.».

[98] Ειδικότερα αναφέρεται στο αρ. 13 ΠΔ στοιχείο στ) ορίζεται ότι «*Πληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών.*»

[99] Ειδικότερα αναφέρεται στο αρ. 13 ΠΔ στοιχείο ζ) ορίζεται ότι «*Ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία.*»

[100] *"e-Evidence: Commission welcomes political agreement to strengthen cross-border access for criminal investigations", Πηγή:*https://ec.europa.eu/commission/presscorner/detail/es/ip_22_7246

υπάρχει επίσης και πίεση η επ' επαπειλούμενη κύρωση προς την πλευρά των παρόχων αν δεν συμμορφωθούν με αυτές. Επιπλέον υπάρχει και η δυνατότητα μία ΕΕΥποβ. να μετατραπεί σε μία ΕΕΕ, αν ο πάροχος δεν παρέχει τα στοιχεία που αιτούνται και οι λόγοι απόρριψης αυτών των εντολών είναι πολύ λιγότερες από ότι στην ΕΕΕ. Ίσως στην περίπτωση αυτή, τα ηλεκτρονικά αποδεικτικά στοιχεία αποτελέσουν τα μόνα στοιχεία ή αυτά γύρω από τα οποία θα στηρίζονται οι κατηγορίες στις ποινικές υποθέσεις χωρίς των αξιοποίηση άλλων αποδεικτικών στοιχείων και χωρίς την δυνατότητα αυτές εντολές (ΕΕΥποβ. και ΕΕΔιατ.) μέχρι τώρα τουλάχιστον, να χρησιμοποιηθούν για την υπεράσπιση του κατηγορούμενου ή του υπόπτου.

Ωστόσο στην περίπτωση των ηλεκτρονικών αποδεικτικών στοιχείων, όπως είδαμε το ευμετάβλητο αυτό, το κόστος διατήρησης αυτών από τους παρόχους και η ταχύτατα με την οποία μπορούν να μεταβάλλονται στην σύγχρονη πραγματικότητα όπως αυτή έχει δημιουργηθεί, απαιτεί και την αντίστοιχη ταχύτητα δράσης από την πλευρά των αρμόδιων αρχών. Ωστόσο από την πλευρά των αρχών επιβολής του νόμου, η ζητούμενη ταχεία πρόσβαση σε δεδομένα ή πληροφορίες τηρούμενα στους παρόχους με τις προτεινόμενες εντολές (ΕΕΥποβ. και ΕΕΔιατ.), ίσως θυσιάζει ένα σημαντικό επίπεδο προστασίας των θεμελιωδών δικαιωμάτων που σε διαφορετική περίπτωση, όπως για παράδειγμα στην περίπτωση εφαρμογής ΕΕΕ, θα εξακολουθούσε να ισχύει, όπως είδαμε προηγουμένως.

6.1 Διαδικασία της ενωσιακής νομοθέτησης

Το πακέτο των προτάσεων για τα ηλεκτρονικά αποδεικτικά στοιχεία από το 2018 που υποβλήθηκε η σχετική πρόταση από την Επιτροπή, μέχρι και πρόσφατα τον Νοέμβριο του 2022, βρισκόταν υπό νομοθετική διαμόρφωση καθώς βρισκόταν στη φάση της αναδιαμόρφωσης από τις αρμόδιες Επιτροπές του Συμβουλίου και του Ευρωπαϊκού Κοινοβουλίου (Τρίλογοι). Ωστόσο με πρόσφατη ανακοίνωση την 29 Νοεμβρίου 2022, η Επιτροπή καλωσορίζει την προσωρινή πολιτική συμφωνία που επιτεύχθηκε από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, αναφορικά με τους νέους κανόνες για την ανταλλαγή ηλεκτρονικών αποδεικτικών στοιχείων σε ολόκληρη την Ένωση. Όπως αναφέρει χαρακτηριστικά η Επιτροπή στην ανακοίνωση της «*Η παρούσα συμφωνία θα οδηγήσει στην επίσημη υιοθέτηση μιας οδηγίας και ενός κανονισμού για την υιοθέτηση της σχετικής πρότασης της Επιτροπής, όπως αναδιαμορφώθηκε*».

Ακολούθως, το Κοινοβούλιο και το Συμβούλιο θα πρέπει να υιοθετήσουν επισήμως και με ψηφοφορία την πολιτική συμφωνία που επιτεύχθηκε στα πλαίσια της νομοθετικής διαδικασίας στην Ευρωπαϊκή Ένωση. Εν συνεχεία, μόλις δημοσιευθεί στην επίσημη εφημερίδα της Ευρωπαϊκής Ένωσης, το τελικό κείμενο του Κανονισμού αναφορικά με τα ηλεκτρονικά αποδεικτικά στοιχεία θα τεθεί σε ισχύ 20 ημέρες μετά τη δημοσίευση στην επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης και θα τεθεί σε εφαρμογή μετά από τρία χρόνια. Το τελικό κείμενο της Οδηγίας, αναφορικά με τα ηλεκτρονικά αποδεικτικά στοιχεία θα τεθεί σε ισχύ 20 ημέρες μετά τη δημοσίευση στην επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης και τα κράτη μέλη θα πρέπει στη συνέχεια να μεταφέρουν τα νέα στοιχεία της οδηγίας στο εθνικό τους δίκαιο σε χρονικό διάστημα εντός δυόμισι ετών.

Με τον τρόπο αυτό, φαίνεται ξεκάθαρα η προθυμία της Ένωσης να δώσει στα κράτη μέλη τον απαραίτητο χρόνο, προκειμένου να μεταφέρουν αφενός πρώτα στο εθνικό τους δίκαιο τις διατάξεις της Οδηγίας αναφορικά με τον ορισμό αντιπρόσωπων των διάφορων παρόχων για την εκτέλεση των σχετικών Εντολών για την απόκτηση και διατήρηση αποδεικτικών στοιχείων σε διάστημα δυόμισι ετών, προκειμένου εν συνεχεία μετά την πάροδο ακόμα ενός εξαμήνου, τα τεθεί τελικά σε εφαρμογή και ο Κανονισμός αναφορικά με την έκδοση των σχετικών εντολών, αλλάζοντας ριζικά το τοπίο και τον τρόπο με τον οποίο οι αρχές επιβολής του νόμου, θα είναι σε θέση να αποκτούν και να συλλέγουν ηλεκτρονικά αποδεικτικά στοιχεία.

