ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

Η ΔΙΑΣΥΝΟΡΙΑΚΗ ΠΡΟΣΒΑΣΗ ΤΩΝ ΑΡΧΩΝ ΣΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΑΠΟΔΕΙΚΤΙΚΑ ΣΤΟΙΧΕΙΑ ΣΕ ΠΟΙΝΙΚΕΣ ΥΠΟΘΕΣΕΙΣ

Διπλωματική Εργασία

του

Ευάγγελου Β. Φαρμακίδη

Θεσσαλονίκη, 11/2019

Η ΔΙΑΣΥΝΟΡΙΑΚΗ ΠΡΟΣΒΑΣΗ ΤΩΝ ΑΡΧΩΝ ΣΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΑΠΟΔΕΙΚΤΙΚΑ ΣΤΟΙΧΕΙΑ ΣΕ ΠΟΙΝΙΚΕΣ ΥΠΟΘΕΣΕΙΣ

Ευάγγελος Β. Φαρμακίδης

Πτυχίο Νομικής Σχολής ΔΠΘ, 2017

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Θεοχάρης Ι. Δαλακούρας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 2/11/2019

Ονοματεπώνυμο 1	Ονοματεπώνυμο 2	Ονοματεπώνυμο 3
.....	.....	.....

Ευάγγελος Β. Φαρμακίδης

Περίληψη

Σήμερα, εγκληματικές πράξεις δύναται να τελούνται ταχύτατα μέσω του Διαδικτύου από τα πιο απομακρυσμένα σημεία του πλανήτη και να αναπτύσσουν τα εγκληματικά αποτελέσματά τους σε πολλά κράτη ταυτόχρονα. Την ίδια στιγμή, τα ηλεκτρονικά αποδεικτικά στοιχεία που θα μπορούσαν να οδηγήσουν στην ανακάλυψη του δράστη ή να αποδείξουν την ενοχή του μπορούν να αποθηκεύονται σε οποιοδήποτε μέρος του πλανήτη. Έτσι, η συνεργασία των Αρχών επιβολής του Νόμου όλων των κρατών του κόσμου αναδεικνύεται περισσότερο αναγκαία από ποτέ για την αντιμετώπιση του Κυβερνοεγκλήματος.

Επί του παρόντος, για την πρόσβαση σε ηλεκτρονικά αποδεικτικά μέσα σε παγκόσμιο επίπεδο τυγχάνουν εφαρμογής οι διατάξεις διεθνούς συνεργασίας της Σύμβασης για το Έγκλημα στον Κυβερνοχώρο. Σε επίπεδο Ευρωπαϊκής Ένωσης (ΕΕ), το βασικότερο «εργαλείο» των Αρχών αποτελεί η Ευρωπαϊκή Εντολή Έρευνας. Ωστόσο, η πλειοψηφία των διαδικτυακών εταιριών – «κολοσσών» εδρεύουν στις Ηνωμένες Πολιτείες της Αμερικής (ΗΠΑ). Μεταξύ ΕΕ και ΗΠΑ έχει υπογραφεί Συμφωνία Αμοιβαίας Δικαστικής Συνδρομής ήδη από το έτος 2003 και εφαρμόζεται από το 2010. Τέλος, ο μεγάλος όγκος των αιτημάτων συνδρομής των Ευρωπαϊκών Αρχών προς τις ΗΠΑ και η ανάγκη για ταχύτερη πρόσβαση στα ηλεκτρονικά αποδεικτικά μέσα, λόγω κυρίως του ευμετάβλητου χαρακτήρα τους, δημιούργησαν ένα νέο μοντέλο συνεργασίας: η νομοθεσία των ΗΠΑ επιτρέπει στους Παρόχους Υπηρεσιών να συνεργάζονται απευθείας με τις Αρχές επιβολής του Νόμου άλλων Κρατών, όπως για παράδειγμα των Κρατών της ΕΕ, θέτοντας όμως κάποιους σημαντικούς περιορισμούς.

Η ανάγκη για τη θέσπιση αποτελεσματικών θεσμών διασυνοριακής συνεργασίας ειδικότερα στον τομέα των ηλεκτρονικών αποδεικτικών μέσων σε ποινικές υποθέσεις οδήγησε πρόσφατα σε έντονες συζητήσεις και διαπραγματεύσεις, τόσο σε Ευρωπαϊκό όσο και σε παγκόσμιο επίπεδο. Στις 17 Απριλίου 2018 η Επιτροπή ενέκρινε δύο νομοθετικές προτάσεις: την Πρόταση Κανονισμού σχετικά με την Ευρωπαϊκή Εντολή Υποβολής και την Ευρωπαϊκή Εντολή Διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις και την Πρόταση Οδηγίας σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον ορισμό νόμιμων εκπροσώπων με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών, η οποία συμπληρώνει τον παραπάνω Κανονισμό. Εξελίξεις στον τομέα των ηλεκτρονικών αποδεικτικών

μέσων σε ποινικές υποθέσεις προηγήθηκαν στις ΗΠΑ., όπου στις 23 Μαρτίου 2018 εκδόθηκε από το Κογκρέσο των Ηνωμένων Πολιτειών της Αμερικής ο Νόμος Clarifying Lawful Use of Overseas Data (CLOUD) Act, για την αποσαφήνιση της νόμιμης χρήσης δεδομένων στο εξωτερικό. Μεταξύ των άλλων ο Νόμος αυτός εξουσιοδοτεί την εκτελεστική εξουσία των ΗΠΑ να συνάπτει συμφωνίες με ξένες κυβερνήσεις, σύμφωνα με τις οποίες οι ξένες κυβερνήσεις μπορούν να αποκτήσουν ταχεία πρόσβαση στα δεδομένα, που διατηρούνται εντός της επικράτειας των ΗΠΑ. Έτσι, άνοιξε ο δρόμος για την έναρξη των διαπραγματεύσεων μεταξύ ΗΠΑ και ΕΕ για την υπογραφή Σύμβασης Αμοιβαίας Δικαστικής Συνδρομής στον τομέα των ηλεκτρονικών αποδεικτικών μέσων σε ποινικές υποθέσεις, διαπραγματεύσεις, οι οποίες ξεκίνησαν επίσημα την 6η Ιουνίου 2019. Τέλος, σε παγκόσμιο επίπεδο, την ίδια ημέρα το Ευρωπαϊκό Συμβούλιο εξουσιοδότησε την Ευρωπαϊκή Επιτροπή να διαπραγματευθεί εκ μέρους της ΕΕ το Δεύτερο Πρόσθετο Πρωτόκολλο της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο.

Λέξεις Κλειδιά: Κυβερνοέγκλημα, Ηλεκτρονικά Αποδεικτικά Μέσα, Ποινικό Δίκαιο, Σύμβαση για το Έγκλημα στον Κυβερνοχώρο, Συμφωνία Αμοιβαίας Δικαστικής Συνδρομής, Ευρωπαϊκή Εντολή Έρευνας, Ευρωπαϊκή Εντολή Υποβολής, Ευρωπαϊκή Εντολή Διατήρησης, Δεύτερο Πρόσθετο Πρωτόκολλο Σύμβασης για το Έγκλημα στον Κυβερνοχώρο, Clarifying Lawful Use of Overseas Data (CLOUD) Act

Abstract

Nowadays, crimes can be carried out quickly through the Internet from the most remote parts of the world and can spread their criminal effects in many states simultaneously. At the same time, electronic evidence that could lead to the discovery of the offender or prove his responsibility can be stored anywhere on the planet. Thus, the co-operation of the law enforcement authorities of all the states of the world is more than ever needed to tackle Cybercrime.

At present, the provisions of international cooperation in the Convention on Cybercrime apply to access to electronic evidence worldwide. At European Union level, the main tool used by the Authorities is the European Investigation Order. However, the vast majority of web-based companies are in the US. An EU-US Mutual Legal Assistance Treaty has been signed since 2003, which has been in force since 2010. Finally, the volume of European Authorities' requests to the US and the need for faster access to electronic evidence, largely due to their volatile nature, have created a new model of cooperation: US law allows Service Providers to work directly with Authorities enforcing the Law of other States, such as those of the EU, but imposing some significant restrictions.

The need to establish effective cross-border co-operation institutions, in particular in the field of electronic evidence in criminal matters, has recently led to intense debate and negotiation, both at European and global level. On 17 April 2018, the Commission adopted two legislative proposals: the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and the Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, which supplements the above Regulation. Developments in the field of electronic evidence in criminal cases preceded the US, where on March 23, 2018, the United States Congress passed the Clarifying Lawful Use of Overseas Data (CLOUD) Act to clarify legal use of data abroad. Among other things, this Act empowers the US executive to conclude agreements with foreign governments that allow foreign governments to gain rapid access to data held within US territory. This opened the way for the opening of negotiations between the US and the EU on the signing of a Mutual Assistance Convention in the field of electronic evidence in criminal matters, negotiations that officially began on 6 June 2019.

Finally, at the global level, day the European Council authorized the European Commission to negotiate on behalf of the EU the Second Additional Protocol to the Council of Europe Convention on Cybercrime.

Keywords: Cybercrime, Electronic Evidence, Criminal Law, Convention on Cybercrime, Mutual Legal Assistance Treaty, European Investigation Order, European Production Order, European Preservation Order, Second Additional Protocol to the Council of Europe Convention on Cybercrime, Clarifying Lawful Use of Overseas Data (CLOUD) Act

Πρόλογος – Ευχαριστίες

Ολοκληρώνοντας τις σπουδές μου στο Διϊδρυματικό Πρόγραμμα Μεταπτυχιακών Σπουδών (ΔΠΜΣ) "*Δίκαιο και Πληροφορική*" με την παράδοση της παρούσας εργασίας, τα συναισθήματά μου είναι ανάμεικτα: αφενός νιώθω χαρά για την επιτυχή ολοκλήρωση των σπουδών μου και αφετέρου λύπη, διότι ένα πολύ όμορφο ταξίδι φτάνει στο τέλος του.

Λίγο πριν το τέλος λοιπόν, νιώθω την ηθική υποχρέωση να ευχαριστήσω θερμά την Διευθύντρια του Προγράμματος, Καθηγήτρια Ευγενία Αλεξανδροπούλου - Αιγυπτιάδου, αλλά και όλους τους διδάσκοντες του -πρωτοποριακού για τα δεδομένα της χώρας μας- Διϊδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών για το νέο «παράθυρο», που μου άνοιξαν σε έναν -μέχρι πρότινος άγνωστο σε εμένα- μαγικό κόσμο, τον κόσμο της Πληροφορικής.

Ιδιαίτερες ευχαριστίες οφείλω στον αξιότιμο Καθηγητή κ. Θεοχάρη Ι. Δαλακούρα για την πολύτιμη υποστήριξή του στην εκπόνηση της παρούσας εργασίας και την αμέριστη εμπιστοσύνη, την οποία επιδεικνύει προς το πρόσωπό μου. Δίχως την εμβρίθειά του, τη γενναιόδωρη, απλόχερη και ανιδιοτελή συνδρομή των βαθύτατων γνώσεών του, του αέναου ενδιαφέροντός του για την επιστήμη του Δικαίου και της ακούραστης εκ μέρους του παρακολούθησης των τρεχουσών εξελίξεων, η εκπόνηση της παρούσας εργασίας θα ήταν ανέφικτη.

Φυσικά, το ταξίδι αυτό δε θα ήταν τόσο όμορφο χωρίς τους «συνεπιβάτες» - συμφοιτητές μου. Δικαστικοί λειτουργοί, δικηγόροι, αστυνομικοί, επιστήμονες της Πληροφορικής αλλά και άλλων επιστημονικών κλάδων, μοιραστήκαμε επιστημονικές ανησυχίες και προβληματισμούς, καθώς και αξέχαστες ακαδημαϊκές και «εξω-ακαδημαϊκές» στιγμές. Σε αυτούς αφιερώνεται η παρούσα εργασία.

Ίσως τελικά, πράγματι, το «ταξίδι» να είναι πιο όμορφο από τον «προορισμό».

Θεσσαλονίκη, Νοέμβριος 2019

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

i. Εισαγωγικό υπόβαθρο

Μια εργασία που πραγματεύεται ζητήματα ηλεκτρονικού εγκλήματος δε θα μπορούσε να ξεκινά με άλλη φράση, πλην της ακόλουθης: "*Η τεχνολογία σήμερα έχει εισχωρήσει σε κάθε πτυχή της καθημερινότητάς μας δημιουργώντας καινοφανείς, ποινικά ενδιαφέρουσες συμπεριφορές και νεοπαγή εγκληματικά φαινόμενα.*" Όσο κοινότυπη όμως και αν ακούγεται η παραπάνω φράση, αποκρυσταλλώνει με τον πιο γλαφυρό τρόπο τη σύγχρονη πραγματικότητα. Αποτελεί κοινό τόπο ότι η Πληροφορική, οι ηλεκτρονικοί υπολογιστές, το Διαδίκτυο και γενικότερα οι σύγχρονες τεχνολογίες έχουν αλλάξει άρδην την καθημερινότητα των ανθρώπων, διευκολύνοντας σε μεγάλο βαθμό τη ζωή μας, αλλά ταυτόχρονα δημιούργησαν ένα νέο, ευρύ πεδίο για την ανάπτυξη αντικοινωνικών, εγκληματικών συμπεριφορών. Σήμερα, σε έναν μεγάλο βαθμό η οικονομική ανάπτυξη και η κοινωνική ευημερία βασίζονται στις νέες τεχνολογίες και σε καινοτόμες υπηρεσίες, όπως είναι τα μέσα κοινωνικής δικτύωσης, το διαδικτυακό ηλεκτρονικό ταχυδρομείο, υπηρεσίες άμεσης ανταλλαγής μηνυμάτων και άλλων εφαρμογών με σκοπό την επικοινωνία, την εργασία, τη συναναστροφή με άλλους ανθρώπους και την απόκτηση πληροφοριών. Οι υπηρεσίες αυτές συνδέουν εκατοντάδες εκατομμύρια χρήστες μεταξύ τους. Παράγουν πολλά και σημαντικά οφέλη για την οικονομία και την κοινωνία. Ωστόσο, είναι επίσης δυνατή η κατάχρησή τους, καθώς μπορούν να αποτελέσουν εργαλεία για τη διάπραξη ή τη διευκόλυνση εγκλημάτων, μεταξύ των οποίων και σοβαρά εγκλήματα όπως τρομοκρατικές επιθέσεις[1]. Η πληροφορική δεν άνοιξε, λοιπόν, μόνον παράθυρα στον κόσμο, αλλά και στις δυνατότητες προσβολής των εννόμων αγαθών[2].

Όταν τελείται ένα Κυβερνοέγκλημα, οι διαδικτυακές υπηρεσίες και εφαρμογές είναι συχνά το μόνο μέρος, στο οποίο οι ερευνητές μπορούν να βρουν ενδείξεις για να προσδιορίσουν ποιος διέπραξε ένα έγκλημα και να συλλέξουν αποδεικτικά στοιχεία, τα οποία μπορούν να χρησιμοποιηθούν στο δικαστήριο[3]. Τα Κυβερνοεγκλήματα - ιδίως τα stricto sensu[4]-

[1] Αιτιολογική Έκθεση, Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις, COM(2018) 225 final

[2] Μ. Καϊάφα - Γκμπάντι, Ποινικό δίκαιο και καταχρήσεις της Πληροφορικής, Αρμενόπουλος 7/2007, σελ. 1058

[3] Αιτιολογική Έκθεση, ο.π.

εξελίσσονται αποκλειστικά στον ψηφιακό και διαδικτυακό χώρο και δεν υφίσταται καμία άλλη δυνατότητα απόδειξής τους, παρά μόνο η χρήση ως αποδεικτικών μέσων των ψηφιακών δεδομένων, τα οποία είτε υπέστησαν βλάβη, είτε χρησιμοποιήθηκαν για την τέλεση ενός Κυβερνοεγκλήματος[5].

ii. Ηλεκτρονικά αποδεικτικά στοιχεία και η δυσκολία διασυνοριακής πρόσβασης σε αυτά

Από τη φύση του, το έγκλημα στον Κυβερνοχώρο δεν έχει σύνορα και χαρακτηρίζεται από ευελιξία και καινοτομία[6]. Ο διεθνής χαρακτήρας του Διαδικτύου επιτρέπει σε μια εταιρία παροχής υπηρεσιών να παρέχει τις υπηρεσίες της οπουδήποτε στον κόσμο και σε πολλά κράτη ταυτόχρονα, χωρίς όμως να έχει απαραίτητα εταιρική παρουσία, προσωπικό ή εγκαταστάσεις [π.χ. διακομιστές (servers) κ.α.] στα κράτη αυτά. Επιπλέον, τα δεδομένα που παράγονται από τη χρήση της υπηρεσίας δύναται να αποθηκεύονται σε οποιοδήποτε μέρος του κόσμου[7]. Σε πολλές περιπτώσεις, τα δεδομένα δεν αποθηκεύονται ούτε υποβάλλονται πλέον σε επεξεργασία σε συσκευή του χρήστη, αλλά καθίστανται διαθέσιμα σε υποδομές υπολογιστικού νέφους[8], δημιουργώντας δυσκολίες στην πρόσβαση των διωκτικών αρχών άλλων κρατών σε αυτά. Ως εκ τούτου, σε έναν συνεχώς αυξανόμενο αριθμό ποινικών υποθέσεων που αφορούν κάθε είδος εγκλήματος, οι Αρχές επιβολής του Νόμου χρειάζονται πρόσβαση σε δεδομένα που θα μπορούσαν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία και αποθηκεύονται εκτός της χώρας τους ή από παρόχους υπηρεσιών σε άλλα κράτη μέλη ή τρίτες χώρες.

Επιπρόσθετα, βασικό χαρακτηριστικό των ηλεκτρονικών αποδεικτικών μέσων, που τα διαφοροποιεί από τα "παραδοσιακά" αποδεικτικά μέσα, είναι ο ιδιαίτερα ευμετάβλητος χαρακτήρας τους. Τα αποθηκευμένα ηλεκτρονικά αποδεικτικά μέσα δύναται να μεταφέρονται με μεγάλη ταχύτητα από ένα κράτος σε άλλο, ακόμη και από ήπειρο σε ήπειρο, να τροποποιούνται

---

[4] Βλ. για την διάκριση ανάμεσα σε γνήσια (stricto-sensu) και μη γνήσια Κυβερνοεγκλήματα, καθώς και παραδείγματα τέτοιων εγκλημάτων, μεταξύ άλλων και Εγκύκλιο ΕισΑΠ 2/22-5-2019, ΠοινΔικ 5/2019, σελ. 644

[5] Α. Καργόπουλος, Ανακριτικές πράξεις επί ψηφιακών δεδομένων: δικαιικοί άξονες και προβληματισμοί, σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, εκδ. Νομική Βιβλιοθήκη, 2019, σελ. 212

[6] Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, Το ευρωπαϊκό θεματολόγιο για την ασφάλεια, COM(2015) 185 final

[7] Αιτιολογική Έκθεση, ο.π.

[8] Αιτιολογική Σκέψη (17) της Πρότασης Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις, COM(2018) 225 final

με μεγάλη ευκολία ή και να διαγράφονται. Έτσι, απαιτούνται ταχύτατες διαδικασίες για την απόκτησή τους.

Οι παραπάνω δυσκολίες κατά τη διασυνοριακή πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία δεν επιτρέπουν μέχρι και σήμερα την αποτελεσματική έρευνα και δίωξη του εγκλήματος. Υπάρχει έλλειψη αποτελεσματικότητας όσον αφορά τη δικαστική συνεργασία μεταξύ των δημόσιων αρχών, την άμεση συνεργασία μεταξύ των δημόσιων αρχών και των παρόχων υπηρεσιών και την άμεση πρόσβαση των δημόσιων αρχών σε ηλεκτρονικά αποδεικτικά στοιχεία. Ως εκ τούτου, οι έρευνες αποτελματώνονται, εγκλήματα μένουν ατιμώρητα, τα θύματα προστατεύονται με λιγότερο αποτελεσματικό τρόπο, και οι πολίτες αισθάνονται λιγότερο ασφαλείς[9]. Έτσι, τα μέτρα για τη συλλογή και τη διατήρηση ηλεκτρονικών αποδεικτικών στοιχείων αποκτούν ολοένα και μεγαλύτερη σημασία, ώστε να είναι εφικτές οι ποινικές έρευνες και διώξεις[10].

Σύμφωνα με το άρθρο 1 περ. β' της Σύμβασης για το Έγκλημα στον Κυβερνοχώρο[11] "*δεδομένα υπολογιστών" σημαίνει αναπαράσταση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη για να υποστεί επεξεργασία σε ένα σύστημα υπολογιστή, περιλαμβανομένου και ενός προγράμματος κατάλληλου για να προκαλέσει την εκτέλεση μιας λειτουργίας από ένα σύστημα υπολογιστή*. Περαιτέρω, με τον Ν. 4411/2016 προστέθηκε στο άρθρο 13 του προϊσχύσαντος ΠΚ ο ορισμός των ψηφιακών δεδομένων. Έτσι, *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*. Ο ορισμός αυτός παρέμεινε αυτούσιος και στον νέο ΠΚ.