Κεφάλαιο Έβδομο

7. Συμπεράσματα

Δεν υπάρχει αμφιβολία ότι με την αυξητική τάση που σημειώνει το έγκλημα στον κυβερνοχώρο απαιτείται και αντίστοιχη δράση από την πλευρά των διωκτικών αρχών. Στο πλαίσιο αυτό, απαιτείται αλλαγή του τρόπου σκέψης για την αντιμετώπιση αυτού του ταχέος εξελισσόμενου φαινομένου που δυστυχώς τρέχει πιο γρήγορα από τους διώκτες του (Jerman Blažič & Klobučar, 2020a).

Για το λόγο, αυτό απαιτείται η εισαγωγή νέων και αποτελεσματικότερων τρόπων καταπολέμησης αυτού του φαινομένου, προκειμένου να ενισχυθεί πιο αποτελεσματικά και το αίσθημα ασφάλειας στον κυβερνοχώρο αλλά και να γίνει αντιληπτό ότι και ο κυβερνοχώρος έχει όρια και ότι διέπεται από κανόνες, όπως και ο πραγματικός κόσμος (Maillart, 2019).

Ένας τρόπος για να γίνουν πιο αποτελεσματικές οι εθνικές και δικαστικές αρχές των κρατών μελών, είναι να καταστεί δυνατή η αποτελεσματικότερη πρόσβαση σε ηλεκτρονικές αποδείξεις και αυτό γιατί γίνεται αντιληπτό ότι ο σύγχρονος ψηφιακός κόσμος επεκτείνεται σε πολλά γεωγραφικά κράτη, ακόμη και πέρα από τα όρια της Ένωσης (Buono, 2019).

Επομένως, είναι λογικό να υποθέσουμε ότι, προκειμένου να λύσουμε το κύριο πρόβλημα της ταχύτητας απόκτησης των ηλεκτρονικών αποδείξεων όπου με την εφαρμογής συμφωνιών αμοιβαίας δικαστικής συνδρομής, απαιτούνται ορισμένες φορές ακόμη και μήνες για την παροχή αυτών, χρειαζόμαστε έναν ταχύτερο δρόμο (Blažič & Klobučar, 2020b; Rojszczak, 2022).

Η Επιτροπή, αντιλαμβανομένη αυτές τις αλλαγές πρότεινε το πακέτο για τα ηλεκτρονικά αποδεικτικά στοιχεία, προκειμένου να επιταχυνθούν οι διαδικασίες απόκτησης αυτών απευθείας από τους παρόχους (Blažič & Klobučar, 2020b; Buono, 2019; Rojszczak, 2022).

Με την εισαγωγή μιας ΕΕΥποβ. και μιας ΕΕΔιατ., θα καθίσταται ευκολότερο για τα κράτη μέλη και τις αρχές αυτών να διασφαλίζουν και να συγκεντρώνουν ηλεκτρονικά αποδεικτικά στοιχεία, για τις ποινικές διαδικασίες που είναι αποθηκευμένα ή τηρούνται από παρόχους υπηρεσιών που είναι εγκατεστημένοι σε άλλη δικαιοδοσία(Μιχαηλίδου, 2018).

Η Επιτροπή, αντιλαμβάνεται τις απαιτήσεις της εποχής για ταχύτητα στην απονομή της δικαιοσύνης και επάνω στη δοκιμασμένη συνταγή της Ευρωπαϊκής Εντολής Έρευνας, έρχεται και προτείνει μία νομοθεσία για να διευκολύνει και να επιταχύνει την πρόσβαση των αρχών επιβολής του νόμου και των δικαστικών αρχών των κρατών μελών στα ηλεκτρονικά αποδεικτικά στοιχεία για την καλύτερη αντιμετώπιση του εγκλήματος αλλά και της τρομοκρατίας (Buono, 2019; Ευρωπαϊκή Επιτροπή, 2018a; Μιχαηλίδου, 2018). Αυτή θα παράσχει στις αρχές τα κατάλληλα εργαλεία για την διερεύνηση και την δίωξη των εγκλημάτων στην ψηφιακή εποχή.

Οι προτεινόμενοι νέοι κανόνες θα είναι σε θέση να παράσχουν ένα πιο γρήγορο εργαλείο για την απόκτηση της ηλεκτρονικής απόδειξης στις εθνικές αρχές των κρατών μελών. Η ΕΕΕ και η Αμοιβαία Δικαστική Συνδρομή, με τρίτες χώρα θα συνεχίσουν να υφίστανται, αλλά θα υπάρξει μια γρήγορη εναλλακτική «***λεωφόρος***» παροχής στοιχείων, η ΕΕΥποβ. Χαρακτηριστικό αυτής είναι ότι θα χαρακτηρίζεται από ταχύτητα για την συγκεκριμένη περίπτωση κτήσης ηλεκτρονικών αποδείξεων, γι' αυτό άλλωστε και χαρακτηρίζεται ως «*λεωφόρος*», αφού τα παραδοσιακά μέσα απόκτησης των ηλεκτρονικών αποδεικτικών στοιχείων διαμέσου της Ευρωπαϊκής Εντολής Έρευνας και της Αμοιβαίας Δικαστικής Συνδρομής παραμένουν χωρίς να εξαφανίζονται από το προσκήνιο (Jerman Blažič & Klobučar, 2019).

Ωστόσο, με την ευρωπαϊκή εντολής έρευνας (ΕΕΕ), όπου πιθανώς θα προτιμάται για λόγους καλύτερης εγγύησης και προστασίας των δικαιωμάτων των υπόπτων (Jerman Blažič & Klobučar, 2020b) πιθανώς θα υπάρχουν καθυστερήσεις στην απόκτηση αυτών αλλά καλύτερη προστασία των δικαιωμάτων των προσώπων που ανήκουν τα αιτούμενα δεδομένα.

Οι νέοι κανόνες της Ένωσης θα επιτρέψουν στην δικαστική αρχή να απευθύνεται απευθείας στον νόμιμο εκπρόσωπο του παρόχου υπηρεσιών σε άλλο κράτος μέλος μέσα από τον ορισμό των νόμιμων εκπροσώπων των παρόχων (Ευρωπαϊκή Επιτροπή, 2018b), οι οποίοι θεσπίζονται στα πρότυπα του Υπευθύνου Επεξεργασίας Δεδομένων κατά τον ΓΚΠΔ.

Οι δύο νέες εντολές υποβολής και διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων δεν απαιτούν έγκριση και έλεγχο από το κράτος εκτέλεσης, αλλά απευθύνονται κατευθείαν στον πάροχο επικοινωνιών, για να παρέχει τα στοιχεία στο κράτος έκδοσης. Για το λόγο αυτό, οι ηλεκτρονικές αποδείξεις, δεν χρειάζεται πλέον

να ταξιδεύουν μέσω πολλών «χεριών», αλλά θα πηγαίνει κατευθείαν από τον νόμιμο εκπρόσωπο στην αρμόδια εθνική αρχή του κράτους έκδοσης, που αιτήθηκε τα δεδομένα(Ευρωπαϊκή Επιτροπή, 2018b).

Ωστόσο στη περίπτωση αυτή, ο διττός έλεγχος της δικαστικής εντολής από μία δικαστική αρχή στο κράτος εκτέλεσης, απαλείφεται και δεν διενεργείται, όπως γίνεται στην Ευρωπαϊκή Εντολής Έρευνας. Αυτό συμβαίνει προκειμένου να εξυπηρετηθεί ο σκοπός της ταχύτητας, απόκτησης αυτών των ηλεκτρονικών αποδείξεων. Οι προτεινόμενοι νέοι κανόνες από την Επιτροπή, περιλαμβάνουν επίσης και μια Ευρωπαϊκή Εντολή Διατήρησης Στοιχείων (ΕΕΔιατ.) που μπορεί να εκδίδεται για να αποφεύγεται η διαγραφή της ηλεκτρονικής απόδειξης (Ευρωπαϊκή Επιτροπή, 2018b), προκειμένου οι αρχές να μπορούν μετέπειτα να αποκτήσουν αυτά μέσω της Ευρωπαϊκή Εντολή Υποβολής Στοιχείων (ΕΕΥποβ.) ή διαμέσου της Ευρωπαϊκής Εντολής Έρευνας (ΕΕΕ). Με την απαίτηση για ταχύτητα υποβολής των απαιτούμενων στοιχείων, εξυπηρετείται κυρίως η αρχή της αποτελεσματικότητας για την ταχεία απόκτηση των ηλεκτρονικών αποδεικτικών στοιχείων (10 ημέρες ή 6 ώρες σε επείγον ζητήματα).

Επιπλέον, με τις προτάσεις αυτές παρατηρούμε ότι τα δεδομένα που τηρούνται από τους παρόχους κατηγοριοποιούνται σε τέσσερις μεγάλες κατηγορίες. Την ίδια στιγμή, σταθμίζονται τα ζητούμενα δεδομένα ανάλογα με το είδος αυτών σε αυξημένης δικαστικής προστασίας και μειωμένης, απαιτώντας διαφορετικές προϋποθέσεις για την έκδοση εντολής υποβολής στοιχείων, για τα δεδομένα που δεν αφορούν περιεχόμενο του χρήστη και γι’ αυτά που αφορούν, όπως τα είδαμε προηγουμένως.

Πέραν αυτών με την υιοθέτηση των νέων ρυθμίσεων και την εκτέλεση των ΕΕΥποβ. και ΕΕΔιατ. από τους παρόχους, ουσιαστικά αναβαθμίζει τις σχέσεις μεταξύ αυτών και των αρχών επιβολής του νόμου. Στην ουσία οι ιδιώτες πάροχοι υπηρεσιών, θα μετατραπούν είτε το θέλουν είτε όχι στο μακρύ χέρι (long arm) αυτών των αρχών στις οποίες θα διαβιβάζουν τα σχετικά στοιχεία χωρίς να περνούν από τον έλεγχο άλλων αρμόδιων δικαστικών ή εισαγγελικών αρχών πίσω στο κράτος έκδοσης των ΕΕΥποβ. και ΕΕΔιατ.

Προβληματικό καθίσταται το ζήτημα ότι ο πάροχος καλείται να σταθμίσει τα δικαιώματα του προσώπου που αφορούν τα δεδομένα, χωρίς να παρεμβάλλεται άλλη

δικαστική αρχή πέραν αυτή (της αρχικής) του κράτους έκδοσης (Φαρμακίδης, 2021), όπως είδαμε για λόγους εξυπηρέτησης της ταχύτητας.

Ακόμη, με το πακέτο προτάσεων τα κράτη μέλη είναι δυνατόν να επιβάλλουν κυρώσεις στους παρόχους για μη συμμόρφωση και την παροχή των απαιτούμενων στοιχείων στις περιπτώσεις που αυτά αιτηθούν και δεν παρασχεθούν. Για το λόγο αυτό, οι αρχές επιβολής του νόμου με την διαβίβαση αυτών των εντολών (ΕΕΥποβ. & ΕΕΔιατ.), θα μπορούν πάντοτε να υπενθυμίζουν τους παρόχους τις ποινές και τα πρόστιμα που δυνητικά μπορούν να τους επιβληθούν σε περιπτώσεις μη συμμόρφωσης με αυτές τις εντολές, καθιστώντας τους τελευταίους (δηλ. τους παρόχους) αναξιόπιστους υπερασπιστές των θεμελιωδών δικαιωμάτων των ευρωπαίων πολιτών (Mitsilegas, 2018), την στιγμή που ορισμένοι εξ' αυτών των παρόχων ίσως δεν προέρχονται ή δεν λειτουργούν με έδρα κάποιο κράτος μέλος της Ένωσης όπου οι νομικές βάσεις προστασίας θεμελιωδών δικαιωμάτων ίσως να ήταν ίδιες με βάση τον Κανονισμό για τα Προσωπικά Δεδομένα, άλλα σε κάποιο τρίτο κράτος, όπου ο νομικός τους κόσμος διαφέρει σημαντικά και δεν παρέχει καν ελάχιστες εγγυήσεις προστασίας που προσφέρει ο χώρος της Ένωσης (βλ. για παράδειγμα την Κίνα).