Ο πιο ολοκληρωμένος ορισμός και η σαφέστερη διάκριση των ηλεκτρονικών αποδεικτικών μέσων –κατά τη γνώμη μου- δίνεται στην Πρόταση Κανονισμού του Ευρωπαϊκού

[9] Περίληψη της Εκτίμησης Επιπτώσεων της Πρότασης Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις και της Πρότασης Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον ορισμό νόμιμων εκπροσώπων με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών, SWD(2018) 119 final

[10] Αιτιολογική Σκέψη (2) της Πρότασης Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις, COM(2018) 225 final

[11] (Cets αριθμ. 185)

Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις. Σύμφωνα με αυτήν, «ηλεκτρονικά αποδεικτικά στοιχεία» είναι *τα αποδεικτικά στοιχεία που είναι αποθηκευμένα σε ηλεκτρονική μορφή από πάροχο υπηρεσιών ή για λογαριασμό του κατά τον χρόνο παραλαβής του πιστοποιητικού εντολής υποβολής ή διατήρησης στοιχείων, τα οποία συνίστανται σε αποθηκευμένα δεδομένα συνδρομητή, δεδομένα πρόσβασης, δεδομένα συναλλαγών και δεδομένα περιεχομένου*. Περαιτέρω, ως «δεδομένα συνδρομητή» ορίζονται *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*. Ως «δεδομένα πρόσβασης», σύμφωνα με την παραπάνω πρόταση, ορίζονται *τα 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. Σ' αυτά συμπεριλαμβάνονται τα μεταδεδομένα ηλεκτρονικών επικοινωνιών, όπως ορίζονται στο άρθρο 4 παράγραφος 3 στοιχείο γ) του [κανονισμού για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες]*. Επίσης, «δεδομένα συναλλαγών» θα πρέπει να θεωρούνται *τα δεδομένα που σχετίζονται με την παροχή μιας υπηρεσίας από πάροχο υπηρεσιών, τα οποία χρησιμεύουν για την παροχή γενικότερου πλαισίου ή πρόσθετων πληροφοριών 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. Σ' αυτά συμπεριλαμβάνονται τα μεταδεδομένα ηλεκτρονικών επικοινωνιών, όπως ορίζονται στο άρθρο 4 παράγραφος 3 στοιχείο γ) του [κανονισμού για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες]. Τέλος, τα «δεδομένα περιεχομένου» είναι *οποιαδήποτε δεδομένα αποθηκεύονται σε ψηφιακή μορφή, όπως κείμενο, φωνή, βίντεο, εικόνες και ήχος, άλλα από δεδομένα συνδρομητή, πρόσβασης ή συναλλαγών.*

iii. Σκοπός της εργασίας

Στην παρούσα εργασία εξετάζεται η δυνατότητα των Ευρωπαϊκών Αρχών να αποκτούν διασυνοριακή πρόσβαση στα ηλεκτρονικά αποδεικτικά μέσα σε ποινικές υποθέσεις και καταγράφονται τα διαθέσιμα "εργαλεία" που έχουν μέχρι σήμερα στα χέρια τους οι Αρχές για τον σκοπό αυτό. Ταυτόχρονα επιχειρείται και μια επισκόπηση των τρεχουσών διεθνών εξελίξεων στο πεδίο των ηλεκτρονικών αποδεικτικών μέσων σε ποινικές υποθέσεις. Ιδιαίτερη έμφαση δίνεται στις Προτάσεις Κανονισμού και Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τα ηλεκτρονικά αποδεικτικά μέσα, οι οποίες πρόκειται να επιφέρουν σημαντικές τομές στο πεδίο αυτό. Πρόκειται για δύο ρηξικέλευθες νομοθετικές προτάσεις, οι οποίες περιέχουν σημαντικές καινοτομίες και οι οποίες παρουσιάζουν ιδιαίτερο θεωρητικό ενδιαφέρον, αλλά την ίδια στιγμή έχουν και μεγάλη πρακτική σημασία, καθώς αναμένεται να αποτελέσουν ιδιαίτερα χρήσιμα «εργαλεία» στα χέρια όσων εμπλέκονται με την ανίχνευση, διερεύνηση και δίωξη των ποινικών αδικημάτων, που τελούνται -εν όλω ή εν μέρει- στον ψηφιακό κόσμο ή με τη βοήθεια των νέων τεχνολογιών.

iv. Διάρθρωση της εργασίας

Η παρούσα εργασία διαρθρώνεται σε δύο κύρια μέρη. Στο πρώτο μέρος εξετάζονται οι δυνατότητες που υπάρχουν σήμερα για τις διωκτικές Αρχές, προκειμένου να αποκτήσουν πρόσβαση στα ηλεκτρονικά αποδεικτικά μέσα. Ειδικότερα, στο πρώτο κεφάλαιο του πρώτου μέρους παρουσιάζονται οι διατάξεις διεθνούς δικαστικής συνεργασίας της Σύμβασης για το Έγκλημα στον Κυβερνοχώρο, η οποία περιέχει ειδικές διατάξεις για τα ηλεκτρονικά αποδεικτικά μέσα. Στο δεύτερο κεφάλαιο του πρώτου μέρους γίνεται λόγος για τον σύγχρονο Ευρωπαϊκό θεσμό δικαστικής συνεργασίας της Ευρωπαϊκής Εντολής Έρευνας, ο οποίος εισήχθη στην

Ευρωπαϊκή έννομη τάξη με την Οδηγία 2014/41/ΕΕ και προσέδωσε μια νέα διάσταση στη διασυνοριακή συνεργασία των Αρχών των Κρατών-Μελών της ΕΕ για τη συγκέντρωση αποδεικτικών μέσων, τόσο σε ποινικές όσο και σε σχετικές διοικητικές υποθέσεις. Ωστόσο, αυτή δεν περιέχει ειδικές διατάξεις για τα ηλεκτρονικά αποδεικτικά μέσα. Αφού ασκηθεί κριτική για την ανεπάρκειά της στον τομέα των ηλεκτρονικών αποδεικτικών μέσων σε ποινικές υποθέσεις, αναδεικνύεται αυτόθροη η ανάγκη για τη θέσπιση ειδικού νομοθετικού πλαισίου για τα ηλεκτρονικά αποδεικτικά. Στο τρίτο κεφάλαιο του πρώτου μέρους γίνεται αναφορά στην Συμφωνία Αμοιβαίας Δικαστικής Συνδρομής του 2003 μεταξύ ΕΕ και ΗΠΑ, συμφωνία που αποτελεί μέχρι σήμερα τον κύριο δίαυλο δικαστικής συνεργασίας των Ευρωπαϊκών αρχών με τις αντίστοιχες Αρχές των ΗΠΑ. Όμως, η καθυστέρηση, την οποία συνεπάγονται οι θεσμοί «παραδοσιακής» αμοιβαίας δικαστικής συνδρομής, είναι ασύμβατη με τον ευμετάβλητο χαρακτήρα των ηλεκτρονικών αποδεικτικών μέσων. Έτσι, σήμερα έχει επικρατήσει ως βασικότερη οδός συνεργασίας στο πεδίο των ηλεκτρονικών αποδεικτικών μέσων, τα οποία διατηρούνται από Παρόχους Υπηρεσιών, που εδρεύουν στις ΗΠΑ, η απευθείας συνεργασία των Ευρωπαϊκών Αρχών με τους Παρόχους αυτούς. Η τελευταία αυτή οδός συνεργασίας αναλύεται στο τέταρτο και τελευταίο κεφάλαιο του πρώτου μέρους.

Στο δεύτερο μέρος της εργασίας γίνεται μια επισκόπηση των διεθνών νομοθετικών εξελίξεων στον τομέα των ηλεκτρονικών αποδεικτικών μέσων και παρουσιάζονται οι θεσμοί δικαστικής συνεργασίας του -όχι και τόσο μακρινού- μέλλοντος. Στο πρώτο κεφάλαιο του δευτέρου μέρους δίνεται ιδιαίτερη έμφαση στις Προτάσεις Κανονισμού και Οδηγίας για τα ηλεκτρονικά αποδεικτικά μέσα σε ποινικές υποθέσεις. Οι Προτάσεις αυτές, που επί του παρόντος βρίσκονται στο στάδιο της πρώτης ανάγνωσης από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, σύμφωνα με τη συνήθη νομοθετική διαδικασία, πρόκειται να αποτελέσουν ένα σύγχρονο νομοθετικό πλαίσιο δικαστικής συνεργασίας ειδικά για τα ηλεκτρονικά αποδεικτικά μέσα, προσαρμοσμένο στην ψηφιακή εποχή. Στο δεύτερο κεφάλαιο του δευτέρου μέρους γίνεται λόγος για τη Συμφωνία Αμοιβαίας Δικαστικής Συνδρομής μεταξύ ΕΕ και ΗΠΑ στον τομέα των ηλεκτρονικών αποδεικτικών μέσων. Η υπόθεση *States v. Microsoft Corp.* πυροδότησε εξελίξεις στον τομέα των ηλεκτρονικών αποδεικτικών μέσων στις ΗΠΑ. Αποτέλεσμα των εξελίξεων αυτών ήταν η έκδοση από το Κογκρέσο των Ηνωμένων Πολιτειών της Αμερικής του Νόμου Clarifying Lawful Use of Overseas Data (CLOUD) Act, για την αποσαφήνιση της νόμιμης χρήσης δεδομένων στο εξωτερικό. Μεταξύ των άλλων ο Νόμος αυτός εξουσιοδοτεί την

εκτελεστική εξουσία των ΗΠΑ να συνάπτει συμφωνίες με ξένες κυβερνήσεις, σύμφωνα με τις οποίες οι ξένες κυβερνήσεις μπορούν να αποκτήσουν ταχεία πρόσβαση στα δεδομένα, που διατηρούνται εντός της επικράτειας των ΗΠΑ. Έτσι, άνοιξε ο δρόμος για την έναρξη των διαπραγματεύσεων μεταξύ ΗΠΑ και ΕΕ για την υπογραφή Σύμβασης Αμοιβαίας Δικαστικής Συνδρομής ειδικά στον τομέα των ηλεκτρονικών αποδεικτικών μέσων σε ποινικές υποθέσεις. Τέλος, σε παγκόσμιο επίπεδο, λαμβάνουν χώρα διαπραγματεύσεις για το Δεύτερο Πρόσθετο Πρωτόκολλο της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο. Οι εξελίξεις αυτές αναπτύσσονται στο τρίτο και τελευταίο κεφάλαιο του δευτέρου μέρους της παρούσας εργασίας.

ΜΕΡΟΣ ΠΡΩΤΟ

Η ΔΙΚΑΣΤΙΚΗ ΣΥΝΕΡΓΑΣΙΑ ΕΠΙ ΤΟΥ ΠΑΡΟΝΤΟΣ

Α. Η Σύμβαση της Βουδαπέστης για το Έγκλημα στον Κυβερνοχώρο

Εισαγωγικά

Οι εργασίες για την δημιουργία μιας Σύμβασης για τον Κυβερνοχώρο ξεκίνησαν το 1997, όταν συστήθηκε επιτροπή ειδικών στον τομέα του ηλεκτρονικού εγκλήματος, με σκοπό να εξετάσει τα νομοθετικά προβλήματα που προκύπτουν από την εγκληματική δραστηριότητα, που αναπτύσσεται και συνεχώς διευρύνεται στον Κυβερνοχώρο[12]. Αν και αρχικά η περαίωση των εργασιών της επιτροπής είχε προσδιοριστεί για το έτος 1999, ωστόσο λόγω των ιδιαίτερων προβλημάτων (η εξέλιξη της τεχνολογίας και η παρουσίαση νέων μορφών συμπεριφορών, που θα μπορούσαν να θεωρηθούν αξιόποινες, "έτρεχαν" ταχύτερα από τις εργασίες της Συμβάσεως) οι εργασίες ολοκληρώθηκαν την άνοιξη του 2001[13]. Τελικά, το κείμενο της Σύμβασης για το Έγκλημα στον Κυβερνοχώρο υπογράφηκε στις 23 Νοεμβρίου 2001 στη Βουδαπέστη από τα περισσότερα μέλη του Ευρωπαϊκού Συμβουλίου και από τις ΗΠΑ, τον Καναδά, την Νότια Αφρική και την Ιαπωνία. Στη συνέχεια, στη Σύμβαση εισχώρησαν και άλλες χώρες, ενώ μέχρι και σήμερα συνεχώς προστίθενται και άλλες. Επί του παρόντος, τα συμβαλλόμενα μέρη της Σύμβασης ανέρχονται σε 62, συμπεριλαμβανομένων 26 Κρατών-Μελών της ΕΕ[14].

Η Σύμβαση συνοδεύεται από την Επεξηγηματική της Έκθεση[15], ένα κείμενο ιδιαίτερα διαφωτιστικό και "προφητικό". Εξαίρει την αξία της Πληροφορίας και των Τεχνολογιών Πληροφορικής και Επικοινωνίας, αναγνωρίζει τη σημασία που αυτές θα διαδραματίσουν στο

[12] Κ. Βλαχόπουλος, Ηλεκτρονικό Έγκλημα, 2007, εκδ. Νομική Βιβλιοθήκη, σελ. 136

[13] Ι. Αγγελής, Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convenction on Cyber-crime), ΠοινΔικ 12/2001, σελ. 1218

[14] Βλ. Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), 5.2.2019, COM(2019) 71 final, σελ.1

[15] Explanatory Report to the Convention on Cybercrime

μέλλον, ενώ ταυτόχρονα αναδεικνύει τα προβλήματα που δημιουργούνται από τα νέα δεδομένα και τονίζει την επιτακτική ανάγκη νομοθετικής ρύθμισης του νεοεμφανιζόμενου χώρου που αποκαλεί "Κυβερνοχώρο"[16]. Τόσο η Σύμβαση της Βουδαπέστης, όσο και η Επεξηγηματική της Έκθεση αποτελούν πρωτοποριακά για την εποχή εκείνη κείμενα με διαχρονική αξία, τα οποία βρίσκουν εφαρμογή ακόμη και σήμερα. Η Σύμβαση έχει ως στόχο την εναρμόνιση των εθνικών νομοθεσιών, σχετικά με το ηλεκτρονικό έγκλημα και την παροχή νομοθετικού πλαισίου στον τομέα του δικονομικού δικαίου για την διερεύνηση και δίωξη εγκλημάτων, που σχετίζονται με τον Κυβερνοχώρο[17]. Επιχειρεί, επίσης, να θέσει τις βάσεις για άμεση και αποτελεσματική διεθνή συνεργασία για τα ηλεκτρονικά εγκλήματα[18]. Έτσι, στο Κεφάλαιο Ι παρατίθενται οι αναγκαίοι ορισμοί, στο Πρώτο Τμήμα του Κεφαλαίου ΙΙ προβλέπονται οι διατάξεις του ουσιαστικού ποινικού δικαίου, ενώ Δεύτερο Τμήμα του δικονομικού δικαίου. Περαιτέρω, στο Κεφάλαιο ΙΙΙ της Σύμβασης προβλέπονται διατάξεις για την διεθνή συνεργασία και την αμοιβαία συνδρομή.

Ι. Οι θεσμοί διεθνούς συνεργασίας της Σύμβασης της Βουδαπέστης για το Έγκλημα στον Κυβερνοχώρο

i. Κατεπείγουσα διατήρηση αποθηκευμένων δεδομένων υπολογιστών

Στο άρθρο 29 της Σύμβασης καθιερώνεται ένας μηχανισμός, ο οποίος καθιστά διαθέσιμα σε διασυνοριακό επίπεδο τα μέτρα που δύναται να λαμβάνονται σε εθνικό επίπεδο, δυνάμει του άρθρου 16 της Σύμβασης, για τη διατήρηση των αποθηκευμένων δεδομένων υπολογιστή. Έτσι, κάθε Συμβαλλόμενο Μέρος μπορεί να ζητήσει από ένα άλλο Συμβαλλόμενο Μέρος να διατάξει ή με άλλο τρόπο εξασφαλίσει την κατεπείγουσα διατήρηση δεδομένων που είναι αποθηκευμένα σε ένα σύστημα υπολογιστή, το οποίο βρίσκεται στην επικράτεια του άλλου Συμβαλλόμενου Μέρους, για τα οποία το αιτούν Συμβαλλόμενο Μέρος προτίθεται να υποβάλει αίτηση αμοιβαίας συνδρομής με σκοπό την έρευνα ή με παρόμοιο τρόπο πρόσβαση, κατάσχεση, εξασφάλιση ή αποκάλυψη των δεδομένων.

[16] Σύμφωνα με τον Θέοδωρο Ν. Κριθαρά, Ποινικό δίκαιο και διαδίκτυο, 2009, σελ. 1 υποσημ. 3 ο όρος "Κυβερνοχώρος" απαντάται για πρώτη φορά στο μυθιστόρημα επιστημονικής φαντασίας του Wlliam Gibson, Neuromancer (Νευρομάντης) (1984) και χρησιμοποιείται, πλέον, προκειμένου να προσδιορίσει τον "χώρο" Διαδικτύου, και γενικότερα, των προηγμένων τηλεπικοινωνιακών συστημάτων.

[17] Κ. Βλαχόπουλος, ο.π., σελ. 137

[18] Κ. Βλαχόπουλος, ο.π.

Η διατήρηση των αποθηκευμένων δεδομένων υπολογιστή είναι ένα περιορισμένο, προσωρινό μέτρο, προορισμένο να εκτελείται ταχύτερα από ότι άλλα μέσα "παραδοσιακής" αμοιβαίας συνδρομής. Ο λόγος που κατέστησε αναγκαία τέτοιου είδους ταχύτερα μέτρα είναι ο ευμετάβλητος χαρακτήρας των δεδομένων υπολογιστή, τα οποία με το πάτημα μερικών πλήκτρων ή με τη λειτουργία αυτόματων προγραμμάτων, είναι δυνατό να διαγραφούν, να μεταβληθούν ή να μετακινηθούν, καθιστώντας αδύνατο τον εντοπισμό του δράστη ενός εγκλήματος ή την καταστροφή κρίσιμων στοιχείων για την απόδειξη της ενοχής του[19]. Συνεπώς, τα Συμβαλλόμενα Μέρη συμφώνησαν ότι απαιτείται ένας μηχανισμός για να εξασφαλιστεί η διαθεσιμότητα αυτών των δεδομένων εν όψει της επικείμενης, περισσότερο χρονοβόρας και πιο περίπλοκης διαδικασίας εκτέλεσης μιας "παραδοσιακής" αίτησης αμοιβαίας δικαστικής συνδρομής, η οποία μπορεί να απαιτήσει εβδομάδες ή μήνες για να εκτελεστεί[20]. Αν και ταχύτερο από άλλους θεσμούς "παραδοσιακής" αμοιβαίας δικαστικής συνδρομής, το μέτρο της διατήρησης αποθηκευμένων δεδομένων υπολογιστών δεν συνεπάγεται και μεγαλύτερη παρέμβαση στο δικαίωμα προστασίας της ιδιωτικής ζωής των Υποκειμένων, καθώς δεν απαιτεί την υποβολή ή γνωστοποίηση των δεδομένων υπολογιστή, παρά μόνο την διατήρησή τους από κάποιον τρίτο, ο οποίος τα έχει ήδη στη διάθεσή του, με σκοπό την μετέπειτα απόκτησή τους. Αυτή η διαδικασία λοιπόν έχει το πλεονέκτημα ότι είναι ταχύτατη, αλλά ταυτόχρονα προστατευτική για την ιδιωτικότητα του Υποκειμένου των δεδομένων.

Προκειμένου να δοθεί επαρκής χρόνος στο αιτούν Συμβαλλόμενο Μέρος, ώστε να υποβάλει στη συνέχεια αίτηση για την έρευνα ή με παρόμοιο τρόπο πρόσβαση, κατάσχεση ή με παρόμοιο τρόπο εξασφάλιση ή αποκάλυψη των δεδομένων, η διατήρηση θα πρέπει να γίνεται για χρονικό διάστημα τουλάχιστον εξήντα ημερών. Μετά τη λήψη μιας τέτοιας επακόλουθης αίτησης, τα δεδομένα θα συνεχίσουν να διατηρούνται μέχρι να εκδοθεί απόφαση επί της αίτησης αυτής[21].

Κάθε αίτηση διατήρησης αποθηκευμένων δεδομένων υπολογιστών θα πρέπει να αναφέρει[22] την αρχή που ζητεί την διατήρηση, το έγκλημα που αποτελεί το αντικείμενο της ποινικής έρευνας ή δίωξης και συνοπτική περιγραφή των συναφών πραγματικών περιστατικών,

[19] Βλ. Explanatory Report to the Convention on Cybercrime, σελ. 50
[20] Βλ. ο.π.
[21] Βλ. Άρθρο 29 παρ. 7
[22] Βλ. Άρθρο 29 παρ. 2

τα προς διατήρηση αποθηκευμένα δεδομένα υπολογιστή και την σχέση τους με το έγκλημα, κάθε διαθέσιμη πληροφορία που ταυτοποιεί τον κατέχοντα τα αποθηκευμένα δεδομένα υπολογιστή ή τη θέση του συστήματος υπολογιστή, την αναγκαιότητα της διατήρησης και ότι το Συμβαλλόμενο Μέρος προτίθεται να υποβάλει αίτηση αμοιβαίας δικαστικής συνδρομής για την έρευνα ή με παρόμοιο τρόπο πρόσβαση, κατάσχεση, εξασφάλιση ή αποκάλυψη των αποθηκευμένων δεδομένων υπολογιστή. Με την λήψη της αίτησης από Συμβαλλόμενο Μέρος, το Συμβαλλόμενο Μέρος, προς το οποίο απευθύνεται η αίτηση, θα πρέπει να λάβει όλα τα αναγκαία μέτρα για την κατεπείγουσα διατήρηση των συγκεκριμένων δεδομένων, σύμφωνα με το εσωτερικό του δίκαιο[23].

Για τη διατήρηση δεδομένων που είναι αποθηκευμένα σε ένα σύστημα υπολογιστή δεν έχει ισχύ η αρχή του διττού αξιοποίνου, όταν η αίτηση αφορά σε αδικήματα που προβλέπονται στα άρθρα 2 έως 11 της Σύμβασης. Ωστόσο, τα Συμβαλλόμενα Μέρη που έχουν θέσει ως προϋπόθεση την ύπαρξη διπλού αξιοποίνου για την ανταπόκριση σε μία αίτηση για αμοιβαία συνδρομή με σκοπό την έρευνα ή τη με ανάλογο τρόπο πρόσβαση, κατάσχεση ή την με ανάλογο τρόπο εξασφάλιση ή γνωστοποίηση των αποθηκευμένων δεδομένων υπολογιστή, μπορούν για τα υπόλοιπα εγκλήματα να διατηρήσουν το δικαίωμα να αρνηθούν την ανταπόκριση στην αίτηση για διατήρηση, στις περιπτώσεις που κατά την στιγμή της γνωστοποίησης των δεδομένων δεν μπορεί να εκπληρωθεί η προϋπόθεση του διπλού αξιοποίνου[24]. Σύμφωνα με το άρθρο έβδομο παράγραφος 2 του ν. 4411/2016, η Ελληνική Δημοκρατία διατηρεί το δικαίωμα άρνησης ικανοποίησης αιτήματος δικαστικής συνδρομής, δυνάμει του παραπάνω άρθρου, σε περιπτώσεις έλλειψης του όρου του διττού αξιοποίνου.

Το Συμβαλλόμενο Μέρος που δέχεται την αίτηση μπορεί, να αρνηθεί τη διατήρηση, μόνον εάν η αίτηση αφορά έγκλημα το οποίο χαρακτηρίζεται από αυτό ως πολιτικό έγκλημα ή έγκλημα που σχετίζεται με πολιτικό έγκλημα ή αν θεωρεί ότι η αποδοχή της αίτησης είναι πιθανόν να θίξει την κυριαρχία, την ασφάλεια, την δημόσια τάξη ή άλλα θεμελιώδη συμφέροντά του[25].

[23] Βλ. Άρθρο 29 παρ. 3
[24] Βλ. Άρθρο 29 παρ. 4
[25] Βλ. άρθρο 29 παρ. 5

ii. Κατεπείγουσα γνωστοποίηση διατηρηθέντων δεδομένων κίνησης

Με το άρθρο 30 της Σύμβασης καθίστανται διαθέσιμα σε διασυνοριακό επίπεδο τα μέτρα που δύναται να λαμβάνονται σε εθνικό επίπεδο, δυνάμει του άρθρου 17 της Σύμβασης. Ένα Συμβαλλόμενο Μέρος δύναται να ζητά από το Συμβαλλόμενο Μέρος, προς το οποίο απευθύνεται η αίτηση, δεδομένα κίνησης, τα οποία αναμένεται να οδηγήσουν στην ταυτοποίηση του δράστη ενός εγκλήματος. Όμως, συμβαίνει συχνά στην πράξη, όταν η επικοινωνία λαμβάνει χώρα μέσω του Διαδικτύου και λόγω του διεθνούς χαρακτήρα του, τα δεδομένα υπολογιστή να «ταξιδεύουν» μέσα από υπολογιστές παρόχων υπηρεσιών, οι οποίοι βρίσκονται σε τρίτα κράτη, εκτός της επικράτειας του Συμβαλλόμενου Μέρους, προς το οποίο απευθύνεται η αίτηση διατήρησης. Στις περιπτώσεις αυτές, όταν υποβάλλεται αίτημα, σύμφωνα με το άρθρο 29 της Σύμβασης, για διατήρηση δεδομένων κίνησης, που αφορούν σε μια συγκεκριμένη επικοινωνία, και το Συμβαλλόμενο Μέρος, προς το οποίο απευθύνεται η αίτηση, διαπιστώσει ότι ένας πάροχος υπηρεσιών σε άλλο Κράτος αναμίχθηκε στη διαβίβαση της επικοινωνίας, προκειμένου να εξασφαλισθεί ότι η κατεπείγουσα διατήρηση των στοιχείων κίνησης θα είναι διαθέσιμη ανεξαρτήτως της συμμετοχής ενός ή περισσοτέρων παρόχων υπηρεσιών στη διαβίβαση αυτών των επικοινωνιών, το Συμβαλλόμενο αυτό Μέρος, θα πρέπει ταυτόχρονα με τη διατήρηση των δεδομένων υπολογιστή, να γνωστοποιήσει κατεπειγόντως στο αιτούν Συμβαλλόμενο Μέρος επαρκή ποσότητα δεδομένων κίνησης, για να ταυτοποιηθεί ο εν λόγω πάροχος υπηρεσιών και η διαδρομή, μέσω της οποίας διαβιβάσθηκε η επικοινωνία αυτή. Η γνωστοποίηση των δεδομένων κίνησης μπορεί να απορριφθεί, εάν η αίτηση αφορά έγκλημα, το οποίο χαρακτηρίζεται από το Συμβαλλόμενο Κράτος, προς το οποίο απευθύνεται η αίτηση, ως πολιτικό έγκλημα ή έγκλημα που σχετίζεται με πολιτικό έγκλημα ή αν θεωρεί ότι η αποδοχή της αίτησης είναι πιθανόν να θίξει την κυριαρχία, την ασφάλεια, την δημόσια τάξη ή άλλα θεμελιώδη συμφέροντά του[26].

iii. Αμοιβαία συνδρομή σχετικά με την πρόσβαση σε αποθηκευμένα δεδομένα υπολογιστή

Σύμφωνα με το άρθρο 31 της Σύμβασης, κάθε Συμβαλλόμενο Μέρος μπορεί να ζητήσει από άλλο Συμβαλλόμενο Μέρος να ερευνήσει ή με παρόμοιο τρόπο αποκτήσει πρόσβαση, κατάσχει ή με παρόμοιο τρόπο εξασφαλίσει ή αποκαλύψει δεδομένα που είναι αποθηκευμένα σε ένα σύστημα υπολογιστή που βρίσκεται στην επικράτεια του Συμβαλλόμενου Μέρους, προς το

[26] Βλ. Άρθρο 30 παρ. 2

οποίο απευθύνεται η αίτηση, περιλαμβανόμενων των δεδομένων που έχουν διατηρηθεί κατ' εφαρμογή του άρθρου 29. Επιπλέον, το αίτημα θα αντιμετωπίζεται σε κατεπείγουσα βάση όταν λογίζεται βάσιμα ότι τα σχετικά δεδομένα είναι ιδιαίτερα ευάλωτα σε απώλεια ή τροποποίηση, ή όταν προβλέπεται κατεπείγουσα συνεργασία βάσει σχετικών διεθνών συμφωνιών διεθνούς συνεργασίας σε ποινικά θέματα, των ρυθμίσεων που έχουν γίνει με βάση την ενιαία ή αμοιβαία νομοθεσία και τους εσωτερικούς νόμους και σύμφωνα με τις λοιπές σχετικές διατάξεις του σχετικού με τη Διεθνή Συνεργασία Κεφαλαίου ΙΙΙ της Σύμβασης[27].

Ένα ζήτημα που συζητήθηκε εκτενώς από τους συντάκτες της Σύμβασης είναι το κατά πόσο θα πρέπει να επιτρέπεται σε ένα Συμβαλλόμενο Μέρος να αποκτά μονομερώς πρόσβαση σε δεδομένα ηλεκτρονικού υπολογιστή αποθηκευμένα σε άλλο Συμβαλλόμενο Μέρος, χωρίς να υποβάλει αίτημα αμοιβαίας συνδρομής[28]. Τελικά, ελλείψει επαρκούς σχετικής εμπειρίας, οι συντάκτες αποφάσισαν να συμπεριλάβουν στο άρθρο 32 της Σύμβασης μόνο καταστάσεις, στις οποίες ομόφωνα συμφώνησαν ότι η μονομερής ενέργεια είναι επιτρεπτή. Συγκεκριμένα, κάθε Συμβαλλόμενο Μέρος μπορεί, χωρίς την εξουσιοδότηση του άλλου Συμβαλλόμενου Μέρους, να έχει πρόσβαση σε αποθηκευμένα δεδομένα υπολογιστή που είναι διαθέσιμα στο κοινό (ανοικτή πηγή), ασχέτως της γεωγραφικής θέσης των δεδομένων, ή να αποκτήσει πρόσβαση ή να λάβει, μέσω ενός συστήματος υπολογιστή στην επικράτειά του, δεδομένα υπολογιστή που είναι αποθηκευμένα σε άλλο Συμβαλλόμενο Μέρος, εάν το Συμβαλλόμενο Μέρος λάβει την νόμιμη και οικειοθελή συναίνεση του προσώπου που έχει την νόμιμη εξουσία να γνωστοποιεί τα δεδομένα στο Συμβαλλόμενο Μέρος, μέσω του συστήματος υπολογιστή του. Για παράδειγμα, τα μηνύματα ηλεκτρονικού ταχυδρομείου ενός ατόμου μπορεί να αποθηκεύονται από έναν πάροχο υπηρεσιών σε άλλο Συμβαλλόμενο Μέρος ή ένα άτομο μπορεί σκόπιμα να αποθηκεύει δεδομένα σε άλλο Συμβαλλόμενο Μέρος. Στις περιπτώσεις αυτές, οι πάροχοι υπηρεσιών μπορούν να ανακτήσουν τα δεδομένα και, υπό την προϋπόθεση ότι έχουν τη νόμιμη εξουσία, μπορούν να αποκαλύψουν οικειοθελώς τα δεδομένα στις Αρχές επιβολής του Νόμου ή να τους επιτρέψουν να έχουν πρόσβαση σε αυτά, όπως προβλέπεται στο άρθρο 32[29]. Η τελευταία αυτή διάταξη θεωρείται ότι παρέχει νόμιμη βάση για αιτήσεις μη υποχρεωτικής (προαιρετικής) υποβολής αποθηκευμένων δεδομένων υπολογιστή προς αλλοδαπούς παρόχους υπηρεσιών, που είναι

[27] Βλ. άρθρο 31 παρ. 3 σε συνδυασμό με παρ. 2 και άρθρο 23
[28] Βλ. Explanatory Report to the Convention on Cybercrime, σελ. 53
[29] Βλ. ο.π

εγκατεστημένοι σε άλλο Συμβαλλόμενο Μέρος[30]. Ωστόσο, σύμφωνα με την Επιτροπή της Σύμβασης για το Κυβερνοέγκλημα, οι πάροχοι υπηρεσιών δε φαίνεται να έχουν τη νόμιμη εξουσία, ώστε να υποβάλουν δεδομένα των χρηστών τους, καθώς αυτοί μόνο διατηρούν τα δεδομένα αυτά, τα οποία όμως δεν τους ανήκουν[31]. Τέλος, αξίζει να σημειωθεί ότι το πεδίο εφαρμογής της παραπάνω διάταξης καλύπτει μόνο τις περιπτώσεις που τα δεδομένα υπολογιστή είναι αποθηκευμένα σε άλλο Συμβαλλόμενο Μέρος και κατά συνέπεια, όταν τα δεδομένα υπολογιστή βρίσκονται σε τρίτο, μη συμβαλλόμενο κράτος δεν μπορεί να εφαρμοστεί το παραπάνω μέτρο.

iv. Δικαστική συνδρομή για την συλλογή δεδομένων κίνησης σε πραγματικό χρόνο

Σε πολλές περιπτώσεις, οι ερευνητές δεν είναι σε θέση να ανιχνεύσουν μια επικοινωνία στην πηγή της ακολουθώντας το ίχνος μέσω αρχείων ιστορικού προηγούμενων μεταδόσεων, επειδή βασικά δεδομένα κίνησης ενδέχεται να έχουν διαγραφεί αυτόματα από έναν πάροχο υπηρεσιών, πριν καν προλάβουν οι Αρχές να ζητήσουν τη διατήρησή τους. Ως εκ τούτου, είναι κρίσιμο για τους ερευνητές σε κάθε Συμβαλλόμενο Μέρος να έχουν τη δυνατότητα να λαμβάνουν δεδομένα κίνησης σε πραγματικό χρόνο, σχετικά με τις επικοινωνίες που διέρχονται από ένα σύστημα ηλεκτρονικών υπολογιστών σε άλλα κράτη[32]. Με βάση το άρθρο 33 της Σύμβασης τα Συμβαλλόμενα Μέρη αναλαμβάνουν την υποχρέωση να παρέχουν αμοιβαία συνδρομή για τη συλλογή σε πραγματικό χρόνο δεδομένων κίνησης σχετικά με συγκεκριμένες επικοινωνίες στην επικράτειά τους, που διαβιβάζονται μέσω ενός συστήματος υπολογιστή. Η συνδρομή θα πρέπει να παρέχεται τουλάχιστον για τα αδικήματα, για τα οποία επιτρέπεται η συλλογή δεδομένων κίνησης σε πραγματικό χρόνο σε παρόμοιες υποθέσεις, σύμφωνα με το εσωτερικό δίκαιο του Συμβαλλόμενου Κράτους, προς το οποίο απευθύνεται η αίτηση, και σύμφωνα με τους όρους και τις διαδικασίες που προβλέπονται από το εσωτερικό δίκαιο αυτού.

[30] B.J. Koops and M. Goodwin, "Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities International Law", in Tilburg Law School Research Paper No. 5/2016, 2014, σελ. 63

[31] Cybercrime Convention Committee (T-CY), T-CY Guidance Note # 3, Transborder access to data (Article 32), adopted by the 12th Plenary of the T-CY on 2–3 December 2014, T-CY (2013)7 E, σελ. 7 (3.6.)

[32] Βλ. Explanatory Report to the Convention on Cybercrime, σελ. 53

ν. Αμοιβαία συνδρομή σχετικά με την άρση απορρήτου δεδομένων περιεχομένου

Στο άρθρο 34 της Σύμβασης προβλέπεται ότι τα Συμβαλλόμενα Μέρη θα παρέχουν αμοιβαία συνδρομή για την συλλογή ή καταγραφή σε πραγματικό χρόνο δεδομένων περιεχομένου σχετικά με συγκεκριμένες επικοινωνίες στην επικράτειά τους, που διαβιβάζονται μέσω ενός συστήματος υπολογιστή, στον βαθμό που επιτρέπεται από τις ισχύουσες συμβάσεις και το εσωτερικό τους δίκαιο. Λόγω του υψηλού βαθμού παρεμβατικότητας της άρσης του απορρήτου δεδομένων περιεχομένου, η υποχρέωση παροχής αμοιβαίας συνδρομής για την παρακολούθηση δεδομένων περιεχομένου περιορίζεται. Η βοήθεια πρέπει να παρέχεται στο βαθμό που επιτρέπεται από τις ισχύουσες συνθήκες και τους νόμους των Συμβαλλομένων Μερών.

ΙΙ. Το Δίκτυο 24/7

Σύμφωνα με το άρθρο 35 της Σύμβασης κάθε Συμβαλλόμενο Μέρος ορίζει ένα σημείο επαφής, το οποίο θα είναι διαθέσιμο σε εικοσιτετράωρη βάση, επτά ημέρες την εβδομάδα, έτσι ώστε να διασφαλίζεται η παροχή άμεσης συνδρομής σε περιπτώσεις έρευνας ή δίωξης αναφορικά με ποινικά αδικήματα σχετιζόμενα με συστήματα και δεδομένα υπολογιστή, ή με σκοπό την συλλογή των αποδεικτικών στοιχείων σε ηλεκτρονική μορφή για ένα ποινικό αδίκημα. Η εν λόγω συνδρομή θα περιλαμβάνει την διευκόλυνση ή, εάν αυτό επιτρέπεται από το εσωτερικό δίκαιο και την πρακτική, την άμεση εφαρμογή των ακόλουθων μέτρων: την παροχή τεχνικών συμβουλών, τη διατήρηση των δεδομένων, σύμφωνα με τα άρθρα 29 και 30, τη συλλογή αποδεικτικών στοιχείων, παροχή νομικής ενημέρωσης και τον εντοπισμό των υπόπτων.

Επιπλέον, το σημείο επαφής κάθε Συμβαλλόμενου Μέρους είναι αρμόδιο να επικοινωνεί σε κατεπείγουσα βάση με το σημείο επαφής ενός άλλου Συμβαλλόμενου Μέρους. Εάν το σημείο επαφής που ορίστηκε από ένα Συμβαλλόμενο Μέρος δεν υπάγεται στην αρχή του Συμβαλλόμενου αυτού Μέρους, η οποία είναι αρμόδια για την παροχή αμοιβαίας συνδρομής, το σημείο επαφής διασφαλίζει ότι είναι σε θέση να συντονίζεται με την αρχή αυτή σε κατεπείγουσα βάση. Τέλος, κάθε Συμβαλλόμενο Μέρος εξασφαλίζει την ύπαρξη διαθέσιμου εκπαιδευμένου και καταρτισμένου προσωπικού για την διευκόλυνση της λειτουργίας του δικτύου. Σύμφωνα με

το άρθρο έκτο του ν. 4411/2016[33], η Ελληνική Δημοκρατία ορίζει ως σημείο επαφής για την εκπλήρωση των σκοπών του παραπάνω άρθρου της Σύμβασης «Δίκτυο 24/7» τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας υπό την εποπτεία Εισαγγελέα Εφετών.

[33] Νόμος 4411/2016 (ΦΕΚ Α' 142/3-8-2016), Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών - Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις

Β. Η Οδηγία 2014/41/ΕΕ

Εισαγωγικά

Σε αντίθεση με τη Σύμβαση της Βουδαπέστης για το Έγκλημα στον Κυβερνοχώρο, σε επίπεδο Ευρωπαϊκής Ένωσης δεν υπάρχει μέχρι σήμερα νομοθέτημα, το οποίο να περιλαμβάνει συγκεκριμένες διατάξεις για την πρόσβαση σε ηλεκτρονικά αποδεικτικά μέσα. Η Οδηγία 2014/41/ΕΕ[34] περιλαμβάνει ένα και μοναδικό "εργαλείο" για την αναζήτηση αποδεικτικών μέσων γενικά από τις Ευρωπαϊκές αρχές, την Ευρωπαϊκή Εντολή Έρευνας (ΕΕΕ). Η έκδοση μιας ΕΕΕ αποσκοπεί στην εκτέλεση ενός ή περισσότερων συγκεκριμένων ερευνητικών μέτρων στο κράτος εκτέλεσης του ευρωπαϊκού εντάλματος («κράτος εκτέλεσης») με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων. Η ΕΕΕ έχει οριζόντιο πεδίο εφαρμογής και επομένως εφαρμόζεται σε όλα τα ερευνητικά μέτρα που στοχεύουν στη συγκέντρωση αποδεικτικών στοιχείων[35]. Αρμόδια να αποφασίζει ποιό ερευνητικό μέτρο θα πρέπει να χρησιμοποιηθεί κάθε φορά είναι η αρχή έκδοσης, βάσει των στοιχείων που διαθέτει, όσον αφορά τις λεπτομέρειες της σχετικής έρευνας[36].

Η Οδηγία τέθηκε σε ισχύ στις 22 Μαΐου του 2017 και αντικατέστησε την Ευρωπαϊκή Σύμβαση του Συμβουλίου της Ευρώπης της 20ής Απριλίου 1959 περί αμοιβαίας δικαστικής συνδρομής επί ποινικών υποθέσεων και τα δύο πρόσθετα πρωτόκολλά της, καθώς και διμερείς συμφωνίες που έχουν συναφθεί δυνάμει του άρθρου 26 της εν λόγω Σύμβασης, τη Σύμβαση για την εφαρμογή της Συμφωνίας του Σένγκεν και τη Σύμβαση για την αμοιβαία δικαστική συνδρομή επί ποινικών υποθέσεων μεταξύ των Κρατών-Μελών της Ευρωπαϊκής Ένωσης και το Πρωτόκολλό της[37]. Επίσης, αντικατέστησε την Απόφαση-Πλαίσιο 2008/978/ΔΕΥ[38] και τις

[34]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, η οποία ενσωματώθηκε στο ελληνικό δίκαιο με τον ν. 4489/2017 (ΦΕΚ 140/Α/21-9-2017)

[35] Βλ. Αιτιολογική Σκέψη (8), Οδηγία 2014/41/ΕΕ

[36] Βλ. Αιτιολογική Σκέψη (10), ο.π.

[37] Βλ. άρθρο 34, Οδηγία 2014/41/ΕΕ

[38]Απόφαση-Πλαίσιο 2008/978/ΔΕΥ του Συμβουλίου, της 18ης Δεκεμβρίου 2008 , σχετικά με το ευρωπαϊκό ένταλμα συγκέντρωσης αποδεικτικών στοιχείων προς λήψη αντικειμένων, εγγράφων και δεδομένων για χρήση σε ποινικές διαδικασίες

διατάξεις της Απόφασης-Πλαισίου 2003/577/ΔΕΥ[39]. Έτσι, σήμερα η ΕΕΕ αποτελεί το βασικότερο μέσο, το οποίο χρησιμοποιείται από τις αρχές των Κρατών-Μελών της ΕΕ, προκειμένου να αποκτήσουν διασυνοριακή πρόσβαση σε αποδεικτικά μέσα, μεταξύ των οποίων περιλαμβάνονται και τα ηλεκτρονικά αποδεικτικά μέσα, που είναι αποθηκευμένα σε Κράτη-Μέλη της ΕΕ. Βασίζεται στην αρχή της αμοιβαίας αναγνώρισης των δικαστικών αποφάσεων και διαταγών, η οποία θεμελιώνεται στο άρθρο 82 παράγραφος 1 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ) και η οποία συστηματικώς χαρακτηρίζεται, από το Ευρωπαϊκό Συμβούλιο του Τάμπερε της 15ης και 16ης Οκτωβρίου 1999 και έπειτα, ως ακρογωνιαίος λίθος της δικαστικής συνεργασίας επί ποινικών υποθέσεων στην Ένωση.

Ι. Η Ευρωπαϊκή Εντολή Έρευνας

i. Ορισμός

Ως Ευρωπαϊκή Εντολή Έρευνας (ΕΕΕ) ορίζεται δικαστική απόφαση, την οποία εκδίδει ή επικυρώνει δικαστική αρχή Κράτους-Μέλους («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 μπορεί επίσης να εκδίδεται για την λήψη αποδεικτικών στοιχείων ευρισκομένων ήδη στην κατοχή των αρμόδιων αρχών του Κράτους Εκτέλεσης[40]. Την έκδοση ΕΕΕ μπορεί να ζητήσει επίσης ύποπτος ή κατηγορούμενος (ή δικηγόρος εξ ονόματός του) στο πλαίσιο των δικαιωμάτων υπεράσπισης που προβλέπει το εθνικό δίκαιο και η ποινική δικονομία[41].

ii. Προϋποθέσεις Έκδοσης ΕΕΕ

Η ΕΕΕ μπορεί να εκδοθεί σε ποινική διαδικασία που κινείται από δικαστική αρχή ή μπορεί να κινηθεί ενώπιόν της για ποινικό αδίκημα βάσει της νομοθεσίας του Κράτους Έκδοσης. Επίσης, μπορεί να εκδοθεί για διαδικασία που κινούν διοικητικές αρχές, όταν η διαδικασία αφορά πράξεις που τιμωρούνται βάσει της νομοθεσίας του Κράτους Έκδοσης ως παραβάσεις των κανόνων δικαίου και η απόφαση της διοικητικής ή δικαστικής αρχής μπορεί να οδηγήσει σε

[39] 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

[40] Βλ. άρθρο 1 παρ. 1, ο.π.