Έτσι ουσιαστικά, οι αρχές επιβολής του νόμου με την έκδοση και την επικύρωση από τις αρμόδιες δικαστικές αρχές των αντίστοιχων ΕΕΥποβ. και ΕΕΔιατ. και εν συνεχεία την παραλαβή αυτών των ηλεκτρονικών αποδεικτικών στοιχείων υποκαθιστούν εθνικές αρχές που είναι αρμόδιες για την αξιολόγηση αυτών των στοιχείων σε πρώτο βαθμό. Ωστόσο τέτοια αξιολόγηση των ηλεκτρονικών αποδεικτικών στοιχείων που αποκτήθηκαν, μπορεί να γίνεται μεταγενέστερα κατά την ποινική διαδικασία είτε στην επ' ακροατήριο διαδικασία είτε στην αξιολόγηση των αποδεικτικών στοιχείων στην διαδικασία της ανάκρισης και του δικαστικού συμβουλίου αν πρόκειται για κακούργημα στην περίπτωση της Ελλάδας.

Καταλήγοντας, χρειάζεται να έχουμε κατά νου ότι με το πακέτο προτάσεων της Επιτροπής, γύρω από τα ηλεκτρονικά αποδεικτικά στοιχεία και ανεξάρτητα από τον τρόπο με τον οποίο αυτά θα εφαρμοστούν στην πράξη, όταν υιοθετηθούν, απαιτείται να εξασφαλιστεί μία αμοιβαία συνοχή και νομιμότητα εξασφάλισης τόσο των επιδιωκόμενων σκοπών όσο και της προστασίας των δικαιωμάτων των υποκειμένων των δεδομένων αυτών, που θα καθίστανται ύποπτοι και κατηγορούμενοι με βάση τις αιτήσεις αυτές (Smuha, 2018).

Έτσι, η εφαρμογή στην πράξη των προτεινόμενων ρυθμίσεων, ίσως στην αρχή αποτελέσει πρόκληση για τις αρχές επιβολής του νόμου ή για τις δικαστικές αρχές, ωστόσο η επιτυχία αυτών θα εξαρτηθεί από τη διασφάλιση ότι στο τελικό υιοθετηθέν σχήμα της νομοθεσίας γύρω από την απόκτηση ηλεκτρονικών αποδεικτικών στοιχείων στην Ένωση, συνάδει με τον νομικό της πολιτισμό για την εγγύηση και την προστασία των δικαιωμάτων των υποκειμένων και επιτυγχάνει από την μία πλευρά, εκείνη την λεπτή την ισορροπία μεταξύ της διευκόλυνσης του έργου των διωκτικών αρχών των κρατών μελών και από την άλλη πλευρά αυτήν της προστασίας και του σεβασμού των δικαιωμάτων των προσώπων που στοχεύουν (Rojszczak, 2022).

8. Βιβλιογραφία[101]

Allegrezza, S. (2014). Collecting criminal evidence across the European union: The European investigation order between flexibility and proportionality. In S. Ruggeri (Ed.), *Transnational Evidence and Multicultural Inquiries in Europe: Developments in Eu Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-Border Cases* (pp. 51–67). Springer. https://doi.org/10.1007/978-3-319-02570-4_5

Armada, I. (2015). The European Investigation Order and the Lack of European Standards for Gathering Evidence: Is a Fundamental Rights-Based Refusal the Solution? *New Journal of European Criminal Law*, *6*(1), 31–38. https://doi.org/https://doi.org/10.1177/203228441500600103

Balzacq, T., Léonard, S., & Ruzicka, J. (2015). 'Securitization' revisited: theory and cases. *International Relations*, *30*(4), 494–531. https://doi.org/10.1177/0047117815596590

Biasiotti, M. A., Cannataci, J. A., Mifsud Bonnici, J. P., & Turchi, F. (2018). Introduction: Opportunities and Challenges for Electronic Evidence. In *Law, Governance and Technology Series* (Vol. 39, pp. 3–12). https://doi.org/10.1007/978-3-319-74872-6_1

Blažič, B. J., & Klobučar, T. (2020a). Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society. *Information and Communications Technology Law*, *29*(1), 66–81. https://doi.org/10.1080/13600834.2020.1705035

Blažič, B. J., & Klobučar, T. (2020b). Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society. *Information and Communications Technology Law*, *29*(1), 66–81. https://doi.org/10.1080/13600834.2020.1705035

Buono, L. (2019). The genesis of the European Union's new proposed legal instrument(s) on e-evidence. *ERA Forum*, *19*(3), 307–312. https://doi.org/10.1007/s12027-018-0525-4

Buzan, B., Waever, O., & Jaap De Wilde. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers Inc.

Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: cross-border criminal investigations and digital evidence. *Journal of Cybersecurity*, *8*(1), tyac014. https://doi.org/10.1093/cybsec/tyac014

CEPOL. (2017). Online Learning Module on Cybercrime. Budapest. Retrieved from https://www.cepol.europa.eu/

Chalmers, D., & Barroso, L. (2014). What Van Gend en Loos stands for. *International Journal of Constitutional Law*, *12*(1), 105–134. https://doi.org/10.1093/icon/mou003

Chavleski, A., & Galev, G. (2019). GATHERING E-EVIDENCE IN CROSS-BORDER CASES: RECENT DEVELOPMENTS IN EU LAW. *Knowledge*

[101]Η βιβλιογραφία έχει συνταχθεί με τη χρήση του ψηφιακού βιβλιογραφικού εργαλείου Mendeley (www.mendeley.com).

International Journal, *32*(1), 155–162. https://doi.org/10.35120/KIJ3201155C

Commission Staff Working Document. (2018). *Impact Assessment Accompanying the document-Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Par* (No. SWD (2018) 118 final). Brussels. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN

Council of Europe. (2001). Convention on Cybercrime. Retrieved October 8, 2017, from http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Darmois, E., & Schméder, G. (2018). Cybersecurity: A case for a European approach. In M. Kaldor, I. Rangelov, & S. Selchow (Eds.), *EU Global Strategy and Human Security* (1st Editio, pp. 194–214). London: Routledge. Retrieved from https://www.taylorfrancis.com/chapters/cybersecurity-geneviève-schméder-emmanuel-darmois/e/10.4324/9781315104232-11?context=ubx&refId=e83d174a-1ed0-46df-8852-d9219bbd9f30

Depauw, S. (2018). Electronic Evidence in Criminal Matters: How About E-Evidence Instruments 2.0? *European Criminal Law Review*, *8*(1), 62–82. https://doi.org/10.5771/2193-5505-2018-1-62

Drent, M., Landman, L., & Zandee, D. (2014). The EU as a Security Provider. The Hague: Clingendael. Retrieved from https://www.clingendael.org/sites/default/files/pdfs/Report_EU_as_a_Security_Provider_december_2014.pdf

EU Global Strategy. (2016). *A Global Strategy for the European Union's Foreign And Security Policy. Shared Vision, Common Action: A Stronger Europe.* Brussels. Retrieved from http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

Eurojust. (2020). *SIRIUS EU Digital Evidence Situation Report.* The Hague, Netherlands. Retrieved from https://www.eurojust.europa.eu/sirius-eu-digital-evidence-situation--report

European Commission. (2020). *EU Security Union Strategy* (No. COM(2020) 605 final). Brussels. Retrieved from https://ec.europa.eu/info/sites/info/files/communication-eu-security-union-strategy.pdf

Europol. (2021). EU Internet Referral Unit - EU IRU: Monitoring terrorism online. Retrieved from https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru#fndtn-tabs-0-bottom-1

Europol SOCTA. (2021). *European Union serious and organised crime threat assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime*. Luxembourg. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

Foggetti, N. (2008). Transnational Cyber Crime, Differences Between National Laws and Development of European Legislation: By Repression? *Masaryk University Journal of Law and Technology*, *2*(2), 31–45. Retrieved from

https://www.ceeol.com/search/article-detail?id=895596

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175. Retrieved from http://www.jstor.org/stable/27735139

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks. *Journal of Strategic Security*, *4*(2), 49–60. Retrieved from http://www.jstor.org/stable/26463926

Ilves, T. H. (2016). The Consequences of Cyber Attacks. *Journal of International Affairs*, *70*(1), 175–181. Retrieved from https://www.jstor.org/stable/90012601

Jerman Blažič, B., & Klobučar, T. (2019). Advancement in Cybercrime Investigation – The New European Legal Instruments for Collecting Cross-border E-evidence BT - Information Technology and Systems. In Á. Rocha, C. Ferrás, & M. Paredes (Eds.) (pp. 858–867). Cham: Springer International Publishing.

Jerman Blažič, B., & Klobučar, T. (2020a). Investigating crime in an interconnected society: will the new and updated EU judicial environment remove the barriers to justice? *International Review of Law, Computers and Technology*, *34*(1), 87–107. https://doi.org/10.1080/13600869.2019.1700434

Jerman Blažič, B., & Klobučar, T. (2020b). Investigating crime in an interconnected society: will the new and updated EU judicial environment remove the barriers to justice? *International Review of Law, Computers and Technology*, *34*(1), 87–107. https://doi.org/10.1080/13600869.2019.1700434

Kim, G. (2022). Enhancing Cooperation Between South Korea and the EU in the Fight Against Cybercrime BT - Cybersecurity Policy in the EU and South Korea from Consultation to Action: Theoretical and Comparative Perspectives. In G. Boulet, M. Reiterer, & R. P. Pardo (Eds.) (pp. 197–213). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-08384-6_10

Kwiecień, R. (2005). The Primacy of European Union Law over National Law Under the Constitutional Treaty. *German Law Journal*, *6*(11), 1479–1495. https://doi.org/DOI: 10.1017/S2071832200014450

Maillart, J.-B. (2019). The limits of subjective territorial jurisdiction in the context of cybercrime. *ERA Forum*, *19*(3), 375–390. https://doi.org/10.1007/s12027-018-0527-2

Mitsilegas, V. (2018). The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence. *Maastricht Journal of European and Comparative Law*, *25*(3), 263–265. https://doi.org/10.1177/1023263X18792240

Moraski, L. (2011). Cybercrime Knows No Borders. *Infosecurity*, *8*(2), 20–23. https://doi.org/https://doi.org/10.1016/S1754-4548(11)70021-3

Pisaric, M. (2021). Encryption as a challenge for European law enforcement agencies. *Australasian Policing*, *13*(1), 30–34. Retrieved from https://search.informit.org/doi/10.3316/informit.692047204127258

Rogalski, M. (2020). The European Commission's e-evidence proposal - Critical remarks and proposals for changes. *European Journal of Crime, Criminal Law and Criminal Justice*, *28*(4), 333–353. https://doi.org/10.1163/15718174-BJA10018

Rojszczak, M. (2022). e-Evidence Cooperation in Criminal Matters from an EU

Perspective. *The Modern Law Review*, *85*(4), 997–1028. https://doi.org/https://doi.org/10.1111/1468-2230.12749

Russell, A. L. (2014). *Cyber Blockades*. Georgetown University Press. Retrieved from http://www.jstor.org/stable/j.ctt9qdsfj

Saurugger, S., & Terpan, F. (2021). Normative transformations in the European Union: on hardening and softening law. *West European Politics*, *44*(1), 1–20. https://doi.org/10.1080/01402382.2020.1762440

Scrivens, R., Gill, P., & Conway, M. (2020). The Role of the Internet in Facilitating Violent Extremism and Terrorism: Suggestions for Progressing Research. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 1417–1435). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_61