[41] Βλ. άρθρο 1 παρ. 3, .ο.π.

δίκη ενώπιον δικαστηρίου , που έχει δικαιοδοσία σε ποινικές υποθέσεις . Τέλος, δύναται να εκδοθεί και σε διαδικασίες , οι οποίες αφορούν αδικήματα ή παραβάσεις δυνάμενα να στοιχειοθετήσουν την ευθύνη ή να επισύρουν την τιμωρία νομικού προσώπου στο Κράτος Έκδοσης. Επιπρόσθετα, μια ΕΕΕ μπορεί να εκδίδεται μόνον όταν η αρχή έκδοσης κρίνει ότι πληρούνται οι εξής προϋποθέσεις : η έκδοση της ΕΕΕ είναι απαραίτητη και αναλογική για τους σκοπούς των παραπάνω διαδικασιών, λαμβανομένων υπόψη των δικαιωμάτων του υπόπτου ή κατηγορουμένου και τα ερευνητικά μέτρα που προβλέπονται στην ΕΕΕ θα μπορούσαν να είχαν διαταχθεί υπό τις ίδιες προϋποθέσεις σε παρόμοια εγχώρια υπόθεση.

ii. Αρμόδιες Αρχές Έκδοσης και Εκτέλεσης

Η ΕΕΕ μπορεί να εκδοθεί από δικαστή , δικαστήριο, ανακριτή ή εισαγγελέα με αρμοδιότητα στη συγκεκριμένη υπόθεση ή κάθε άλλη αρμόδια αρχή ορισθείσα από το Κράτος Έκδοσης η οποία στη συγκεκριμένη περίπτωση ενεργεί ως ανακριτική αρχή σε ποινικές διαδικασίες, αρμοδία να διατάσσει τη συγκέντρωση αποδεικτικών στοιχείων, σύμφωνα με το εθνικό δίκαιο. Στη δεύτερη περίπτωση, προτού διαβιβαστεί στην αρχή εκτέλεσης , η ΕΕΕ πρέπει να επικυρώνεται από δικαστή , δικαστήριο, ανακριτή ή εισαγγελέα στο Κράτος Έκδοσης, αφού διαπιστωθεί ότι πληρεί τις προϋποθέσεις για την έκδοση ΕΕΕ , σύμφωνα με την Οδηγία 2014/41/ΕΕ[42]. Για παράδειγμα, αρμόδια αρχή για την έκδοση της ΕΕΕ από την Ελλάδα είναι: α) δικαστής, δικαστήριο, ανακριτής ή εισαγγελέας με αρμοδιότητα στη συγκεκριμένη υπόθεση και β) κάθε άλλη αρμόδια αρχή, η οποία στη συγκεκριμένη υπόθεση ενεργεί ως ανακριτική αρχή σε ορισμένη ποινική διαδικασία, υπό τον όρο ότι η ΕΕΕ που εκδίδεται από αυτή επικυρώνεται από τον αρμόδιο εισαγγελέα, ο οποίος την επικυρώνει, αφού ερευνήσει την τήρηση των προϋποθέσεων του παρόντος νόμου[43].

Τέλος, ως αρχή εκτέλεσης ορίζεται η αρχή που είναι αρμόδια να αναγνωρίζει μια ΕΕΕ και να εξασφαλίζει την εκτέλεσή της, σύμφωνα με την Οδηγία 2014/41/ΕΕ και τις ισχύουσες διαδικασίες σε παρόμοια εγχώρια υπόθεση. Οι εν λόγω διαδικασίες μπορεί να απαιτούν έγκριση δικαστηρίου στο Κράτος Εκτέλεσης, όταν αυτό προβλέπεται από την εθνική του νομοθεσία. Για παράδειγμα, στην Ελλάδα έχει οριστεί ως αρχή εκτέλεσης ο εισαγγελέας εφετών στη δικαστική

[42] Βλ. άρθρο 2, περ. γ', ο.π.
[43] Βλ. άρθρο 6 του ν. 4489/2017, ΦΕΚ Α' 140/21-09-2017

περιφέρεια του οποίου πρόκειται να εκτελεστεί η ΕΕΕ, ο οποίος μεριμνά, κατά περίπτωση, για την εκτέλεσή της[44].

iii. Περιεχόμενο της ΕΕΕ

Η ΕΕΕ περιλαμβάνει τουλάχιστον τις ακόλουθες πληροφορίες: στοιχεία σχετικά με την αρχή έκδοσης, το αντικείμενο και τους λόγους έκδοσης της ΕΕΕ, τις απαραίτητες διαθέσιμες πληροφορίες για τα ενδιαφερόμενα πρόσωπα, περιγραφή της αξιόποινης πράξης που αποτελεί αντικείμενο έρευνας ή διαδικασίας και των ισχυουσών διατάξεων του ποινικού δικαίου του Κράτους Έκδοσης, καθώς και περιγραφή των ερευνητικών μέτρων που ζητούνται και των αποδεικτικών στοιχείων που πρέπει να συγκεντρωθούν. Η ΕΕΕ συμπληρώνεται σύμφωνα με το προτυπωμένο έντυπο του Παραρτήματος Α της Οδηγίας 2014/41/ΕΕ και υπογράφεται από την Αρχή Έκδοσης, η οποία πιστοποιεί την ακρίβεια και βεβαιώνει την ορθότητα του περιεχομένου της. Διαβιβάζεται από την Αρχή Έκδοσης στην Αρχή Εκτέλεσης με οποιοδήποτε μέσο δυνάμενο να τεκμηριωθεί εγγράφως και κατά τρόπον, ώστε το Κράτος Εκτέλεσης να μπορεί να πιστοποιήσει τη γνησιότητά της. Η Αρχή Έκδοσης μπορεί ενδεικτικά να διαβιβάζει τις ΕΕΕ μέσω του συστήματος τηλεπικοινωνιών του Ευρωπαϊκού Δικαστικού Δικτύου (ΕΔΔ) που δημιουργήθηκε με την κοινή δράση 98/428/ΔΕΥ του Συμβουλίου[45]. Εάν η Αρχή Έκδοσης εκδώσει ΕΕΕ που συμπληρώνει προγενέστερη ΕΕΕ («συμπληρωματική ΕΕΕ»), επισημαίνει το γεγονός αυτό στην ΕΕΕ, σύμφωνα με το έντυπο του παραρτήματος Α, στο τμήμα Δ.

iv. Η εκτέλεση της ΕΕΕ

Η Αρχή Εκτέλεσης αναγνωρίζει άνευ ετέρου ΕΕΕ διαβιβασθείσα σύμφωνα με την Οδηγία 2014/41/ΕΕ και μεριμνά για την εκτέλεσή της κατά τον ίδιο τρόπο και την ίδια διαδικασία σαν να επρόκειτο για ερευνητικό μέτρο διαταχθέν από αρχή του Κράτους Εκτέλεσης. Ωστόσο, όταν μια ΕΕΕ παραλαμβάνεται από Αρχή Εκτέλεσης και δεν έχει εκδοθεί ή επικυρωθεί από δικαστική αρχή, επιστρέφεται στο Κράτος Έκδοσης. Η έκδοση της απόφασης σχετικά με την αναγνώριση ή την εκτέλεση και η εκτέλεση του ερευνητικού μέτρου πραγματοποιούνται με

[44] Βλ. άρθρο 11, ο.π.

[45] 98/428/ΔΕΥ: Κοινή δράση της 29ης Ιουνίου 1998 που θεσπίστηκε από το Συμβούλιο βάσει του άρθρου Κ.3 της συνθήκης για την Ευρωπαϊκή Ένωση, για τη δημιουργία ευρωπαϊκού δικαστικού δικτύου

την ταχύτητα και την προτεραιότητα που θα δινόταν για παρόμοια εγχώρια υπόθεση. Σε κάθε περίπτωση η απόφαση για την αναγνώριση ή την εκτέλεση ΕΕΕ θα πρέπει να εκδίδεται από την αρμόδια αρχή εκτέλεσης το συντομότερο δυνατόν και πάντως εντός 30 ημερών από την παραλαβή της ΕΕΕ. Εάν δεν συντρέχουν λόγοι αναβολής δυνάμει του άρθρου 15 της Οδηγίας, η αρχή εκτέλεσης εκτελεί αμελλητί το ερευνητικό μέτρο και το αργότερο 90 ημέρες μετά τη λήψη της απόφασης αναγνώρισης ή εκτέλεσης. Όταν σε συγκεκριμένη περίπτωση δεν είναι πρακτικά εφικτό για την αρμόδια αρχή εκτέλεσης να τηρήσει την προθεσμία που ορίζεται, 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 αυτήν την περίπτωση, η προθεσμία μπορεί να παρατεθεί το ανώτατο κατά 30 ημέρες. Η πρόβλεψη προθεσμιών κρίθηκε απαραίτητη για να εξασφαλισθεί η ταχεία, αποτελεσματική και συνεπής συνεργασία των κρατών μελών σε ποινικές υποθέσεις[46].

ΙΙ. Κριτική επί της ΕΕΕ αναφορικά με τα ηλεκτρονικά αποδεικτικά μέσα

Εισαγωγικά

Στη συνάντηση της 4ης Οκτωβρίου 2016 η ομάδα ειδικών, την οποία αποτελούσαν επαγγελματίες προερχόμενοι από Κράτη-Μέλη της ΕΕ, καθώς και εκπρόσωποι του Ευρωπαϊκού Δικαστικού Δικτύου και της Ευρωπόλ, εξέτασε την πιθανότητα προσαρμογής της ΕΕΕ στις ιδιαίτερες ανάγκες των ηλεκτρονικών αποδεικτικών μέσων, κυρίως μέσα από την τροποποίηση του υποδείγματος αίτησης ΕΕΕ που βρίσκεται στο παράρτημα Α της Οδηγίας, ώστε να καταστεί αυτό κατάλληλο για αποστολή αιτημάτων πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία και την δημιουργία μιας ηλεκτρονικής «πύλης» για την ταχύτερη αποστολή και παραλαβή των αιτημάτων αυτών[47]. Ωστόσο κρίθηκε ότι το πεδίο εφαρμογής της ΕΕΕ δεν είναι κατάλληλο για την πρόσβαση στα ηλεκτρονικά αποδεικτικά στοιχεία και ότι οι προβλεπόμενες διατάξεις δεν επαρκούν για να καλύψουν την ανάγκη αυτή.

[46] Βλ. Αιτιολογική Σκέψη (21), ο.π.

[47] Commission, Staff Working Document, 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 Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD (2018) 118 final, 17 April 2018, p. 137

i. Η έλλειψη ομοιομορφίας στη νομοθεσία των Κρατών-Μελών

Όπως προαναφέρθηκε, η ΕΕΕ έχει οριζόντιο πεδίο εφαρμογής και επομένως εφαρμόζεται σε όλα τα ερευνητικά μέτρα που στοχεύουν στη συγκέντρωση αποδεικτικών στοιχείων[48]. Αρμόδια να αποφασίζει ποιο ερευνητικό μέτρο θα πρέπει να χρησιμοποιηθεί κάθε φορά είναι η αρχή που εκδίδει την ΕΕΕ. Ελλείψει όμως ομοιόμορφου νομοθετικού πλαισίου στην Ευρωπαϊκή Ένωση, το οποίο θα ορίζει συγκεκριμένες διαδικασίες για τη συλλογή, επεξεργασία και υποβολή των ηλεκτρονικών αποδεικτικών μέσων σε ποινικές υποθέσεις, κάθε Αρχή Έκδοσης μπορεί να επιλέξει κατά την κρίση της διαφορετικό ερευνητικό μέτρο σε κάθε περίπτωση, κάτι που οδηγεί σε κατακερματισμό των διαδικασιών συλλογής ηλεκτρονικών αποδεικτικών μέσων εντός της ΕΕ, στη δημιουργία αισθήματος ανασφάλειας δικαίου και πιθανότατα σε λιγότερες εγγυήσεις ως προς τις διαδικασίες αυτές. Επίσης, η ανομοιομορφία που υπάρχει γενικότερα στις νομοθεσίες των Κρατών-Μελών μπορεί να οδηγήσει στην εκτέλεση άλλου ερευνητικού μέτρου από αυτό που ζητήθηκε[49] ή ακόμα και σε μη αναγνώριση ή μη εκτέλεση της ΕΕΕ[50].

ii. Έλλειψη ειδικών διατάξεων για τα ηλεκτρονικά αποδεικτικά μέσα

Στα άρθρα 22 και επόμενα της Οδηγίας 2014/41/ΕΕ προβλέπονται ειδικές διατάξεις για ορισμένα διερευνητικά μέτρα. Ωστόσο δεν υπάρχει καμία πρόβλεψη ειδικά για τα ηλεκτρονικά αποδεικτικά μέσα. Ακόμα και στο άρθρο 28, όπου προβλέπονται ερευνητικά μέτρα που συνεπάγονται τη συγκέντρωση αποδεικτικών στοιχείων σε πραγματικό χρόνο, συνεχώς και για ορισμένο χρονικό διάστημα, δε γίνεται λόγος για ηλεκτρονικά δεδομένα. Περαιτέρω στο Κεφάλαιο V για την παρακολούθηση επικοινωνιών, φαίνεται ότι καλύπτονται μόνο οι "παραδοσιακές" τηλεπικοινωνίες[51], χωρίς ειδική πρόβλεψη για τις over-the-top υπηρεσίες[52],

[48] Βλ. Αιτιολογική Σκέψη (8), ο.π.
[49] Βλ. άρθρο 10, Οδηγία 2014/41/ΕΕ
[50] Βλ. άρθρο 11, ο.π.
[51] Βλ. Αιτιολογική Σκέψη (30), Οδηγία 2014/41/ΕΕ, όπου γίνεται λόγος για τηλεφωνικές συνδιαλέξεις και για δεδομένα κίνησης και θέσης ως προς αυτές τις τηλεπικοινωνίες
[52] Ως over-the-top (OTT) χαρακτηρίζεται κάθε υπηρεσία ή εφαρμογή που παρέχεται μέσω Διαδικτύου, παρακάμπτοντας την παραδοσιακή διανομή (π.χ. μέσω καλωδίου ή δορυφόρου). Τέτοιου είδους υπηρεσίες σχετίζονται συνήθως με το ψηφιακό περιεχόμενο και τις επικοινωνίες. Χαρακτηριστικά παραδείγματα αποτελούν η Netflix, η Amazon Prime, η Hulu κ.α., οι οποίες αντικαθιστούν την "παραδοσιακή" καλωδιακή ή δορυφορική τηλεόραση και η Skype, η WhatsApp, η Viber κ.α., οι οποίες αντικαθιστούν την "παραδοσιακή" επικοινωνία μέσω καλωδίου σταθερής τηλεφωνίας ή κεραιών κινητής τηλεφωνίας.

όπως είναι οι τηλεφωνικές κλήσεις που χρησιμοποιούν το Πρωτόκολλο του Διαδικτύου (Voice over IP - VoIP), οι υπηρεσίες άμεσης ανταλλαγής μηνυμάτων (instant messengers) και τα μηνύματα ηλεκτρονικού ταχυδρομείου (e-mails), υπηρεσίες οι οποίες χρησιμοποιούνται κατά κόρον σήμερα από ολοένα και περισσότερους ανθρώπους και τείνουν να αντικαταστήσουν τα "παραδοσιακά" μέσα επικοινωνίας. Η μόνη σχετική αναφορά σε ζητήματα που σχετίζονται με το Διαδίκτυο αφορά στο ερευνητικό μέτρο της αναγνώρισης προσώπων, που έχουν συνδρομή σε έναν συγκεκριμένο αριθμό τηλεφώνου ή διεύθυνση IP.

Προκειμένου λοιπόν να εκτελεστεί μια ΕΕΕ, που περιλαμβάνει αίτημα διατήρησης ή υποβολής ηλεκτρονικών δεδομένων, θα πρέπει τα ειδικά αυτά μέτρα, της διατήρησης και της υποβολής ηλεκτρονικών δεδομένων να είναι διαθέσιμα, τόσο στο Κράτος Έκδοσης της ΕΕΕ όσο και στο Κράτος Εκτέλεσης της ΕΕΕ, κάτι το οποίο δεν είναι καθόλου βέβαιο δεδομένης της ανομοιομορφίας που παρατηρείται στο δίκαιο των Κρατών-Μελών, όπως προαναφέρθηκε.

iii. Η ταχύτητα της πρόσβασης στα ηλεκτρονικά αποδεικτικά μέσα

Μια από τις καινοτομίες της Οδηγίας 2014/41/ΕΕ είναι η πρόβλεψη ανώτατων χρονικών ορίων για την παροχή της δικαστικής συνδρομής. Όπως προαναφέρθηκε, η απόφαση για την αναγνώριση ή την εκτέλεση ΕΕΕ εκδίδεται το αργότερο 30 ημέρες μετά την παραλαβή της ΕΕΕ και εάν δεν συντρέχουν λόγοι αναβολής, δυνάμει του άρθρου 15 της Οδηγίας, η Αρχή Εκτέλεσης εκτελεί το ερευνητικό μέτρο το αργότερο 90 ημέρες μετά τη λήψη της απόφασης . Σε ορισμένες περιπτώσεις η Οδηγία ΕΕΕ επιτρέπει πιο σύντομες προθεσμίες. Η Αρχή Έκδοσης μπορεί για παράδειγμα να αναφέρει στην ΕΕΕ ότι απαιτείται συντομότερη προθεσμία "λόγω διαδικαστικών προθεσμιών, σοβαρότητας του αδικήματος ή άλλων ιδιαίτερα επειγουσών περιστάσεων[53]. Ωστόσο, η εξέλιξη αυτή θεωρείται από ειδικούς των Κρατών Μελών ανεπαρκής για την πρόσβαση σε ηλεκτρονικά αποδεικτικά μέσα σε ποινικές έρευνες, για τα οποία η ΕΕΕ δεν είναι αρκετά γρήγορη και κατά συνέπεια χαρακτηρίζεται ως αναποτελεσματική. Ο χρόνος είναι κρίσιμος παράγοντας για την πρόσβαση στα ηλεκτρονικά αποδεικτικά μέσα. Ελλείψει υποχρεώσεων διατήρησης, οι Πάροχοι Υπηρεσιών δεν έχουν κανένα κίνητρο να αποθηκεύουν δεδομένα - ιδίως μεταδεδομένα - για περισσότερο από το αναγκαίο χρονικό διάστημα. Τουναντίον, η αποθήκευση δεδομένων συνεπάγεται επιπρόσθετο κόστος για αυτούς.

[53] Βλ. άρθρο 12 παρ. 2, ο.π.

Επιπρόσθετα, η αρχή της ελαχιστοποίησης των δεδομένων που είναι εγγενής στους κανόνες προστασίας δεδομένων[54] υποχρεώνει τους Παρόχους Υπηρεσιών να αποθηκεύουν τα δεδομένα, μόνο για όσο διάστημα είναι απολύτως απαραίτητο.

Επιπλέον, η μεσολάβηση τόσο των Δημοσίων Αρχών του Κράτους Έκδοσης της ΕΕΕ όσο και των Δημοσίων Αρχών του Κράτους Εκτέλεσης της ΕΕΕ συμβάλλουν στην καθυστέρηση της διαδικασίας πρόσβασης στα ηλεκτρονικά αποδεικτικά στοιχεία. Πρακτικά, αφού η Δημόσια Αρχή του Κράτους Εκτέλεσης λάβει την ΕΕΕ και εξετάσει τη βασιμότητά της, αποστέλλει η ίδια αίτημα στον Πάροχο Υπηρεσιών, στην κατοχή του οποίου βρίσκονται αποθηκευμένα τα ζητούμενα ηλεκτρονικά δεδομένα. Ο τελευταίος αποστέλλει τα ζητούμενα δεδομένα στη Δημόσια Αρχή του Κράτους Εκτέλεσης, η οποία τα μεταβιβάζει με τη σειρά της στη Δημόσια Αρχή του Κράτους Έκδοσης της ΕΕΕ.

Τέλος, ένας παράγοντας που συμβάλει ακόμα περισσότερο στην καθυστέρηση των διαδικασιών είναι το γεγονός ότι τα αιτήματα για Αμοιβαία Δικαστική Συνδρομή (τα οποία ανέρχονται επί του παρόντος σε 5.000 περίπου ανά έτος συνολικά για όλα τα είδη συνδρομής, όχι μόνο για την πρόσβαση σε ηλεκτρονικά αποδεικτικά μέσα[55]), τα αιτήματα για την αναγνώριση και εκτέλεση ΕΕΕ, καθώς και οι επακόλουθες απαντήσεις και έρευνες αποστέλλονται ακόμα με "παραδοσιακά" μέσα, όπως για παράδειγμα ταχυδρομικά ή μέσω τηλεομοιοτυπίας (Φαξ).

iii. Το περιορισμένο πεδίο εφαρμογής της ΕΕΕ και η μη συμμετοχή όλων των Κρατών-Μελών της ΕΕ

Σημαντικό μειονέκτημα της ΕΕΕ, που καθιστά το μέτρο αυτό ημιτελές στον τομέα των ηλεκτρονικών αποδεικτικών στοιχείων, είναι το γεγονός ότι το πεδίο εφαρμογής της εκτείνεται μόνο στους Παρόχους Υπηρεσιών που έχουν την έδρα τους σε Κράτος-Μέλος της Ένωσης, ενώ δεν εμπίπτουν σε αυτό οι Πάροχοι Υπηρεσιών που εδρεύουν εκτός της ΕΕ, όπως για παράδειγμα στις ΗΠΑ, ακόμα και αν τα ζητούμενα δεδομένα είναι αποθηκευμένα εντός της ΕΕ. Δεδομένου του γεγονότος ότι οι μεγαλύτεροι Πάροχοι Υπηρεσιών στο Διαδίκτυο εδρεύουν στις ΗΠΑ, η

[54] Βλ. άρθρο 5 παρ. 1 περ. γ', άρθρο 89 παρ. 1 και Αιτιολογική Σκέψη (156) Γενικού Κανονισμού Προστασίας Δεδομένων

[55] E-CODEX, Criminal Justice – Mutual Legal Assistance

ΕΕΕ αποδεικνύεται σε μεγάλο βαθμό ανεπαρκής για την πρόσβαση στα ηλεκτρονικά δεδομένα που διατηρούνται από αυτούς.