Smuha, N. A. (2018). Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency. *European Criminal Law Review*, *8*(1), 83–115. Retrieved from https://ssrn.com/abstract=3501421

Stritzel, H. (2014). Securitization Theory and the Copenhagen School. In *Security in Translation* (pp. 11–37). London: Palgrave Macmillan UK. https://doi.org/10.1057/9781137307576_2

Terziev, V., Petkov, M., & Dragomir, K. (2021). Concept of joint investigation teams. *IJASOS- International E-Journal of Advances in Social Sciences*, *7*(19), 324–331. https://doi.org/https://dx.doi.org/10.2139/ssrn.3838627

Tinoco-Pastrana, Á. (2020). The Proposal on Electronic Evidence in the European Union. *Eucrim*, (1), 46–50. https://doi.org/10.30709/eucrim-2020-004

Tosza, S. (2018). The European Commission's proposal on cross-border access to E-evidence. *Eucrim: The European Criminal Law Associations' Fórum, ISSN 1862-6947, Nº. 4, 2018, Pág. 1*, (4), 1. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=6844099&info=resumen&idioma=ENG

Tosza, S. (2019). The European Commission's Proposal on Cross-Border Access to E-Evidence. Overview and Critical Remarks. *Eucrim*, *2018*(4), 212–219. https://doi.org/10.30709/EUCRIM-2018-021

Tosza, S. (2020). All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order. *New Journal of European Criminal Law*, *11*(2), 161–183. https://doi.org/10.1177/2032284420919802

Trstenjak, V. (2013). National Sovereignity and the Principle of Primacy in EU Law and Their Importance for the Member States. *Beijing Law Review*, *04*(2), 71–76. https://doi.org/10.4236/blr.2013.42009

Zaharieva, R. (2017). The European Investigation Order and the Joint Investigation Team—which road to take. *ERA Forum*, *18*(3), 397–408. https://doi.org/10.1007/s12027-017-0483-2

Αρβανίτης, Δ. (2021). *Η Ευρωπαϊκή Εντολή Έρευνας: Συστηματική Προσέγγιση του θεσμού της συνεργασίας σε ποινικές υποθέσεις στην Ευρωπαϊκή Ένωση κατά τη*

χρονική του διάσταση. Αθήνα: Π.Ν. Σάκκουλα.

Γέρμανος, Γ., & Γεωργίου, Ν. (2021). *Κυβερνοέγλημα: Πρόληψη, Διευρένηση, Αντιμετώπιση.* (1η). Αθήνα: Αυτοέκδδοση.

Ευρωπαϊκή Επιτροπή. (2018a). *Πρόταση ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις* (No. 2018/0108 (COD)). Στρασβούργο: COM(2018) 225 final. Retrieved from https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52018PC0225&from=EN#footnote8

Ευρωπαϊκή Επιτροπή. (2018b). *Πρόταση ΟΔΗΓΙΑ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον ορισμό νόμιμων εκπροσώπων με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών* (2018/0107(COD) No. COM(2018) 226 final). Στρασβούργο. Retrieved from https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52018PC0226&from=EN

Λιαρόπουλος, Α. (2018). Το ΝΑΤΟ και οι προκλήσεις στον κυβερνοχώρο. Retrieved from https://www.tanea.gr/print/2018/11/06/opinions/to-nato-kai-oi-prokliseis-ston-kyvernoxoro/

Μιχαηλίδου, Χ. (2018, November). Κυβερνοέγκλημα και ηλεκτρονική απόδειξη – ένας τρόπος εξακρίβωσης του ψηφιακού αποτυπώματός του. Ευρώπη με μια ματιά. Retrieved May 20, 2022, from shorturl.at/egluJ

Παπαγιάννης, Δ. (2008). *Ο χώρος της Ασφάλειας στην Ευρωπαϊκή Ένωση*. Αθήνα: ΕΚδ. Αντ. Ν. Σάκκουλα.

Παπαγιάννης, Δ. (2016). *Ευρωπαϊκό Δίκαιο* (5η). Αθήνα: Νομική Βιβλιοθήκη.

Παπακωνσταντής, Μ. (2019). *Η τρομοκρατία στο χώρο ελευθερίας, ασφάλειας και δικαιοσύνης της Ευρωπαϊκής Ένωσης* (1η). Αθήνα: Νομική Βιβλιοθήκη.

ΣΛΕΕ. (2012, October 26). Ενοποιημένη απόδοση της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης - Πρωτόκολλα - Παραρτήματα - Δηλώσεις οι οποίες προσαρτώνται στην Τελική Πράξη της Διακυβερνητικής Διάσκεψης η οποία υιοθέτησε τη Συνθήκη της Λισσαβώνας που υπογράφηκε στις 13 Δεκεμβρίου 2007. Retrieved April 4, 2020, from https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:12012M/TXT

Τσιλίκης, Δ. (2021). Η διασυνοριακή συλλογή ηλεκτρονικών αποδείξεων στον ενωσιακό χώρο-Προβληματισμοί για την σχεδιαζόμενη νομοθετική ρύθμιση της η-απόδειξης (e-evidence). *Ποινικά Χρονικά, Απρίλιος*(4), 241. Retrieved from https://www.sakkoulas.com/pinika-chronika/i-diasynoriaki-syllogi-ilektronikon-apodeikseon-ston-enosiako-choro-provlimatismoi-gia-tin-schediazomeni-nomothetiki-rythmisi-tis-i-apodeiksis-e-evidence/

Φαρμακίδης, Ε. (2021). Ευρωπαϊκή Εντολή Υποβολής και Ευρωπαϊκή Εντολή Διατήρησης στοιχείων - Η προσαρμογή των θεσμών δικαστικής συνεργασίας σε ποινικές υποθέσεις στην ψηφιακή εποχή. *Ποινική Δικαιοσύνη*, *1*, 28–43.