Ακόμη όμως και αν οι Πάροχοι Υπηρεσιών διαθέτουν έδρα σε Κράτος-Μέλος της ΕΕ, δεν είναι καθόλου βέβαιο ότι το Κράτος-Μέλος αυτό δεσμεύεται από την ΕΕΕ. Ένα βασικό μειονέκτημα της Οδηγίας 2014/41/ΕΕ, όσον αφορά στο πεδίο των ηλεκτρονικών αποδεικτικών μέσων, είναι το γεγονός ότι Κράτη-Μέλη της ΕΕ, όπως για παράδειγμα η Δανία και η Ιρλανδία, η οποία σημειωτέον αποτελεί την Ευρωπαϊκή έδρα πολλών από τους μεγαλύτερους Παρόχους Υπηρεσιών στο Διαδίκτυο, δεν συμμετείχαν στην έκδοση της Οδηγίας και κατά συνέπεια δεν δεσμεύονται από αυτήν, ούτε υπόκεινται στην εφαρμογή της[56]. Για τις χώρες αυτές συνεχίζουν να βρίσκονται σε ισχύ οι "παραδοσιακοί" οδοί αμοιβαίας δικαστικής συνδρομής εντός της ΕΕ.

[56] Βλ. Αιτιολογική Σκέψη (44), ο.π.

Γ. Η Συμφωνία Αμοιβαίας Δικαστικής Συνδρομής του 2003 μεταξύ ΕΕ και ΗΠΑ

Η Συμφωνία Αμοιβαίας Δικαστικής Συνδρομής (Agreement on Mutual Legal Assistance-MLA) μεταξύ ΕΕ και ΗΠΑ[57] υπογράφηκε στις 25 Ιουνίου 2003 και τέθηκε σε ισχύ την 1η Φεβρουαρίου του 2010. Η ιδέα μιας συμφωνίας δικαστικής συνεργασίας μεταξύ των Αμερικανικών και των Ευρωπαϊκών Αρχών ωρίμασε μετά τα τρομοκρατικά χτυπήματα της 11ης Σεπτεμβρίου 2001, όταν κατέστη σαφές και στις δυο πλευρές ότι μια τέτοια διατλαντική συμφωνία είναι απαραίτητη για την αντιμετώπιση του εγκλήματος και της τρομοκρατίας. Τα συμβαλλόμενα μέρη της Συμφωνίας αποτελούσαν η ΕΕ και οι ΗΠΑ, παρόλο που πολλά Κράτη-Μέλη της ΕΕ είχαν ήδη υπογράψει διμερείς συμφωνίες Αμοιβαίας Δικαστικής Συνδρομής με τις ΗΠΑ. Η Συμφωνία έδωσε νέα διάσταση στην Αμοιβαία Δικαστική Συνδρομή μεταξύ ΕΕ και ΗΠΑ δίνοντας νέες δυνατότητες συνεργασίας, όπως για παράδειγμα τη δυνατότητα πρόσβασης σε τραπεζικούς λογαριασμούς (άρθρο 4), τη σύσταση κοινών ερευνητικών ομάδων (άρθρο 5), την εξέταση μαρτύρων μέσω τηλεδιάσκεψης (άρθρο 6), την ταχύτερη αποστολή των αιτημάτων δικαστικής συνδρομής και των απαντήσεων (άρθρο 7) και τη συνδρομή σε έρευνες που λαμβάνουν χώρα από διοικητικές αρχές (άρθρο 8).

Ο αριθμός των υποθέσεων που αφορούσαν αιτήματα από τις Ευρωπαϊκές Αρχές προς τις Αρχές των ΗΠΑ την περίοδο 2010-2014 ανερχόταν, σύμφωνα με έρευνα της Ευρωπαϊκής Επιτροπής, στα 7.000, εκ των οποίων τα 1.700 στάλθηκαν το έτος 2014[58]. Αξίζει να σημειωθεί ότι, σύμφωνα με την ίδια έρευνα, μεταξύ των πέντε Κρατών-Μελών, από τα οποία στάλθηκαν τα περισσότερα αιτήματα για το έτος 2014, συμπεριλαμβανόταν και η Ελλάδα[59]. Ένα μεγάλο μέρος των αιτημάτων αυτών αφορούσαν ηλεκτρονικά αποδεικτικά μέσα, κυρίως σε υποθέσεις διαδικτυακής απάτης, παιδικής πορνογραφίας και παράνομης διείσδυσης σε υπολογιστικά συστήματα. Ωστόσο, υπήρξαν και αιτήματα, τα οποία έμειναν ανεκτέλεστα. Οι κύριοι λόγοι για τη μη εκτέλεση των αιτημάτων αυτών ήταν είτε ότι αυτά αφορούσαν ήσσονος σημασίας -σύμφωνα τις Αρχές των ΗΠΑ- εγκλήματα, είτε ότι ερχόντουσαν σε σύγκρουση με άλλα

[57] Agreement on mutual legal assistance between the European Union and the United States of America, ΕΕ L 181/34 της 19.7.2003

[58] Council of the European Union, Review of the 2010 EU-US MLA Agreement - Examination of draft texts, Brussels, 7 April 2016, 7403/16

[59] Ο.π.

υπέρτερα -σύμφωνα με το Δίκαιο των ΗΠΑ- δικαιώματα, όπως αυτό της ελευθερίας του λόγου, είτε τέλος, επειδή δεν πληρούταν ο όρος της "πιθανής αιτίας" που απαιτεί ο Αμερικανός Νόμος για τις Ηλεκτρονικές Επικοινωνίες, προκειμένου να υποχρεωθεί ο Πάροχος Υπηρεσιών με έδρα τις ΗΠΑ να υποβάλει τα ηλεκτρονικά δεδομένα που ζητούνταν.

Περαιτέρω, το άρθρο 17 της Συμφωνίας προέβλεπε επανεξέταση της Συμφωνίας το αργότερο 5 έτη μετά την έναρξη της εφαρμογής της. Έτσι, κατά τη διάρκεια την συζητήσεων για την επανεξέταση της Συμφωνίας ανέκυψαν ως βασικά ζητήματα, μεταξύ των άλλων, η αυξανόμενη ταχύτητα και ο αριθμός των αιτημάτων των Αρχών της ΕΕ, που εκτελέστηκαν, ειδικά σε υποθέσεις που περιελάμβαναν ηλεκτρονικά αποδεικτικά μέσα και η βελτίωση της απευθείας πρόσβασης των Ευρωπαϊκών Αρχών στα δεδομένα, που διατηρούν οι Αμερικανικοί Πάροχοι Υπηρεσιών. Ανάμεσα στις προτεραιότητες για τη βελτίωση της Συμφωνίας συμπεριλήφθηκαν η στενότερη συνεργασία μεταξύ ΕΕ και ΗΠΑ στον τομέα των ηλεκτρονικών αποδεικτικών μέσων σε ποινικές υποθέσεις και η βελτίωση της διαδικασίας απόκτησης ηλεκτρονικών αποδεικτικών μέσων, τα οποία διατηρούνται στις ΗΠΑ, από τις Αρχές της ΕΕ.

Δ. Η απευθείας επικοινωνία με τους Παρόχους Υπηρεσιών

Επί του παρόντος, σε διασυνοριακές υποθέσεις που αφορούν στην διερεύνηση ηλεκτρονικών εγκλημάτων υπάρχει και μια άλλη πιθανή οδός για την πρόσβαση των αρχών της ΕΕ στα ηλεκτρονικά αποδεικτικά στοιχεία, πέρα από την "παραδοσιακή οδό της Αμοιβαίας Δικαστικής Συνδρομής. Η τελευταία έχει αποδειχθεί ιδιαίτερα χρονοβόρα και ενέχει τον κίνδυνο ότι τα δεδομένα που ζητούνται πιθανόν να έχουν διαγραφεί στο μεσοδιάστημα, από την υποβολή του αιτήματος μέχρι την εκτέλεσή του, ή να έχουν μεταφερθεί σε άλλο κράτος κατά τη στιγμή της εκτέλεσης του αιτήματος ΑΔΣ, και κατά συνέπεια να είναι απαραίτητη η υποβολή ενός νέου αιτήματος ΑΔΣ με αποδέκτη το κράτος, στο οποίο έχουν ήδη μεταφερθεί τα ζητούμενα δεοδομένα, καθιστώντας έτσι ιδιαίτερα αργή και ίσως μάταιη την αναζήτηση των ηλεκτρονικών αποδεικτικών μέσων. Η δεύτερη αυτή οδός αφορά την απευθείας συνεργασία των δικαστικών αρχών με τους αλλοδαπούς Παρόχους Υπηρεσιών. Στην πράξη, οι Δημόσιες Αρχές των Κρατών-Μελών επικοινωνούν με τους Παρόχους Υπηρεσιών που εδρεύουν στις ΗΠΑ και ζητούν, σύμφωνα με το δίκαιο των ΗΠΑ, να έχουν πρόσβαση στα δεδομένα που τους αφορούν. Ο Αμερικανικός Νόμος επιτρέπει στους Παρόχους Υπηρεσιών να συνεργάζονται απευθείας με τις Αρχές άλλων κρατών, συμπεριλαμβανομένης και των Κρατών-Μελών της ΕΕ[60].

Το μοντέλο αυτό αποτελεί τον κανόνα όσον αφορά την πρόσβαση των Ευρωπαϊκών δικαστικών αρχών σε ηλεκτρονικά αποδεικτικά μέσα, που διατηρούν Πάροχοι Υπηρεσιών στις ΗΠΑ. Είναι χαρακτηριστικό ότι το διάστημα 2013-2016 σημειώθηκε αύξηση κατά 70% των αιτημάτων που προέρχονταν από Αρχές Κρατών-Μελών της ΕΕ προς τους Παρόχους Υπηρεσιών[61]. Για παράδειγμα, το 2016 οι αμερικανικοί κολοσσοί Apple, Facebook, Google, Microsoft, και Twitter δέχθηκαν περισσότερα από 120.000 αιτήματα δικαστικής συνδρομής από

[60] Βλ. Παράγραφο 2701(2) του Νόμου Electronic Communications and Privacy Act 1986 (ECPA)

[61] Commission, Staff Working Document, 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 Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD (2018) 118 final, 17 April 2018, p. 15

Ευρωπαϊκές δικαστικές αρχές[62], ενώ και το 2017 τα αιτήματα που προέρχονταν από την ΕΕ προς τους αμερικανικούς Παρόχους Υπηρεσιών συνολικά ξεπέρασαν τα 124.000[63].

Η ανταπόκριση σε τέτοιου είδους αιτήματα παρουσιάζει σταθερά αυξητική πορεία. Οι Πάροχοι Υπηρεσιών ανταποκρίθηκαν στο 58% των αιτημάτων που υποβλήθηκαν το δεύτερο εξάμηνο του 2016, ποσοστό κατά 12% μεγαλύτερο από το αντίστοιχο του έτους 2013[64]. Ωστόσο βασικό μειονέκτημα αυτού του μοντέλου αποτελεί το γεγονός ότι η συνεργασία δεν είναι υποχρεωτική για τους αποδέκτες των αιτημάτων, αλλά εξαρτάται από την ευχέρεια του εκάστοτε Παρόχου Υπηρεσιών και από την πολιτική που ακολουθεί η εταιρία.

Τέλος, άλλο ένα σημαντικό μειονέκτημα είναι ότι το μοντέλο αυτό δικαστικής συνεργασίας καλύπτει μόνο δεδομένα, που δεν αφορούν το περιεχόμενο[65], ενώ η πρόσβαση σε δεδομένα περιεχομένου απαγορεύεται από τη νομοθεσία των ΗΠΑ.

[62] Ο.π.

[63] European Commission, Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Brussels, 5.2.2019 COM(2019) 70 final

[64] Commission, Staff Working Document, Impact Assessment, ο.π., σελ. 16

[65] Για την διάκριση ανάμεσα σε "δεδομένα που αφορούν το περιεχόμενο" και σε "δεδομένα που δεν αφορούν το περιεχόμενο" βλ. ενδεικτικά παρακάτω σελ. 47 της παρούσης

ΜΕΡΟΣ ΔΕΥΤΕΡΟ
Η ΔΙΚΑΣΤΙΚΗ ΣΥΝΕΡΓΑΣΙΑ ΣΤΟ ΜΕΛΛΟΝ

Α. Οι Προτάσεις Κανονισμού και Οδηγίας για τα ηλεκτρονικά αποδεικτικά μέσα σε ποινικές υποθέσεις

Εισαγωγικά

Η Ευρωπαϊκή Επιτροπή παρατήρησε ότι διάφορες δυσκολίες κατά τη διασυνοριακή πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία δεν επιτρέπουν σήμερα την αποτελεσματική έρευνα και δίωξη του εγκλήματος στην ΕΕ. Υπάρχει έλλειψη αποτελεσματικότητας όσον αφορά τη δικαστική συνεργασία μεταξύ των δημόσιων αρχών, την άμεση συνεργασία μεταξύ των δημόσιων αρχών και των παρόχων υπηρεσιών και την άμεση πρόσβαση των δημόσιων αρχών σε ηλεκτρονικά αποδεικτικά στοιχεία. Ως εκ τούτου, οι έρευνες αποτελματώνονται, εγκλήματα μένουν ατιμώρητα, τα θύματα προστατεύονται με λιγότερο αποτελεσματικό τρόπο, και οι πολίτες της ΕΕ αισθάνονται λιγότερο ασφαλείς[66]. Τα τρία βασικότερα προβλήματα που εντόπισε είναι ότι στο πλαίσιο των υφιστάμενων διαδικασιών δικαστικής συνεργασίας απαιτείται υπερβολικά πολύς χρόνος για την πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία σε διασυνοριακό επίπεδο, κάτι που καθιστά την έρευνα και τη δίωξη λιγότερο αποτελεσματικές, ότι οι ανεπάρκειες στη συνεργασία δημόσιου και ιδιωτικού τομέα μεταξύ των παρόχων υπηρεσιών και των δημόσιων αρχών δημιουργούν κωλύματα για την αποτελεσματικότητα των ερευνών και των διώξεων και τέλος, ότι τα προβλήματα στον καθορισμό της δικαιοδοσίας μπορούν να δυσχεράνουν την αποτελεσματική διασυνοριακή έρευνα και δίωξη[67].

Για την αντιμετώπιση των προβλημάτων αυτών στις 17 Απριλίου 2018 η Επιτροπή ενέκρινε δύο νομοθετικές προτάσεις: την Πρόταση Κανονισμού σχετικά με την Ευρωπαϊκή Εντολή Υποβολής και την Ευρωπαϊκή Εντολή Διατήρησης ηλεκτρονικών αποδεικτικών

[66] Περίληψη της Εκτίμησης Επιπτώσεων που συνοδεύει το έγγραφο Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις και Πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον ορισμό νόμιμων εκπροσώπων με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών, SWD(2018) 119 final, σελ. 1

[67] Βλ. Περίληψη Εκτίμησης Επιπτώσεων, ο.π.

στοιχείων σε ποινικές υποθέσεις[68] και την Πρόταση Οδηγίας σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον ορισμό νόμιμων εκπροσώπων με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών[69], η οποία συμπληρώνει τον παραπάνω Κανονισμό. Ο γενικός στόχος είναι να διασφαλιστεί η αποτελεσματική έρευνα και δίωξη των εγκλημάτων στην ΕΕ με τη βελτίωση της διασυνοριακής πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία μέσω της ενίσχυσης της δικαστικής συνεργασίας σε ποινικές υποθέσεις και της προσέγγισης των κανόνων και των διαδικασιών. Επιπλέον, υπάρχουν τρεις ειδικοί στόχοι: η μείωση των καθυστερήσεων στη διασυνοριακή πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία, η διασφάλιση της διασυνοριακής πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία, εκεί όπου αυτή είναι επί του παρόντος ανεπαρκής, η βελτίωση της ασφάλειας δικαίου, της προστασίας των θεμελιωδών δικαιωμάτων, της διαφάνειας και της λογοδοσίας[70].

I. Τα κυριότερα χαρακτηριστικά και οι βασικότερες έννοιες των Προτάσεων Κανονισμού και Οδηγίας

i. Η εξέλιξη στον τομέα της αμοιβαίας δικαστικής αναγνώρισης

Από το έτος 1999 ακρογωνιαίος λίθος της δικαστικής συνεργασίας επί ποινικών υποθέσεων στην Ευρωπαϊκή Ένωση θα πρέπει να θεωρείται η αρχή της αμοιβαίας αναγνώρισης των δικαστικών αποφάσεων και διαταγών[71]. Η δυσχέρεια πραγμάτωσης της δικαστικής συνεργασίας και της κτήσης των αποδείξεων μέσω της παραδοσιακής οδού της δικαστικής συνδρομής, παρώθησε την Ευρωπαϊκή Επιτροπή και τα Κράτη-Μέλη της ΕΕ να αναζητήσουν μια πιο εποικοδομητική λύση, την οποία βρήκαν στην αμοιβαία αναγνώριση[72]. Η τελευταία θεμελιώνεται στο άρθρο 82 παρ. 1 ΣΛΕΕ[73], και είχε εισαχθεί το πρώτον με το Ευρωπαϊκό Συμβούλιο του Τάμπερε της 15ης και 16ης Οκτωβρίου 1999[74].

[68] COM(2018) 225 final
[69] COM(2018) 226 final
[70] Βλ. Περίληψη Εκτίμησης Επιπτώσεων, ο.π.
[71] Βλ. Presidency Conclusions of the Tampere European Council, 15 and 16 October 1999, παρ. 33.
[72] Χ. Δημόπουλος, Έκδοση εγκληματιών: Ευρωπαϊκή Εντολή Έρευνας (Μέρος Β΄), ΠοινΔικ, 6/2018, σελ. 577
[73]«Η δικαστική συνεργασία σε ποινικές υποθέσεις στην Ένωση θεμελιώνεται στην αρχή της αμοιβαίας αναγνώρισης των δικαστικών αποφάσεων και περιλαμβάνει την προσέγγιση των νομοθετικών και κανονιστικών διατάξεων των κρατών μελών στους τομείς που προβλέπονται στην παρ. 2 και στο άρθρο 83».
[74] Βλ. Presidency Conclusions of the Tampere European Council, 15 and 16 October 1999, Chapter VI. Mutual recognition of judicial decisions

Στην αρχή της αμοιβαίας αναγνώρισης βασίζεται ο θεσμός της Ευρωπαϊκής Εντολής Έρευνας στις ποινικές υποθέσεις[75], η οποία παρόλο που συνιστά ένα σύγχρονο θεσμικό πλαίσιο αμοιβαίας δικαστικής συνεργασίας στις ποινικές υποθέσεις εντός της Ευρωπαϊκής Ένωσης, ωστόσο, στο πεδίο των ηλεκτρονικών αποδεικτικών στοιχείων αποδεικνύεται ανεπαρκής, καθώς, πέραν των άλλων[76], οι διατάξεις που σχετίζονται με ηλεκτρονικά αποδεικτικά στοιχεία περιορίζονται στην αναγνώριση προσώπων που έχουν συνδρομή σε έναν συγκεκριμένο αριθμό τηλεφώνου ή διεύθυνση IP[77] και στην παρακολούθηση τηλεπικοινωνιών με την τεχνική βοήθεια άλλου κράτους μέλους[78].

Με την Πρόταση Κανονισμού για τα ηλεκτρονικά αποδεικτικά στοιχεία προσδίδεται μια νέα διάσταση στην αμοιβαία αναγνώριση, πέρα από την παραδοσιακή δικαστική συνεργασία εντός της Ένωσης[79]. Η τελευταία βασίζεται μέχρι σήμερα σε διαδικασίες με τη συμμετοχή δύο Δικαστικών Αρχών, μίας στο Κράτος Έκδοσης και μίας στο Κράτος Εκτέλεσης. Η καινοτομία του Κανονισμού έγκειται στο ότι χρησιμοποιεί για πρώτη φορά τη νομική βάση της αμοιβαίας δικαστικής αναγνώρισης στο πλαίσιο της απευθείας υποβολής αιτημάτων μεταξύ Δημοσίων Αρχών (Αρχών Έκδοσης) και Ιδιωτών (Παρόχων Υπηρεσιών). Η επιλογή αυτή δικαιολογείται μάλλον από την ανάγκη προσαρμογής του μηχανισμού συνεργασίας στην ψηφιακή εποχή.

Ωστόσο, πρέπει να σημειωθεί ότι σκοπός της Πρότασης Κανονισμού και της Πρότασης Οδηγίας για τη διαβίβαση ηλεκτρονικών αποδεικτικών στοιχείων και την πρόσβαση σε αυτά δεν είναι η υποκατάσταση προηγούμενων μέσων συνεργασίας σε ποινικές υποθέσεις, που προβλέπονται σε άλλα νομοθετήματα, όπως η Σύμβαση της Βουδαπέστης[80] και η Ευρωπαϊκή

[75] Βλ. άρθρο 1 παρ. 2, 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 της 1.5.2014, η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν. 4489/2017, ΦΕΚ Α' 140/21-9-2017

[76] Βλ. Eurojust / Europol, Common challenges in combating cybercrime, 7021/17, σελ. 11

[77] Βλ. άρθρο 10, παρ. 2 περ. ε', ο.π.

[78] Βλ. άρθρο 30, ο.π.

[79] Βλ. European Commission: Commission Staff Working Document 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 Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD(2018) 118 final, σελ. 37

[80] Σύμβαση της Βουδαπέστης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (CETS αριθ. 185)

Εντολή Έρευνας[81], αλλά η δημιουργία νέων "λεωφόρων" και "ταχέων διαδρομών" για τα ηλεκτρονικά αποδεικτικά μέσα[82]. Οι νέοι θεσμοί είναι σχεδιασμένοι, ώστε να "συνυπάρχουν" με τους ήδη υπάρχοντες θεσμούς, οι οποίοι μπορούν να χρησιμοποιηθούν, κατά περίπτωση, από τις αρμόδιες αρχές[83]. Για παράδειγμα, σύμφωνα με το άρθρο 6 παράγραφος 2 της Πρότασης Κανονισμού, η Ευρωπαϊκή Εντολή Διατήρησης στοιχείων εκδίδεται, ώστε να αποτραπεί η αφαίρεση, η διαγραφή ή η αλλοίωση των δεδομένων ενόψει επακόλουθου αιτήματος υποβολής των εν λόγω δεδομένων είτε μέσω Αμοιβαίας Δικαστικής Συνδρομής[84] ή ΕΕΕ ή Ευρωπαϊκής Εντολής Υποβολής στοιχείων. Επίσης, σύμφωνα με το άρθρο 23 της Πρότασης Κανονισμού οι αρχές των Κρατών-Μελών μπορούν να συνεχίσουν να εκδίδουν ΕΕΕ, σύμφωνα με την Οδηγία 2014/41/ΕΕ, για τη συγκέντρωση αποδεικτικών στοιχείων που επίσης εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού.

ii. Οι Αποδέκτες-Πάροχοι Υπηρεσιών, η υποχρέωση ορισμού νομίμου εκπροσώπου και η κατάργηση των κριτηρίων τοποθεσίας

Αποδέκτες των Ευρωπαϊκών Εντολών Υποβολής και Διατήρησης είναι, όπως προαναφέρθηκε, όχι οι Δημόσιες Αρχές του Κράτους Εκτέλεσης, αλλά απευθείας οι ίδιοι οι Πάροχοι Υπηρεσιών. Ως Πάροχος Υπηρεσιών, σύμφωνα με την Πρόταση Κανονισμού για τα ηλεκτρονικά αποδεικτικά στοιχεία[85] και την Πρόταση Οδηγίας για τον ορισμό νομίμων εκπροσώπων[86], νοείται κάθε φυσικό ή νομικό πρόσωπο, που παρέχει είτε υπηρεσίες ηλεκτρονικών επικοινωνιών, όπως αυτές ορίζονται στο άρθρο 2 περίπτωση 4 της Οδηγίας για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών[87], είτε υπηρεσίες της κοινωνίας

[81] 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 της 1.5.2014

[82] L. Buono, The genesis of the European Union's new proposed legal instrument(s) on e-evidence, ERA Forum 3/19, σελ. 307

[83] B. Jerman Blažič/T. Klobučar, Advancement in Cybercrime Investigation – The New European Legal Instruments for Collecting Cross-border E-evidence σε Information Technology and Systems - Proceedings of ICITS 2019, σελ. 871-877

[84] Όπως για παράδειγμα η Συμφωνία μεταξύ της Ευρωπαϊκής Ένωσης και της Ιαπωνίας για την Αμοιβαία Δικαστική Συνδρομή επί ποινικών υποθέσεων, ΕΕ L 39/19 της 12.2.2010 και η Συμφωνία σχετικά με την Αμοιβαία Δικαστική Συνδρομή μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής, ΕΕ L 181/34 της 19.7.2003

[85] Βλ. άρθρο 2 περ. 3 Πρότασης Κανονισμού

[86] Βλ. άρθρο 2 περ. 2 Πρότασης Οδηγίας

[87] Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018 για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών, ΕΕ L 321/36 της 17.12.2018

της πληροφορίας, όπως ορίζονται στο άρθρο 1 παράγραφος 1 στοιχείο β' της Οδηγίας (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[88], για τις οποίες η αποθήκευση δεδομένων είναι καθοριστικό στοιχείο της υπηρεσίας που παρέχεται στον χρήστη, συμπεριλαμβανομένων των κοινωνικών δικτύων, των επιγραμμικών αγορών που διευκολύνουν τις συναλλαγές μεταξύ των χρηστών τους, και άλλων παρόχων υπηρεσιών φιλοξενίας, είτε τέλος υπηρεσίες ονομάτων χώρου και αρίθμησης IP του διαδικτύου, όπως οι πάροχοι διευθύνσεων IP, τα μητρώα ονομάτων χώρου, οι καταχωρητές ονομάτων χώρου και οι σχετικές υπηρεσίες ιδιωτικής ζωής και διακομιστή μεσολάβησης. Πρακτικά, στις δύο πρώτες κατηγορίες υπάγονται υπηρεσίες, όπως για παράδειγμα η Skype, η WhatsApp, η Amazon, η Ebay, η Dropbox και οι υπηρεσίες ηλεκτρονικού ταχυδρομείου[89]. Σ' αυτές ανήκουν επίσης και τα μέσα κοινωνικής δικτύωσης, όπως το Twitter και το Facebook, που επιτρέπουν στους χρήστες την κοινή χρήση περιεχομένου[90]. Στην τρίτη κατηγορία εντάσσονται, υπηρεσίες όπως είναι για παράδειγμα η GoDaddy[91].

Περαιτέρω, οι Πάροχοι Υπηρεσιών που δραστηριοποιούνται στην εσωτερική αγορά της ΕΕ μπορούν να χωριστούν σε τρεις κύριες κατηγορίες[92] με κριτήριο τον τόπο, όπου έχουν την έδρα τους, σε συνάρτηση με τον τόπο, όπου παρέχουν τις υπηρεσίες τους. Έτσι, την πρώτη κατηγορία αποτελούν οι Πάροχοι Υπηρεσιών που έχουν την έδρα τους σε Κράτος-Μέλος και προσφέρουν υπηρεσίες μόνο στην επικράτεια του εν λόγω Κράτους-Μέλους, κατηγορία που δεν εμπίπτει στο πεδίο εφαρμογής της Πρότασης Οδηγίας[93] ούτε και της Πρότασης Κανονισμού[94].

---

[88] Οδηγία (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Σεπτεμβρίου 2015 για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας των πληροφοριών, ΕΕ, L 241/1 της 17.9.2015

[89] B. Jerman Blažič/T. Klobučar, ο.π.

[90] Βλ. Αιτιολογική Έκθεση Πρότασης Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις, COM(2018) 225 final

[91] European Commission: Commission Staff Working Document 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 Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD (2018) 118 final (2018)

[92] Βλ. Αιτιολογική έκθεση της Πρότασης Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον ορισμό νόμιμων εκπροσώπων με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών, COM(2018) 226 final, σελ. 1

[93] Βλ. άρθρο 1 παρ. 3 της Πρότασης Οδηγίας

[94] Βλ. άρθρο 1 παρ. 1 της Πρότασης Κανονισμού

Οι Πάροχοι Υπηρεσιών εμπίπτουν στο πεδίο εφαρμογής της Πρότασης Κανονισμού, αν παρέχουν τις υπηρεσίες τους εντός της Ευρωπαϊκής Ένωσης ή έχουν εγκατάσταση σε Κράτος - Μέλος της, διαφορετικό από αυτό, στο οποίο ανήκουν οι αρχές που υποβάλουν την Ευρωπαϊκή Εντολή Υποβολής ή την Ευρωπαϊκή Εντολή Διατήρησης στοιχείων, καθώς η Πρόταση Κανονισμού καλύπτει μόνο την διασυνοριακή πρόσβαση στα ηλεκτρονικά αποδεικτικά στοιχεία, ενώ η «εθνική» πρόσβαση δεν εμπίπτει εντός του πεδίου εφαρμογής της[95]. Από την άλλη, η Πρόταση Οδηγίας δεν θίγει την εξουσία των εθνικών αρχών, σύμφωνα με το ενωσιακό και το εθνικό δίκαιο για την επικοινωνία τους με παρόχους υπηρεσιών, που είναι εγκατεστημένοι στην επικράτειά τους[96]. Στη δεύτερη κατηγορία ανήκουν οι Πάροχοι Υπηρεσιών που έχουν την έδρα τους σε Κράτος-Μέλος και προσφέρουν υπηρεσίες σε διάφορα Κράτη-Μέλη της Ένωσης και τέλος, στην τρίτη κατηγορία ανήκουν οι Πάροχοι Υπηρεσιών που έχουν την έδρα τους εκτός της ΕΕ και προσφέρουν υπηρεσίες σε ένα ή περισσότερα Κράτη-Μέλη της, με ή χωρίς εγκαταστάσεις σε ένα ή περισσότερα από αυτά.

Η Πρόταση Οδηγίας θεσπίζει υποχρέωση ορισμού νομίμου εκπροσώπου για τις δύο τελευταίες κατηγορίες Παρόχων Υπηρεσιών που δραστηριοποιούνται στην Ένωση και αποσκοπεί στο να διασφαλίσει ότι υπάρχει πάντα ένας σαφής αποδέκτης των παραπάνω εντολών, οι οποίες στοχεύουν στη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών. Ο νόμιμος εκπρόσωπος θα είναι αρμόδιος για την παραλαβή, τη συμμόρφωση με και την εκτέλεση των εν λόγω εντολών εξ ονόματος του Παρόχου Υπηρεσιών και θα διαμένει ή θα είναι εγκατεστημένος σε ένα από τα Κράτη-Μέλη, όπου είναι εγκατεστημένος ή παρέχει τις υπηρεσίες του ο Πάροχος Υπηρεσιών[97]. Με τον όρο «εγκατάσταση» νοείται είτε η πραγματική άσκηση οικονομικής δραστηριότητας για αόριστο χρόνο μέσω σταθερής υποδομής, από όπου ασκείται η επιχειρηματική δραστηριότητα παροχής υπηρεσιών, είτε η σταθερή υποδομή από την οποία ασκείται η δραστηριότητα[98]· Ως «παροχή υπηρεσιών στην Ένωση» ορίζεται η παροχή δυνατότητας προς φυσικά ή νομικά πρόσωπα σε ένα ή περισσότερα Κράτη-Μέλη να χρησιμοποιούν τις υπηρεσίες που αναφέρονται ανωτέρω. Ωστόσο, μόνη η προσβασιμότητα μιας ηλεκτρονικής διεπαφής όπως, για παράδειγμα, η δυνατότητα πρόσβασης στον ιστότοπο του

[95]Βλ. Αιτιολογική Σκέψη (15) της Πρότασης Κανονισμού
[96]Βλ. Αιτιολογική Σκέψη (10) της Πρότασης Οδηγίας
[97] Βλ. άρθρο 3 παρ. 1 και 2 της Πρότασης Οδηγίας
[98] Βλ. άρθρο 2 περ. 5 Πρότασης Κανονισμού και άρθρο 2 περ. 4 Πρότασης Οδηγίας

Παρόχου Υπηρεσιών, δε θα πρέπει να αποτελεί επαρκή προϋπόθεση[99]. Για τον καθορισμό του πεδίου εφαρμογής των Προτάσεων Κανονισμού και Οδηγίας θα πρέπει να λαμβάνεται επιπλέον υπόψη τυχόν ουσιώδης σύνδεση με την Ένωση[100]. Σε διαφορετική περίπτωση θα επερχόταν τεράστια διεύρυνση του πεδίου εφαρμογής, αφού πρακτικά θα υπαγόταν σε αυτό κάθε Πάροχος Υπηρεσιών στον κόσμο[101], η ιστοσελίδα του οποίου είναι προσβάσιμη από την ΕΕ. Η εν λόγω ουσιώδης σύνδεση θα πρέπει να θεωρείται δεδομένη, όταν ο Πάροχος Υπηρεσιών διαθέτει εγκατάσταση στην Ένωση. Ελλείψει τέτοιας εγκατάστασης, το κριτήριο της ουσιώδους σύνδεσης θα πρέπει να εκτιμάται με βάση την ύπαρξη σημαντικού αριθμού χρηστών σε ένα ή περισσότερα Κράτη-Μέλη ή τη στόχευση δραστηριοτήτων προς ένα ή περισσότερα Κράτη-Μέλη. Η στόχευση δραστηριοτήτων προς ένα ή περισσότερα Κράτη-Μέλη μπορεί να προσδιοριστεί με βάση όλες τις σχετικές περιστάσεις, συμπεριλαμβανομένων στοιχείων όπως η επιλογή της γλώσσας ή του νομίσματος που χρησιμοποιείται γενικά στο οικείο Κράτος-Μέλος ή η δυνατότητα παραγγελίας αγαθών ή υπηρεσιών. Η στόχευση δραστηριοτήτων προς ένα Κράτος- Μέλος θα μπορούσε, επίσης, να συναχθεί από τη διαθεσιμότητα μιας εφαρμογής στο οικείο εθνικό κατάστημα εφαρμογών (π.χ. App Store, Google Play κ.α.), από την παροχή διαφημίσεων στη γλώσσα του εν λόγω Κράτους Μέλους ή από τη διαχείριση των σχέσεων με τους πελάτες, όπως η εξυπηρέτηση πελατών στη γλώσσα του εν λόγω Κράτος-Μέλους[102].

Συμπερασματικά, μία από τις σημαντικές αλλαγές που επιφέρουν οι Προτάσεις αυτές είναι η κατάργηση των κριτηρίων τοποθεσίας σε ποινικές υποθέσεις μέσω της υποχρέωσης για ορισμό νομίμου εκπροσώπου για Παρόχους που δεν είναι εγκατεστημένοι στην ΕΕ, αλλά προσφέρουν υπηρεσίες στην ΕΕ και η δυνατότητα των αρμόδιων αρχών να ζητούν τη διατήρηση και την υποβολή δεδομένων ανεξάρτητα από την ακριβή τοποθεσία αποθήκευσης των εν λόγω δεδομένων. 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 Ευρωπαϊκή Νομοθεσία, καθώς η κατάργηση των κριτηρίων τοποθεσίας είχε προηγηθεί ήδη στον τομέα προστασίας των δεδομένων. Είναι γνωστό ότι το δίκαιο της ΕΕ για την προστασία δεδομένων εφαρμόζεται ανεξάρτητα από την τοποθεσία αποθήκευσης των δεδομένων των

[99] Αιτιολογική Σκέψη (27) της Πρότασης Κανονισμού και (12) της Πρότασης Οδηγίας
[100] Αιτιολογική Σκέψη (28) της Πρότασης Κανονισμού
[101] Dr. Stanislaw Tosza, The European Commission's Proposal on Cross-Border Access to E-Evidence, eucrim 4/2018, σελ. 215
[102] Αιτιολογική Σκέψη (28) της Πρότασης Κανονισμού

ενδιαφερομένων. Πράγματι, ο Γενικός Κανονισμός Προστασίας Δεδομένων[103] εφαρμόζεται είτε αν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι εγκατεστημένος εντός της ΕΕ, είτε αν υποβάλλονται σε επεξεργασία δεδομένα Υποκειμένων της ΕΕ, ακόμη και όταν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δεν είναι εγκατεστημένοι στο έδαφος της ΕΕ[104], περίπτωση στην οποία πρέπει επίσης να ορίσουν νόμιμο εκπρόσωπο στην ΕΕ[105]. Η κατάργηση των κριτηρίων τοποθεσίας εμφανίζεται επιπλέον τόσο στο άρθρο 18 της Οδηγίας (ΕΕ) 2016/1148[106] όσο και στο άρθρο 3 της Πρότασης Κανονισμού για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες[107].

iii. Η επιτάχυνση της διαδικασίας συλλογής των (ηλεκτρονικών) αποδεικτικών μέσων

Σύμφωνα με την Επιτροπή, οι προτάσεις για τα ηλεκτρονικά αποδεικτικά στοιχεία αποσκοπούν στη βελτίωση της δικαστικής συνεργασίας σε ποινικές υποθέσεις μεταξύ αρχών και παρόχων υπηρεσιών στο εσωτερικό της Ευρωπαϊκής Ένωσης, καθώς και με τρίτες χώρες. Βασικός στόχος είναι η ευελιξία και η ταχύτητα των ερευνών για άντληση ηλεκτρονικών αποδεικτικών στοιχείων. Σε αντίθεση με τα υπάρχοντα μέσα συνεργασίας 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 Αμοιβαίας Δικαστικής Συνδρομής- προθεσμίες, εντός των οποίων οφείλει ο Πάροχος να απαντήσει στα αιτήματα, αναμένεται να επιταχύνουν σημαντικά τις διαδικασίες. Πράγματι, ακόμα και στον σύγχρονο θεσμό δικαστικής συνεργασίας της Ευρωπαϊκής Εντολής Έρευνας, η Αρχή Εκτέλεσης έχει στη διάθεσή της προθεσμία 30 ημερών

[103] 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 119/1 της 4.5.2016

[104] Βλ. άρθρο 3, ιδίως παρ. 2, Γενικός Κανονισμός Προστασίας Δεδομένων

[105] Βλ. άρθρο 27, ο.π.

[106] Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, ΕΕ L 194/1 της 19.7.2016

[107] Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ, COM(2017) 10 final

για τη λήψη απόφασης σχετικά με την αναγνώριση της αίτησης[108] και, στη συνέχεια, οφείλει να εκτελέσει την εντολή εντός 90 ημερών[109]. Έτσι, η ΕΕΕ μπορεί να μην καλύπτει την ταχύτητα που απαιτείται για τη συλλογή ηλεκτρονικών αποδεικτικών στοιχείων[110]. Από την άλλη μεριά, η Πρόταση Κανονισμού για τα ηλεκτρονικά αποδεικτικά μέσα σε ποινικές υποθέσεις προβλέπει ότι κατά την παραλαβή του Πιστοποιητικού Ευρωπαϊκής Εντολής Υποβολής στοιχείων, ο Αποδέκτης διασφαλίζει ότι τα ζητούμενα δεδομένα διαβιβάζονται απευθείας στην Αρχή Έκδοσης, το αργότερο εντός 10 ημερών[111] από την παραλαβή του πιστοποιητικού ΕΕΥ ή το αργότερο εντός 6 ωρών[112] σε περιπτώσεις έκτακτης ανάγκης[113].

iv. Τα ηλεκτρονικά αποδεικτικά στοιχεία και η διάκριση των δεδομένων

Ως "ηλεκτρονικά αποδεικτικά στοιχεία" ορίζονται τα αποδεικτικά στοιχεία που είναι αποθηκευμένα σε ηλεκτρονική μορφή από πάροχο υπηρεσιών ή για λογαριασμό του κατά τον χρόνο παραλαβής του πιστοποιητικού εντολής υποβολής ή διατήρησης στοιχείων, τα οποία συνίστανται σε αποθηκευμένα "δεδομένα συνδρομητή", "δεδομένα πρόσβασης", "δεδομένα συναλλαγών" και "δεδομένα περιεχομένου"[114]. Η διάκριση αυτή των δεδομένων κρίνεται απαραίτητη για την κατανόηση και εφαρμογή του παρόντος Κανονισμού. Η ίδια διάκριση, εκτός από τα "δεδομένα πρόσβασης", υπάρχει στις έννομες τάξεις πολλών Κρατών-Μελών, καθώς και στο νομικό πλαίσιο τρίτων χωρών[115].

Πιο συγκεκριμένα, ως «δεδομένα συνδρομητή» ορίζονται[116] οποιαδήποτε δεδομένα αφορούν την ταυτότητα συνδρομητή ή πελάτη, όπως είναι το όνομα, η ημερομηνία γέννησης, η

[108] Βλ. άρθρο 12 παρ. 3, Οδηγία 2014/41/ΕΕ
[109] Βλ. άρθρο 12 παρ. 4, ο.π.
[110] Eurojust / Europol, ο.π.
[111] Βλ. άρθρο 9 παρ. 1 Πρότασης Κανονισμού
[112] Βλ. άρθρο 9 παρ. 2, ο.π.
[113] Ως «περιπτώσεις έκτακτης ανάγκης» ορίζονται, σύμφωνα με το άρθρο 2 περ. 15 της Πρότασης Κανονισμού, ως οι καταστάσεις, στις οποίες υπάρχει επικείμενη απειλή για τη ζωή ή τη σωματική ακεραιότητα προσώπου ή για υποδομές ζωτικής σημασίας, δηλαδή για τα περιουσιακά στοιχεία, συστήματα ή μέρη αυτών που βρίσκονται εντός των κρατών μελών και τα οποία είναι ουσιώδη για τη διατήρηση των λειτουργιών ζωτικής σημασίας της κοινωνίας, της υγείας, της ασφάλειας, της οικονομικής και κοινωνικής ευημερίας των μελών της, και των οποίων η διακοπή λειτουργίας ή η καταστροφή θα είχε σημαντικό αντίκτυπο για ένα κράτος μέλος, ως αποτέλεσμα της αδυναμίας διατήρησης των λειτουργιών αυτών (όπως οι υποδομές ζωτικής σημασίας ορίζονται στο άρθρο 2 στοιχείο α' της οδηγίας 2008/114/ΕΚ του Συμβουλίου)
[114] Βλ. άρθρο 2 περ. 6 Πρότασης Κανονισμού
[115] Βλ. Αιτιολογική Έκθεση Πρότασης Κανονισμού, σελ. 17
[116] Βλ. άρθρο 2 περ. 7, ο.π.

ταχυδρομική ή η γεωγραφική διεύθυνση, δεδομένα τιμολόγησης και πληρωμών, τηλέφωνο ή ηλεκτρονικό ταχυδρομείο κ.α.. Ως "δεδομένα συνδρομητή" θεωρούνται επίσης και αυτά που σχετίζονται με το είδος της υπηρεσίας και τη διάρκειά της. Από την έννοια των "δεδομένων συνδρομητή" εξαιρούνται ρητά[117] οι κωδικοί πρόσβασης ή άλλα μέσα επαλήθευσης ταυτότητας που χρησιμοποιούνται αντί του κωδικού πρόσβασης (όπως είναι για παράδειγμα η αναγνώριση δακτυλικού αποτυπώματος, η αναγνώριση προσώπου κ.α.) και που παρέχονται από τον χρήστη ή δημιουργούνται κατόπιν αιτήματός του. Τα τελευταία αυτά αποτελούν τα λεγόμενα "δεδομένα πρόσβασης", δηλαδή τα 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 είναι για παράδειγμα 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. Στα "δεδομένα πρόσβασης" συμπεριλαμβάνονται με ρητή πρόβλεψη[118] και τα "μεταδεδομένα ηλεκτρονικών επικοινωνιών", όπως ορίζονται στο άρθρο 4 παράγραφος 3 στοιχείο γ'[119] της Πρότασης Κανονισμού για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες[120]. Περαιτέρω, ως "δεδομένα συναλλαγών" ορίζονται[121] τα δεδομένα που σχετίζονται με την παροχή μιας υπηρεσίας από Πάροχο Υπηρεσιών, τα οποία χρησιμεύουν για την παροχή γενικότερου πλαισίου ή πρόσθετων πληροφοριών 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

[117] Βλ. άρθρο 2, περ. 7, υποπερ. Β', ο.π

[118] Βλ. άρθρο 2, περ. 8, εδ. Τελευταίο, ο.π.