9. Παράρτημα

Πίνακας 1: Βασικά σημεία σύγκρισης μεταξύ Ευρωπαϊκής Εντολής Έρευνας και Ευρωπαϊκής Εντολής Διατήρησης και Υποβολής Ηλεκτρονικών αποδεικτικών στοιχείων

Σημεία Σύγκρισης	***Ευρωπαϊκή Εντολή Έρευνας***	***Ευρωπαϊκή Εντολή Διατήρησης Ηλεκτρονικών αποδεικτικών στοιχείων***	***Ευρωπαϊκή Εντολή Υποβολής Ηλεκτρονικών αποδεικτικών στοιχείων***
Θεσμός στον οποίο βασίζονται (Νομική βάση)	Αμοιβαία αναγνώριση δικαστικών αποφάσεων	Αμοιβαία αναγνώριση δικαστικών αποφάσεων	Αμοιβαία αναγνώριση δικαστικών αποφάσεων
Είδος νομοθεσίας με την οποία εισάγονται στο εθνικό δίκαιο	Οδηγία	Κανονισμός	Κανονισμός
Σκοπός του μέτρου	Συλλογή αποδεικτικών στοιχείων σε άλλο κράτος μέλος	Συλλογή ηλεκτρονικών αποδεικτικών στοιχείων που κατέχει ένας πάροχος	Διατήρηση ηλεκτρονικών αποδεικτικών στοιχείων που κατέχει ένας πάροχος
Είδος στοιχείων που πρόκειται να αποκτηθούν	Χρησιμοποιείται και για άλλα αποδεικτικά στοιχεία αλλά και για ηλεκτρονικά αποδεικτικά στοιχεία	Χρησιμοποιείται αποκλειστικά για ηλεκτρονικά αποδεικτικά στοιχεία	Χρησιμοποιείται αποκλειστικά για ηλεκτρονικά αποδεικτικά στοιχεία
Κράτος Έκδοσης	Ναι υπάρχει	Ναι υπάρχει	Ναι υπάρχει
Κράτος Εκτέλεσης	Ναι υπάρχει	Δεν υπάρχει, απευθύνεται στον πάροχο απευθείας	Δεν υπάρχει, απευθύνεται στον πάροχο απευθείας
Συνθήκες που χρειάζεται να ισχύουν για να εκδοθεί	Αναγκαιότητα και Αναλογικότητα. Το ερευνητικό μέτρο να υπάρχει στο εγχώριο δίκαιο του κράτους εκτέλεσης.	Αναγκαιότητα και Αναλογικότητα. Το ερευνητικό μέτρο να υπάρχει στο εγχώριο δίκαιο του κράτους εκτέλεσης. Εντολές για την υποβολή δεδομένων συνδρομητή και πρόσβασης μπορούν να εκδοθούν για οποιοδήποτε ποινικό αδίκημα. Για δεδομένα περιεχομένου και συναλλαγών απαιτούνται να συντρέχουν περισσότερες προϋποθέσεις.	Η ευρωπαϊκή εντολή διατήρησης στοιχείων υπόκειται στις ίδιες προϋποθέσεις με την ευρωπαϊκή εντολή υποβολής στοιχείων, δηλαδή: Α. Αναγκαιότητα και Αναλογικότητα. Β. Το ερευνητικό μέτρο να υπάρχει στο εγχώριο δίκαιο του κράτους εκτέλεσης. Γ. Μπορεί να εκδοθεί για οποιοδήποτε αδίκημα.
Δικαστικές Αρχές Έκδοσης	Μπορεί να είναι δικαστικές αρχές εξ' αρχής.	Μπορεί να είναι δικαστικές αρχές εξ' αρχής.	Μπορεί να είναι δικαστικές αρχές εξ' αρχής.
Άλλες αρχές έκδοσης	Μπορεί να είναι άλλες αρμόδιες αρχές, ωστόσο απαιτείται επικύρωση από αρμόδια δικαστική αρχή.	Μπορεί να είναι άλλες αρμόδιες αρχές, ωστόσο απαιτείται επικύρωση από αρμόδια δικαστική αρχή.	Μπορεί να είναι άλλες αρμόδιες αρχές, ωστόσο απαιτείται επικύρωση από αρμόδια δικαστική αρχή.