[119] «μεταδεδομένα ηλεκτρονικών επικοινωνιών»: τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών για τους σκοπούς της μετάδοσης, της διανομής ή της ανταλλαγής περιεχομένου ηλεκτρονικών επικοινωνιών· συμπεριλαμβάνονται τα δεδομένα που χρησιμοποιούνται για την παρακολούθηση και την ταυτοποίηση της πηγής και του προορισμού μιας επικοινωνίας, τα δεδομένα τοποθεσίας της συσκευής που παράγονται στο πλαίσιο της παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών και της ημερομηνίας, της ώρας, της διάρκειας και του είδους της επικοινωνίας·

[120] Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες), 10.1.2017, COM(2017) 10 final

[121] Βλ. άρθρο 2, περ. 9, ο.π.

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". Σε αυτά συμπεριλαμβάνονται και τα "μεταδεδομένα ηλεκτρονικών επικοινωνιών", όπως ορίζονται στο άρθρο 4 παράγραφος 3 στοιχείο γ' της Πρότασης Κανονισμού για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες. Οι τρεις παραπάνω κατηγορίες δεδομένων συνήθως αναφέρονται από κοινού ως «δεδομένα που δεν αφορούν το περιεχόμενο». Τέλος, ως «δεδομένα περιεχομένου» ορίζονται[122] οποιαδήποτε δεδομένα αποθηκεύονται σε ψηφιακή μορφή, όπως κείμενο, φωνή, βίντεο, εικόνες και ήχος, άλλα από τα δεδομένα συνδρομητή, πρόσβασης ή συναλλαγών.

Από την σκοπιά της παρέμβασης στα θεμελιώδη δικαιώματα η Πρόταση Κανονισμού διαχωρίζει τα δεδομένα σε δυο κατηγορίες: την πρώτη κατηγορία αποτελούν τα "δεδομένα συνδρομητή" και τα "δεδομένα πρόσβασης", ενώ τη δεύτερη τα "δεδομένα συναλλαγών" και τα "δεδομένα περιεχομένου". Στη δεύτερη κατηγορία η παρεμβατικότητα θεωρείται σαφώς μεγαλύτερη[123]. Η διάκριση αυτή έχει αξία όσον αφορά την αρμοδιότητα και τις προϋποθέσεις έκδοσης των Ευρωπαϊκών Εντολών Υποβολής στοιχείων, όπως αναλυτικά εκτίθενται παρακάτω.

Συμπερασματικά, δύο πράγματα θα πρέπει να τονιστούν: αρχικά, ότι όλες οι παραπάνω υποκατηγορίες δεδομένων συνιστούν δεδομένα προσωπικού χαρακτήρα με την έννοια που προσδίδουν σε αυτά ο Γενικός Κανονισμός Προστασίας Δεδομένων[124], η Πρόταση Κανονισμού για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες[125] και η Αστυνομική Οδηγία[126], αφού συνιστούν πληροφορίες που αφορούν ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο και

[122] Βλ. άρθρο 2, περ. 10, ο.π.

[123] Dr. Stanislaw Tosza, The European Commission's Proposal on Cross-Border Access to E-Evidence, eucrim 4/2018, σελ. 214

[124] Βλ. άρθρο 4 παρ. 1, Γενικός Κανονισμός για την Προστασία Δεδομένων

[125] Βλ. άρθρο 4 παρ. 1 περ. Α' Πρότασης Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες), 10.1.2017, COM(2017) 10 final

[126] Βλ. άρθρο 3 περ. 1 Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου, ΕΕ L 119/89 της 4.5.2016

κατά συνέπεια εμπίπτουν στο προστατευτικό πεδίο των παραπάνω νομοθετημάτων. Επιπλέον, απαραίτητη είναι η επισήμανση ότι οι δυο νέοι θεσμοί που περιλαμβάνονται στην Πρόταση Κανονισμού αποτελούν ερευνητικές πράξεις στα πλαίσια ποινικών διαδικασιών και αφορούν συγκεκριμένη κάθε φορά ποινική διαδικασία. Η σύνδεση με συγκεκριμένη έρευνα τις διαχωρίζει από τα προληπτικά μέτρα ή τις υποχρεώσεις διατήρησης δεδομένων που προβλέπονται από τον νόμο και διασφαλίζει την εφαρμογή των δικονομικών δικαιωμάτων που ισχύουν σε ποινικές διαδικασίες[127]. Η Πρόταση Κανονισμού ρυθμίζει τη συλλογή μόνο των αποθηκευμένων δεδομένων, δηλαδή των δεδομένων που τηρεί ο Πάροχος Υπηρεσιών κατά τον χρόνο παραλαβής του Πιστοποιητικού Ευρωπαϊκής Εντολής Υποβολής ή Διατήρησης στοιχείων. Δεν προβλέπει γενική υποχρέωση διατήρησης των δεδομένων, ούτε επιτρέπει την υποκλοπή δεδομένων ή τη συλλογή δεδομένων που θα αποθηκευτούν σε μελλοντικό χρονικό σημείο σε σχέση με τον χρόνο παραλαβής του Πιστοποιητικού Εντολής Υποβολής ή Διατήρησης στοιχείων[128]. Ως εκ τούτου δε θα πρέπει οι υποχρεώσεις των Παρόχων, που απορρέουν από αυτόν τον Κανονισμό, να συγχέονται με τις υποχρεώσεις των Παρόχων για την διατήρηση των δεδομένων επικοινωνιών[129].

ΙΙ. Η Ευρωπαϊκή Εντολή Υποβολής (ΕΕΥ) στοιχείων

i. Ορισμός

Σύμφωνα με τους ορισμούς της Πρότασης Κανονισμού[130], ως Ευρωπαϊκή Εντολή Υποβολής στοιχείων ορίζεται η δεσμευτική απόφαση Αρχής Έκδοσης Κράτους - Μέλους της ΕΕ, η οποία υποχρεώνει Πάροχο Υπηρεσιών, που παρέχει υπηρεσίες στην Ένωση και είναι εγκατεστημένος ή εκπροσωπείται σε άλλο Κράτος-Μέλος, να υποβάλλει ηλεκτρονικά αποδεικτικά στοιχεία. Με την έννοια "άλλο Κράτος-Μέλος" νοείται Κράτος-Μέλος διαφορετικό από αυτό, στο οποίο ανήκει η Αρχή Έκδοσης. Η παρούσα Πρόταση Κανονισμού έχει εφαρμογή μόνο στις περιπτώσεις, στις οποίες ο πάροχος της υπηρεσίας είναι εγκατεστημένος ή

[127] Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής με θέματα «Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις», ΕΕ C 367/90 της 10.10.2018

[128] Αιτιολογική Σκέψη (19) της Πρότασης Κανονισμού Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις

[129] Νόμος 3917/2011, ΦΕΚ Α' 22/21-2-2011

[130] Βλ. άρθρο 2 Πρότασης Κανονισμού

εκπροσωπείται σε άλλο Κράτος-Μέλος. Οι εντολές που προβλέπονται από τον Κανονισμό, δεν μπορούν να χρησιμοποιηθούν για εγχώριες έρευνες. Συνεπώς, ο Κανονισμός δε θα πρέπει να περιορίζει τις εξουσίες των αρμόδιων εθνικών αρχών που ήδη προβλέπονται από την εθνική νομοθεσία, ώστε να υποχρεώνουν σε συμμόρφωση τους παρόχους υπηρεσιών που είναι εγκατεστημένοι ή εκπροσωπούνται στην επικράτειά τους[131].

ii. Οι προϋποθέσεις για την έκδοση ΕΕΥ

Η έκδοση ΕΕΥ στοιχείων, με τις οποίες ζητείται η υποβολή "δεδομένων συνδρομητή" ή "δεδομένων πρόσβασης", επιτρέπεται αρχικά για οποιοδήποτε αδίκημα, υπό την προϋπόθεση όμως ότι είναι αναγκαία και αναλογική και ότι διατίθεται παρόμοιο μέτρο για το ίδιο ποινικό αδίκημα σε συγκρίσιμη εγχώρια κατάσταση στο Κράτος Έκδοσης[132]. Ειδικά για τις ΕΕΥ στοιχείων με τις οποίες ζητείται η υποβολή "δεδομένων συναλλαγών" ή "δεδομένων περιεχομένου" θα πρέπει να συντρέχει επιπλέον κάποια από τις παρακάτω προϋποθέσεις: είτε α) θα πρέπει αυτές να αφορούν ποινικά αδικήματα, που επισύρουν στο κράτος έκδοσης στερητική της ελευθερίας ποινή με ανώτατο όριο τουλάχιστον τριών ετών, ή β) να αφορούν τα αδικήματα του άρθρου 3, 4 και 5 της Απόφασης-Πλαισίου 2001/413/ΔΕΥ[133], τα αδικήματα των άρθρων 3 έως 7 της Οδηγίας 2011/93/ΕΕ[134], τα αδικήματα των άρθρων 3 έως 8 της Οδηγίας 2013/40/ΕΕ[135], εφόσον αυτά διαπράχθηκαν εν όλω ή εν μέρει μέσω πληροφοριακού συστήματος ή γ) να αφορούν τα εγκλήματα των άρθρων 3 έως 12 και του άρθρου 14 της Οδηγίας (ΕΕ)

[131] Βλ. Αιτιολογική Σκέψη (15), ο.π.

[132] Βλ. άρθρο 5 παρ. 1, 2, 3, ο.π.

[133] Η Απόφαση-Πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου, της 28ης Μαΐου 2001, "για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών" (ΕΕ L 149/1 της 2.6.2001) έχει ήδη αντικατασταθεί από την Οδηγία (ΕΕ) 2019/713 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, "για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών και την αντικατάσταση της απόφασης-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου", ΕΕ L 123/18 της 10.5.2019, και ως εκ τούτου απαιτείται στο σημείο αυτό επικαιροποίηση της Πρότασης Κανονισμού

[134] Οδηγία 2011/92/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 2011, σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου, ΕΕ L 335/1 της 17.12.2011

[135] Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ΕΕ L 218/8 της 14.8.2013

2017/541[136]. Από τις τρεις αυτές προϋποθέσεις, οι οποίες δεν πρέπει να συντρέχουν σωρευτικά, η πρώτη σχετίζεται με το εθνικό δίκαιο του Κράτους Έκδοσης, ενώ η δεύτερη και τρίτη αναφέρονται σε Ευρωπαϊκές Οδηγίες και Αποφάσεις-Πλαισίου, ανεξάρτητα από το ύψος της απειλούμενης ποινής στο εθνικό δίκαιο του Κράτους Έκδοσης. Επιπλέον, προτού εκδώσει ΕΕΥ στοιχείων, η Αρχή Έκδοσης πρέπει να λαμβάνει υπόψη τυχόν ασυλίες και προνόμια με τα οποία μπορεί να προστατεύονται τα ζητούμενα δεδομένα, σύμφωνα με το δίκαιο του Κράτους - Μέλους του Παρόχου Υπηρεσιών ή τυχόν επιπτώσεις στα θεμελιώδη συμφέροντα του Κράτους-Μέλους, όπως η εθνική ασφάλεια και άμυνα. Οι ασυλίες και τα προνόμια, που ενδέχεται να αφορούν κατηγορίες προσώπων (όπως διπλωμάτες) ή ειδικά προστατευόμενες σχέσεις (όπως το δικηγορικό απόρρητο), αναφέρονται και σε άλλες πράξεις αμοιβαίας αναγνώρισης, όπως η Ευρωπαϊκή Εντολή Έρευνας[137].

iii. Η αρμόδια Αρχή Έκδοσης ΕΕΥ

Η ΕΕΥ στοιχείων για "δεδομένα συναλλαγών" και "δεδομένα περιεχομένου" μπορεί να εκδοθεί από δικαστή, δικαστήριο και ανακριτή με αρμοδιότητα στη συγκεκριμένη υπόθεση[138]. ΕΕΥ στοιχείων που αφορά στα παραπάνω δεδομένα εκδίδεται επίσης από κάθε άλλη αρμόδια αρχή, η οποία στη συγκεκριμένη υπόθεση ενεργεί ως ανακριτική αρχή με αρμοδιότητα να διατάσσει τη συγκέντρωση αποδεικτικών στοιχείων, σύμφωνα με το εθνικό δίκαιο του Κράτους-Μέλους, αφού όμως προηγουμένως εξεταστεί ότι συντρέχουν οι απαιτούμενες προϋποθέσεις για την έκδοσή της και εγκριθεί αυτή από δικαστή, δικαστήριο ή ανακριτή του Κράτους Έκδοσης[139]. Από την άλλη, η ΕΕΥ στοιχείων που αφορά "δεδομένα συνδρομητή" και "δεδομένα πρόσβασης" εκδίδεται από τα ίδια πρόσωπα και υπό τις ίδιες προϋποθέσεις που ισχύουν για τις ΕΕΥ στοιχείων για "δεδομένα συναλλαγών" και "δεδομένα περιεχομένου", αλλά επιπρόσθετα, οι τελευταίες δύναται να εκδίδονται ή να εγκρίνονται και από εισαγγελέα με αρμοδιότητα στη συγκεκριμένη υπόθεση[140]. Καθώς τα "δεδομένα συνδρομητή" και τα "δεδομένα πρόσβασης" θεωρούνται λιγότερο ευαίσθητα, οι ΕΕΥ στοιχείων, με τις οποίες ζητείται η γνωστοποίησή τους,

[136] Οδηγία (ΕΕ) 2017/541 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2017, για την καταπολέμηση της τρομοκρατίας και την αντικατάσταση της απόφασης-πλαισίου 2002/475/ΔΕΥ του Συμβουλίου και για την τροποποίηση της απόφασης 2005/671/ΔΕΥ του Συμβουλίου, ΕΕ L 88/6 της 31.3.2017

[137] Αιτιολογική σκέψη (35) Πρότασης Κανονισμού

[138] Βλ. άρθρο 4 παρ. 2 περ. α' Πρότασης Κανονισμού

[139] Βλ. άρθρο 4 παρ. 2 περ. α', ο.π.

[140] Βλ. άρθρο 4 παρ. 1 περ. α', ο.π.

μπορούν να εκδίδονται ή να εγκρίνονται και από τους αρμόδιους εισαγγελείς. Από την άλλη, η ιδιαίτερη αντιμετώπιση των "δεδομένων συναλλαγών" και των "δεδομένων περιεχομένου", καθώς και οι αυξημένες προϋποθέσεις που θέτει ο Νομοθέτης για την έκδοση των ΕΕΥ, με τις οποίες ζητούνται αυτά, δικαιολογούνται από το γεγονός ότι αυτά θεωρούνται περισσότερο ευαίσθητα.

iv. Το περιεχόμενο των ΕΕΥ

Η ΕΕΥ στοιχείων πρέπει να περιλαμβάνει τις ακόλουθες πληροφορίες[141]: την αρχή έκδοσης, τον αποδέκτη, τα πρόσωπα των οποίων τα δεδομένα ζητούνται, την κατηγορία των ζητούμενων δεδομένων, το χρονικό διάστημα για το οποίο ζητείται η υποβολή, τις ισχύουσες διατάξεις του ποινικού δικαίου του Κράτους Έκδοσης, σε περίπτωση έκτακτης ανάγκης ή αιτήματος να πραγματοποιηθεί νωρίτερα η γνωστοποίηση τους λόγους στους οποίους συνίσταται αυτά, σε περίπτωση που τα ζητούμενα δεδομένα αποθηκεύονται ή υποβάλλονται σε επεξεργασία ως μέρος υποδομής που παρέχεται από Πάροχο Υπηρεσιών σε εταιρεία ή άλλη οντότητα που δεν είναι φυσικό πρόσωπο, επιβεβαίωση ότι η εντολή συμμορφώνεται με την παράγραφο 6 του άρθρου 5 της Πρότασης Κανονισμού και τέλος τους λόγους ως προς την αναγκαιότητα και την αναλογικότητα του μέτρου. Οι ΕΕΥ 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 Πρόταση Οδηγίας σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον διορισμό νόμιμων εκπροσώπων με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών. Η διαβίβαση θα πρέπει να έχει τη μορφή Πιστοποιητικού Ευρωπαϊκής Εντολής Υποβολής στοιχείων ("Πιστοποιητικό ΕΕΥ"), σύμφωνα με το Παράρτημα Ι της Πρότασης Κανονισμού[142].

III. Η Ευρωπαϊκή Εντολή Διατήρησης (ΕΕΔ) στοιχείων

i. Ορισμός

Ως «ευρωπαϊκή εντολή διατήρησης στοιχείων», σύμφωνα με τους ορισμούς της Πρότασης Κανονισμού[143], νοείται η δεσμευτική απόφαση αρχής έκδοσης Κράτους Μέλους, η

[141] Βλ. άρθρο 5 παρ. 5, ο.π.
[142] Βλ. άρθρο 8, ο.π.
[143] Βλ. άρθρο 2, ο.π.

οποία υποχρεώνει πάροχο υπηρεσιών που παρέχει υπηρεσίες στην Ένωση και είναι εγκατεστημένος ή εκπροσωπείται σε άλλο Κράτος-Μέλος, να διατηρήσει ηλεκτρονικά αποδεικτικά στοιχεία ενόψει επακόλουθου αιτήματος υποβολής τους. Όπως συνάγεται από τον ορισμό και επιβεβαιώνεται από την Αιτιολογική Έκθεση[144] του Κανονισμού σκοπός της είναι να αποτρέψει την αφαίρεση, τη διαγραφή ή την αλλοίωση των σχετικών δεδομένων σε περιπτώσεις, όπου ενδέχεται να χρειαστεί περισσότερος χρόνος για να διασφαλιστεί η υποβολή τους, για παράδειγμα επειδή θα χρησιμοποιηθούν δίαυλοι δικαστικής συνεργασίας.

ii. Οι προϋποθέσεις για την έκδοση ΕΕΔ

Μια ΕΕΔ με την οποία ζητείται η διατήρηση στοιχείων εκδίδεται για οποιοδήποτε ποινικό αδίκημα, υπό τον μοναδικό όρο ότι είναι απαραίτητη και αναλογική[145]. Ο λόγος που δικαιολογεί την επιλογή αυτή του Νομοθέτη είναι ότι η Ευρωπαϊκή Εντολή Έρευνας μπορεί να εκδοθεί για οποιοδήποτε αδίκημα, χωρίς να περιορίζεται σε συγκεκριμένα όρια[146]. Η θέσπιση ορίων αναφορικά με την έκδοση ΕΕΔ θα οδηγούσε τις αρμόδιες Αρχές στην έκδοση ΕΕΕ αντί ΕΕΔ με αποτέλεσμα το εν λόγω μέσο να καθίσταται αναποτελεσματικό. Επιπλέον, καθώς η ΕΕΔ στοιχείων συνεπάγεται σαφώς μικρότερη επέμβαση στα θεμελιώδη δικαιώματα του ανθρώπου σε σχέση με τις ΕΕΥ στοιχείων, δικαιολογούνται και οι μειωμένες απαιτήσεις για την έκδοση της.

iii. Η αρμόδια Αρχή Έκδοσης ΕΕΔ

Αναφορικά με την αρμόδια Αρχή για την έκδοση ΕΕΔ στοιχείων ισχύει ότι και για τις ΕΕΥ στοιχείων, με τις οποίες ζητούνται "δεδομένα συνδρομητή" και "δεδομένα πρόσβασης". Δηλαδή, αυτή εκδίδεται από δικαστή, δικαστήριο, ανακριτή ή εισαγγελέα με αρμοδιότητα στη συγκεκριμένη υπόθεση ή 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 συλλογή αποδεικτικών στοιχείων, σύμφωνα με το εθνικό δίκαιο. Στη δεύτερη περίπτωση, δικαστής, δικαστήριο, ανακριτής ή εισαγγελέας με αρμοδιότητα στη συγκεκριμένη

[144] Αιτιολογική Έκθεση της Πρότασης Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις, COM(2018) 225 final, σελ. 21

[145] Βλ. άρθρο 6 παρ. 2, ο.π.

[146] Αιτιολογική Έκθεση, ο.π.

υπόθεση του Κράτος Έκδοσης θα πρέπει να εγκρίνει την ΕΕΔ στοιχείων, αφού διαπιστώσει τη συμμόρφωσή της με τις προϋποθέσεις για την έκδοσή της, σύμφωνα με τον Κανονισμό[147].

iv. Το περιεχόμενο των ΕΕΔ

Μια ΕΕΔ στοιχείων θα πρέπει να περιέχει τις ακόλουθες πληροφορίες[148]: την αρχή έκδοσης, τον αποδέκτη, τα πρόσωπα των οποίων τα δεδομένα ζητείται να διατηρηθούν, την κατηγορία των προς διατήρηση δεδομένων, το χρονικό διάστημα για το οποίο ζητείται η διατήρηση, τις ισχύουσες διατάξεις του ποινικού δικαίου του Κράτους Έκδοσης και τους λόγους ως προς την αναγκαιότητα και την αναλογικότητα του μέτρου. Όπως ακριβώς ισχύει για τις ΕΕΥ, έτσι και οι ΕΕΔ 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 Πρόταση Οδηγίας 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 πρέπει να έχει τη μορφή Πιστοποιητικού Ευρωπαϊκής Εντολής Διατήρησης στοιχείων («Πιστοποιητικό ΕΕΔ»), σύμφωνα με το Παράρτημα ΙΙ της Πρότασης Κανονισμού[149].