Αρχή Εκτέλεσης/ Αποδέκτης Εντολής	Αρμόδια αρχή στο κράτος εκτέλεσης	Αρμόδιος πάροχος υπηρεσιών διαδικτύου ή επικοινωνιών.	Αρμόδιος πάροχος υπηρεσιών διαδικτύου ή επικοινωνιών.
Μπορεί να την αιτηθεί ο κατηγορούμενος;	Ναι μπορεί για υπερασπιστικούς λόγους	Δεν υπάρχει αντίστοιχη πρόβλεψη.	Δεν υπάρχει αντίστοιχη πρόβλεψη.
Διάκριση αποδεικτικών στοιχείων που ζητούνται	Οποιουδήποτε είδους αποδεικτικό στοιχείο, με τους περιορισμούς που έχει η Οδηγία της ΕΕΕ, συμπεριλαμβανομένου και ηλεκτρονικά αποδεικτικά στοιχεία.	Διάκριση δεδομένων ανάλογα με την δικαστική προστασία που απαιτείται για κάθε ένα από αυτά. Για δεδομένα περιεχομένου απαιτούνται να συντρέχουν περισσότερες προϋποθέσεις.	Διατήρηση οποιοδήποτε είδους ηλεκτρονικά αποδεικτικά στοιχεία τηρούνται στον πάροχο.
Συγκεκριμένα αδικήματα επί των οποίων εκδίδεται	Ισχύει η γενική αρχή του διττού αξιόποινου της συμπεριφοράς για την οποία εκδίδεται.	Το διττό αξιόποινο εισάγεται μόνο για την υποβολή δεδομένων περιεχομένου.	Είναι δυνατή για όλα τα αδικήματα.
Διαβούλευση μεταξύ αρχής έκδοσης και αρχής εκτέλεσης	Ναι υπάρχει αυτή η δυνατότητα επί συγκεκριμένων θεμάτων	Ναι υπάρχει αυτή η δυνατότητα επί συγκεκριμένων θεμάτων	Ναι υπάρχει αυτή η δυνατότητα επί συγκεκριμένων θεμάτων
Μέρη της διαβούλευσης μεταξύ αρχής έκδοσης και αρχής εκτέλεσης	Κράτος Έκδοσης και Κράτος Εκτέλεσης	Κράτος Έκδοσης και Πάροχος Σε ειδικές περιπτώσεις μπορεί να είναι κράτος έκδοσης και κράτος εκτέλεσης	Κράτος Έκδοσης και Πάροχος Σε ειδικές περιπτώσεις μπορεί να είναι κράτος έκδοσης και κράτος εκτέλεσης
Έλεγχος διττού αξιόποινου	Το διττό αξιόποινο της συμπεριφοράς ορίζεται ως λόγος άρνησης αναγνώρισης ή εκτέλεσης.	Το διττό αξιόποινο εισάγεται μόνο για την υποβολή δεδομένων περιεχομένου, οπότε και απαιτούνται να συντρέχουν περισσότερες προϋποθέσεις.	Δεν πραγματοποιείται έλεγχος διττού αξιόποινου. Μπορεί να εκδοθεί για οποιοδήποτε ποινικό αδίκημα.
Ένδικα μέσα κατά αυτής	Παρέχονται για συγκεκριμένους λόγους.	Παρέχονται για λόγους που αφορούν την αναγκαιότητα και την αναλογικότητα του μέτρου.	Δεν παρέχονται.
Λόγοι αναβολής εκτέλεσης	Συγκεκριμένοι λόγοι που εδράζονται σε συγκεκριμένα άρθρα της Οδηγίας ΕΕΕ	Συγκεκριμένοι λόγοι, πιο περιορισμένοι με την ΕΕΕ Αναφορά σε συγκεκριμένα άρθρα της ΠροτΚανονισμού	Συγκεκριμένοι λόγοι, πιο περιορισμένοι με την ΕΕΕ Αναφορά σε συγκεκριμένα άρθρα της ΠροτΚανονισμού
Λόγοι άρνησης εκτέλεσης	Συγκεκριμένοι λόγοι που εδράζονται σε συγκεκριμένα άρθρα της Οδηγίας ΕΕΕ	Συγκεκριμένοι λόγοι αναφορικά με τη φύση και τις προϋποθέσεις της εν λόγω εντολής (βλ. αρ. 14 παρ. 4 της ΠροτΚανονισμού)	Συγκεκριμένοι λόγοι αναφορικά με τη φύση και τις προϋποθέσεις της εν λόγω εντολής (βλ. αρ. 14 παρ. 5 της ΠροτΚανονισμού)
Δυνατότητα υπαναχώρησης	Ναι υπάρχει από το κράτος έκδοσης της ΕΕΕ, αν δεν είναι δυνατόν να εκτελεστεί	Δεν υπάρχει δυνατότητα υπαναχώρησης της εντολής. Δυνατότητα υπαναχώρησης μόνο αν η εντολή αφορά	Δεν υπάρχει δυνατότητα υπαναχώρησης της εντολής. Δυνατότητα υπαναχώρησης μόνο αν η εντολή αφορά

		ασυλίες ή άλλα προνόμια σύμφωνα με το δίκαιο τρίτης χώρας. Μπορεί υπό προϋποθέσεις να ανακαλείται η εντολή.	ασυλίες ή άλλα προνόμια σύμφωνα με το δίκαιο τρίτης χώρας. Μπορεί υπό προϋποθέσεις να ανακαλείται η εντολή.
Μη συμμόρφωση με εντολή	Δεν υπάρχει τέτοια πρόβλεψη, η συμμόρφωση στο κράτος εκτέλεσης διασφαλίζεται από την αρχή της αμοιβαίας αναγνώρισης των δικαστικών αποφάσεων στο πεδίο της Ένωσης.	Μετατρέπεται σε εν είδει ΕΕΕ και συμμετέχει το κράτος εκτέλεσης για την διασφάλιση συμμόρφωσης του παρόχου.	Μετατρέπεται σε εν είδει ΕΕΕ και συμμετέχει το κράτος εκτέλεσης για την διασφάλιση συμμόρφωσης του παρόχου.
Επιβολή ποινής για μη συμμόρφωση με εντολή	Δυνητική κίνηση της διαδικασίας από το κράτος μέλος προς την Επιτροπή, αναφορικά με τις περιπτώσεις μη εφαρμογή Οδηγίας της ΕΕ, με βάση το πρωτογενές δίκαιο της Ένωσης.	Ναι υπάρχει τέτοια πρόβλεψη. Πρόβλεψη για φυλάκιση τουλάχιστον τεσσάρων (4) ετών. Πρόβλεψη για πρόστιμο ίσο με το 2% του παγκόσμιου τζίρου του παρόχου. Δεν υπάρχει πρόβλεψη για ποιο κράτος είναι αρμόδιο για την επιβολή της ποινής	Ναι υπάρχει τέτοια πρόβλεψη
Προθεσμίες εκτέλεσης της Εντολής	Μέχρι την συγκεκριμένη ημερομηνία που ορίζεται από το κράτος έκδοσης, υπό αίρεση. Σε χρονικό διάστημα μεταξύ 30 και 90 ημερών, ανάλογα με προθεσμίες ή άλλα κωλύματα.	Μέσα σε 10 μέρες παροχή στοιχείων από τον πάροχο. Σε έκτακτες περιπτώσεις παροχή στοιχείων μέσα σε 6 ώρες.	Άμεση δέσμευση των στοιχείων που ζητούνται από την εντολή.
Καθιέρωση τυποποιημένης μορφής εντολής	Ναι υπάρχει σχετική πρόβλεψη στην Οδηγία ΕΕΕ. Σχετικό υπόδειγμα υπάρχει στο επίσημο κείμενο της ευρωπαϊκής νομοθεσίας	Ναι υπάρχει σχετική πρόβλεψη στην προτεινόμενη νομοθεσία. Σχετικό υπόδειγμα υπάρχει στο επίσημο κείμενο της ευρωπαϊκής νομοθεσίας.	Ναι υπάρχει σχετική πρόβλεψη στην προτεινόμενη νομοθεσία. Σχετικό υπόδειγμα υπάρχει στο επίσημο κείμενο της ευρωπαϊκής νομοθεσίας.