IV. Η υποβολή και η εκτέλεση των ΕΕΥ και ΕΕΔ στην πράξη

Σε αδρές γραμμές, η διαδικασία έκδοσης και εκτέλεσης των Ευρωπαϊκών Εντολών Υποβολής ή Διατήρησης στοιχείων, σύμφωνα με τον Κανονισμό, φαίνεται να είναι η ακόλουθη: Ανάλογα με το είδος των ζητούμενων δεδομένων και το είδος της εντολής, η αρμόδια δικαστική αρχή (Αρχή Έκδοσης) εκδίδει ή εγκρίνει την εντολή, σύμφωνα με τις προϋποθέσεις που αναφέρθηκαν ανωτέρω και αποστέλλει την εντολή μέσω του εναρμονισμένου Πιστοποιητικού στον νόμιμο εκπρόσωπο του Παρόχου Υπηρεσιών ή σε οποιαδήποτε εγκατάστασή του εντός της ΕΕ (Αποδέκτης).

Πιο συγκεκριμένα, όσον αφορά την αρμοδιότητα, τόσο στην έκδοση ΕΕΥ όσο και ΕΕΔ, πρέπει πάντα να συμμετέχει δικαστική αρχή, είτε ως αρχή έκδοσης είτε ως αρχή έγκρισης, προκειμένου να εξασφαλίζονται οι απαραίτητες εγγυήσεις. Ειδικότερα, προκειμένου για ΕΕΥ

[147] Βλ. άρθρο 4 παρ. 3, ο.π.
[148] Βλ. άρθρο 6 παρ.3, ο.π.
[149] Βλ. άρθρο 8, ο.π.

“δεδομένων συναλλαγών” και “δεδομένων περιεχομένου”, η δικαστική αρχή έκδοσης ή έγκρισης πρέπει να είναι υποχρεωτικά δικαστής, ανακριτής ή δικαστήριο. Για ΕΕΥ “δεδομένων συνδρομητή” και “δεδομένων πρόσβασης”, καθώς επίσης και για τις ΕΕΔ στοιχείων, η εν λόγω αρχή έκδοσης ή έγκρισης μπορεί να είναι και ο αρμόδιος στη συγκεκριμένη υπόθεση εισαγγελέας. Από τα παραπάνω συνάγεται ότι στην έννοια των δικαστικών αρχών με αρμοδιότητα έκδοσης ΕΕΥ και ΕΕΔ ηλεκτρονικών αποδεικτικών στοιχείων στην Ελλάδα υπάγονται α) τα ποινικά δικαστήρια μέσω της αναβολής για κρείσσονες αποδείξεις (α. 352 παρ. 3 νΚΠΔ), β) οι ανακριτές, γ) οι αρμόδιοι στη συγκεκριμένη υπόθεση εισαγγελείς, προκειμένου για ΕΕΔ και ΕΕΥ “δεδομένων συνδρομητή” και “δεδομένων πρόσβασης”, εκτός δηλαδή από τις περιπτώσεις των ΕΕΥ που αφορούν στοιχεία “δεδομένων συναλλαγών” και “δεδομένων περιεχομένου” και δ) οι ανακριτικοί υπάλληλοι, όπως οι πταισματοδίκες και ειρηνοδίκες (α. 31 παρ. 1 περ. α΄ νΚΠΔ), που είναι δικαστικοί λειτουργοί, όχι όμως άλλοι γενικοί ή ειδικοί ανακριτικοί υπάλληλοι, που δεν έχουν την ιδιότητα του δικαστή, όπως οι αστυνομικοί (α. 31 παρ. 1 περ. β΄ νΚΠΔ) και οι ειδικοί ανακριτικοί υπάλληλοι (α. 31 παρ. 1 περ. γ΄ νΚΠΔ). Όταν στους τελευταίους -μη δικαστικούς- γενικούς ανακριτικούς υπαλλήλους (α. 31 παρ. 1 περ. β΄ νΚΠΔ) και ειδικούς ανακριτικούς υπαλλήλους (α. 31 παρ. 1 περ. γ΄ νΚΠΔ) προκύψουν οι κατά νόμο προϋποθέσεις έκδοσης ΕΕΥ και ΕΕΔ στα πλαίσια άσκησης των ανακριτικών τους καθηκόντων σε συγκεκριμένη υπόθεση στην ποινική προδικασία, αυτοί έχουν αρμοδιότητα να εκδώσουν την αντίστοιχη εντολή υπό την προϋπόθεση ότι αυτή θα επικυρωθεί από δικαστική αρχή με αρμοδιότητα να εκδίδει ΕΕΥ και ΕΕΔ, αφού διαπιστωθεί μετά από έλεγχο, ότι συνέτρεχαν στην προκειμένη περίπτωση οι προϋποθέσεις για την έκδοσή τους, όπως αναλυτικά αναφέρονται παραπάνω[150].

Στη συνέχεια, τόσο η ΕΕΥ όσο και η ΕΕΔ στοιχείων, διαβιβάζονται απευθείας στον Αποδέκτη (Πάροχο Υπηρεσιών) μέσω του Πιστοποιητικού ΕΕΥ και του Πιστοποιητικού ΕΕΔ αντίστοιχα, με οποιοδήποτε μέσο δίνει τη δυνατότητα γραπτής τεκμηρίωσης, όπως για παράδειγμα με συστημένη επιστολή, με ασφαλές ηλεκτρονικό μήνυμα και πλατφόρμες ή άλλους ασφαλείς διαύλους[151], σύμφωνα με τα αντίστοιχα υποδείγματα που παρέχονται στα

[150] Κατ’ αναλογία με Σταμάτη Δασκαλόπουλο, Ευρωπαϊκή Εντολή Έρευνας (Ε.Ε.Ε.): Ο νέος θεσμός Δικαστικής Συνεργασίας επί ποινικών υποθέσεων εντός της Ευρωπαϊκής Ένωσης, ΠοινΧρ 2018, σελ. 173

[151] Αιτιολογική Σκέψη (39), ο.π.

Παραρτήματα Ι και ΙΙ της Πρότασης Κανονισμού[152]. Αξίζει να σημειωθεί 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 πρέπει να εμποδίζεται από τον Κανονισμό, αφ' ης στιγμής επιτρέπουν την υποβολή των Πιστοποιητικών ΕΕΥ και ΕΕΔ στη μορφή που προβλέπεται στα σχετικά Παραρτήματα της Πρότασης Κανονισμού, χωρίς να ζητούνται περισσότερα στοιχεία σχετικά με την εντολή[153]. Τέλος, αναφορικά με το περιεχόμενο των Πιστοποιητικών, αυτά θα πρέπει να περιέχουν τις ίδιες υποχρεωτικές πληροφορίες με τις εντολές, εκτός από τους λόγους της αναγκαιότητας και της αναλογικότητας του μέτρου ή περαιτέρω πληροφορίες σχετικά με την υπόθεση, ώστε να αποτραπεί ο κίνδυνος υπονόμευσης των ερευνών[154].

Μετά την παραλαβή του Πιστοποιητικού ΕΕΥ ή ΕΕΔ, ο Αποδέκτης εκτελεί την εντολή, δηλαδή διαβιβάζει τα δεδομένα εντός 10 ημερών[155], (ή εντός 6 ωρών σε περίπτωση έκτακτης ανάγκης[156]) ή τα διατηρεί για μέγιστο χρονικό διάστημα 60 ημερών[157] αντίστοιχα, εκτός εάν η εκτέλεση της εντολής δεν είναι δυνατή, επειδή το Πιστοποιητικό παρουσιάζει ελλείψεις ή για λόγους ανωτέρας βίας ή πραγματικής αδυναμίας του Αποδέκτη, ή σε περίπτωση άρνησης του Αποδέκτη λόγω συγκρουόμενων υποχρεώσεων, είτε όσον αφορά τα θεμελιώδη δικαιώματα ή τα θεμελιώδη συμφέροντα τρίτης χώρας είτε για άλλους λόγους. Για τις περιπτώσεις αυτές προβλέπεται μια διαδικασία "διαλόγου" μεταξύ των Παρόχων Υπηρεσιών και της Αρχής Έκδοσης, ώστε να δίνεται η δυνατότητα στους πρώτους να αντιμετωπίζουν τις παραπάνω καταστάσεις. Όταν συντρέχει τέτοια περίπτωση, ο Πάροχος ενημερώνει την Αρχή Έκδοσης χωρίς αδικαιολόγητη καθυστέρηση χρησιμοποιώντας το σχετικό υπόδειγμα του Παραρτήματος ΙΙΙ της Πρότασης Κανονισμού. Η Αρχή Έκδοσης επανεξετάζει την εντολή υπό το πρίσμα των πληροφοριών που παρασχέθηκαν από τον Πάροχο, και αν πληρούνται οι προϋποθέσεις, διορθώνει ή ανακαλεί το Πιστοποιητικό.

Σε περίπτωση που ο αποδέκτης δεν συμμορφωθεί με την παραληφθείσα εντολή αναιτιολόγητα, προβλέπονται διαδικασίες για την εκτέλεση της εντολής από αρμόδια Αρχή

[152] Βλ. άρθρο 8, ο.π.
[153] Βλ. Αιτιολογική Έκθεση, ο.π.
[154] Βλ. Αιτιολογική Σκέψη (38), ο.π.
[155] Βλ. άρθρο 9 παρ. 1, ο.π.
[156] Βλ. άρθρο 9 παρ. 2, ο.π
[157] Βλ. άρθρο 10 παρ. 1, ο.π

Εκτέλεσης στο Κράτος Μέλος, στο οποίο εκπροσωπείται ή είναι εγκατεστημένος ο Πάροχος Υπηρεσιών. Με τον τρόπο αυτό οι εν λόγω θεσμοί μετατρέπονται σε θεσμούς "παραδοσιακής" αμοιβαίας αναγνώρισης, όπου πλέον μια Δημόσια Αρχή παίζει τον ρόλο του Αποδέκτη της Εντολής[158]. Τα Κράτη Μέλη οφείλουν, με την επιφύλαξη της εθνικής νομοθεσίας που προβλέπει επιβολή ποινικών κυρώσεων, να θεσπίσουν κανόνες που να περιλαμβάνουν αποτελεσματικές, αναλογικές και αποτρεπτικές χρηματικές κυρώσεις που θα επιβάλλονται στους Παρόχους για τυχόν παραβάσεις των υποχρεώσεών τους[159]. Σε εθνικό επίπεδο, τέτοιου είδους κυρώσεις εναντίον Παρόχων Υπηρεσιών για παραβάσεις των υποχρεώσεών τους, αναφορικά με τον ορισμό νομίμου εκπροσώπου και την απόκριση σε αιτήσεις παροχής πληροφοριών, προβλέφθηκαν στη Γερμανία με τον Netzwerkdurchsetzungsgesetz (NetzDG)[160], ο οποίος προβλέπει πρόστιμα ύψους έως 500.000 ευρώ για τις παραβάσεις αυτές[161].

Καθώς οι θεσμοί ΕΕΥ και ΕΕΔ επηρεάζουν θεμελιώδη δικαιώματα του προσώπου, του οποίου τα δεδομένα προσπελαύνονται, όπως είναι το δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα και το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής, όπως επίσης και δικαιώματα των Παρόχων Υπηρεσιών, ιδίως την επιχειρηματική ελευθερία, για την προστασία των παραπάνω θεμελιωδών δικαιωμάτων, προβλέπονται, υπό το πρίσμα του δικαιώματος δικαστικής προστασίας, στο 4ο Κεφάλαιο της Πρότασης Κανονισμού με τίτλο "μέσα έννομης προστασίας", διαδικασίες ελέγχου από αρμόδιο δικαστήριο, τόσο υπέρ των παρόχων όσο και υπέρ των υπόπτων, των κατηγορουμένων και κάθε άλλου Υποκειμένου, των οποίων τα δεδομένα υφίστανται επεξεργασία.

Με βάση τα παραπάνω, σε περίπτωση που ο Αποδέκτης προβάλει αιτιολογημένη ένσταση κατά της εντολής για λόγους συγκρουόμενων υποχρεώσεων[162], η Αρχή Έκδοσης παραπέμπει την υπόθεση σε αρμόδιο δικαστήριο του οικείου Κράτους-Μέλους, το οποίο είναι

---

[158] Dr. Stanislaw Tosza, The European Commission's Proposal on Cross-Border Access to E-Evidence, eucrim 4/2018, σελ. 216

[159] Άρθρο 13, ο.π.

[160] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken. Για περισσότερες πληροφορίες σχετικά βλ. και Δ. Καραγκούνη, Η επιβολή περιορισμών στα μέσα κοινωνικής δικτύωσης μετά τον νέο γερμανικό Νόμο περί Βελτίωσης της Επιβολής της Νομοθεσίας στα Κοινωνικά Δίκτυα (Netzwerkdurchsetzungsgesetz) - Επίθεση στην ελευθερία έκφρασης ή αναγκαίο μέσο καταπολέμησης της διαδικτυακής εγκληματικότητας;, σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, εκδ. Νομική Βιβλιοθήκη, 2019, σελ. 223

[161] § 4(1) αριθμ. 7, 8 και § 4(2) NetzDG

[162] Άρθρα 15 και 16, Πρόταση Κανονισμού

στη συνέχεια αρμόδιο να εκτιμήσει την πιθανή σύγκρουση και να κάνει δεκτή την εντολή, εφόσον κρίνει ότι δεν υφίσταται σύγκρουση[163]. Εάν υφίσταται σύγκρουση υποχρεώσεων, που αφορούν τα θεμελιώδη δικαιώματα ή τα θεμελιώδη συμφέροντα τρίτης χώρας[164], το αρμόδιο δικαστήριο απευθύνεται στις κεντρικές αρχές της τρίτης χώρας, μέσω των εθνικών κεντρικών αρχών του, τάσσοντας προθεσμία 15 ημερών για την απάντηση, η οποία μπορεί να παραταθεί κατά 30 ημέρες κατόπιν αιτιολογημένου αιτήματος. Όταν συντρέχουν άλλοι λόγοι άρνησης, τους οποίους επικαλείται ο Αποδέκτης[165], αποφαίνεται το ίδιο αν θα κάνει δεκτή ή θα αποσύρει την εντολή. Περαιτέρω, στο άρθρο 17 της Πρότασης Κανονισμού διασφαλίζεται ότι τα πρόσωπα που επηρεάζονται από την ΕΕΥ στοιχείων, όπως για παράδειγμα οι ύποπτοι, οι κατηγορούμενοι, αλλά και τρίτοι, έχουν στη διάθεσή τους μέσα αποτελεσματικής έννομης προστασίας. Τα εν λόγω μέσα έννομης προστασίας ασκούνται στο Κράτος Έκδοσης, σύμφωνα με το εθνικό δίκαιο.

V. Προβληματισμοί σχετικά με τις Προτάσεις

i. Αναφορικά με τη νομική βάση

Η πρώτη και βασικότερη επιφύλαξη που εκφράζεται αφορά την ίδια τη νομική θεμελίωση του Κανονισμού. Η προτεινόμενη νομική βάση όσον αφορά το σχέδιο Κανονισμού για τα ηλεκτρονικά αποδεικτικά στοιχεία, όπως προαναφέρθηκε, είναι το άρθρο 82 της ΣΛΕΕ, σχετικά με τη δικαστική συνεργασία σε ποινικές υποθέσεις. Η νομική αυτή βάση όμως δεν έχει μέχρι πρότινος χρησιμοποιηθεί ξανά για την υιοθέτηση ενός νομοθετικού κειμένου που θα επιτρέπει την απευθείας πρόσβαση των Αρχών σε δεδομένα πολιτών άλλων Κρατών-Μελών[166]. Έτσι, ένας βασικός προβληματισμός που ανακύπτει ως συνέπεια από την εξέλιξη αυτή, σχετίζεται με την "παράκαμψη" των δημοσίων αρχών του Κράτους Εκτέλεσης, οι οποίες ελέγχοντας κάθε φορά αν πληρούνται οι προϋποθέσεις των ζητουμένων από τα Κράτη Έκδοσης αιτήσεων, λειτουργούσαν ως "φίλτρο" νομιμότητας για την εκτέλεση της ζητούμενης διαδικασίας[167]. Κατά αποτέλεσμα της "παράκαμψης" αυτής, με τις ΕΕΥ στοιχείων δύναται να ζητούνται απευθείας από τους ιδιώτες Παρόχους Υπηρεσιών δεδομένα Υποκειμένων άλλων

[163] Άρθρο 15 παρ. 5 εδ. α' και άρθρο 16 παρ. 5 εδ. Α', ο.π.
[164] Άρθρο 15 παρ. 5 εδ. β' και γ', ο.π.
[165] Άρθρο 16 παρ. 5 εδ. β', ο.π.
[166] Meijers Committee, CM1809 Comments on the proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters, 18 July 2018
[167] Council of Bars and Law Societies of Europe (CCBE), CCBE position on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, 19/10/2018

Κρατών-Μελών, χωρίς να ενημερώνονται οι αρμόδιες Δημόσιες Αρχές αυτών, ακόμα και στην περίπτωση των (πιο ευαίσθητων) "δεδομένων περιεχομένου". Με άλλες λέξεις, οι δημόσιες αρχές του Κράτους Έκδοσης θα μπορούν να λαμβάνουν κάθε είδους δεδομένων απευθείας από τον εκάστοτε Πάροχο Υπηρεσιών χωρίς τις εγγυήσεις που θα παρείχε ο έλεγχος από τις Δημόσιες Αρχές του Κράτους Εκτέλεσης. Επιπλέον, η επιλογή να αφήνεται αποκλειστικά σε ιδιώτες (Παρόχους) η κρίση για το αν συντρέχει ή όχι περίπτωση παραβίασης θεμελιωδών δικαιωμάτων δε φαίνεται να προσφέρει επαρκείς εγγυήσεις για τα δικαιώματα των υπόπτων, των κατηγορουμένων και άλλων προσώπων που επηρεάζονται από την εκτέλεση των παραπάνω εντολών[168]. Ο φόβος αυτός ενισχύεται και από τις σύντομες προθεσμίες, εντός των οποίων οφείλει ο Πάροχος να εκτελέσει την ΕΕΥ. Όπως αναφέρθηκε ήδη παραπάνω, βασικός στόχος της Πρότασης Κανονισμού και της Πρότασης Οδηγίας είναι η δραστική μείωση των καθυστερήσεων στις διαδικασίες που περιλαμβάνουν ηλεκτρονικά αποδεικτικά μέσα και τηρούνται από Παρόχους Υπηρεσιών που είναι εγκατεστημένοι σε άλλη έννομη τάξη. Η προθεσμία των 10 ημερών (ή 6 ωρών κατά περίπτωση) που προβλέπεται στις προτάσεις για τα ηλεκτρονικά αποδεικτικά στοιχεία όσον αφορά την εκτέλεση του πιστοποιητικού ΕΕΥ στοιχείων, δεν παρέχει στους Παρόχους ικανό χρόνο εξέτασης της αίτησης και κατά συνέπεια δεν επιτρέπει να διαπιστωθεί με ορθό τρόπο, αν το πιστοποιητικό ΕΕΥ πληροί όλα τα κριτήρια και αν έχει συμπληρωθεί σωστά[169].

ii. Αναφορικά με τη διάκριση των δεδομένων

Οι τέσσερις προτεινόμενες κατηγορίες δεδομένων δεν φαίνεται να είναι σαφώς οριοθετημένες[170], ούτε γενικότερα φαίνεται να υπάρχει ομοιομορφία σε σχέση και με άλλα νομοθετικά κείμενα της ΕΕ, ως προς την κατηγοριοποίηση των δεδομένων. Για παράδειγμα, τα "μεταδεδομένα" των ηλεκτρονικών επικοινωνιών περιλαμβάνονται τόσο στην κατηγορία των "δεδομένων πρόσβασης"[171], όσο και στην κατηγορία των "δεδομένων συναλλαγών"[172] με την

[168] Marco Stefan / Gloria González Fuster, Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters - State of the art and latest developments in the EU and the US, CEPS Paper in Liberty and Security in Europe, 07/2018, σελ. 34

[169] Βλ. Γνωμοδότηση 23/2018 του Συμβουλίου Προστασίας Δεδομένων σχετικά με τις προτάσεις της Επιτροπής για την Ευρωπαϊκή Εντολή Υποβολής και την Ευρωπαϊκή Εντολή Διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις [άρθρο 70 παράγραφος 1 στοιχείο β)] της 26ης Σεπτεμβρίου 2018

[170] Statement of the Article 29 Working Party, 29 November 2017, Data protection and privacy aspects of cross-border access to electronic evidence

[171] Άρθρο 2 περ. 8 εδ. τελευταίο, ο.π.

προϋπόθεση όμως, ότι αυτά δεν αποτελούν "δεδομένα πρόσβασης"[173]. Επιπλέον, οι διευθύνσεις IP, για παράδειγμα, θα μπορούσαν να χαρακτηριστούν τόσο "δεδομένα συναλλαγών" όσο και "δεδομένα συνδρομητή"[174].

Περαιτέρω, υπάρχουν διάφορες έννοιες στη Νομοθεσία της ΕΕ για τα δεδομένα που επεξεργάζονται οι πάροχοι υπηρεσιών και που μπορεί να ενδιαφέρουν τις Δημόσιες Αρχές επιβολής του νόμου σε ένα Κράτος-Μέλος. Για παράδειγμα, στη Σύμβαση της Βουδαπέστης για το Κυβερνοέγκλημα απαντάται ο όρος "πληροφορίες για συνδρομητές"[175], στην Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες[176] απαντώνται οι όροι "δεδομένα θέσης" και "δεδομένα κίνησης"[177], στην Πρόταση Κανονισμού για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες[178] εντοπίζονται οι όροι "περιεχόμενο ηλεκτρονικών επικοινωνιών" και "μεταδεδομένα ηλεκτρονικών επικοινωνιών"[179]. Επιπλέον, σε καμία Οδηγία, ούτε στον Γενικό Κανονισμό Προστασίας Δεδομένων, αλλά ούτε και στη Σύμβαση της Βουδαπέστης δεν συναντάται η έννοια των "δεδομένων συνδρομητή"[180]. Ως εκ τούτου θα ήταν ωφέλιμο να υπάρξει στο μέλλον μια ευθυγράμμιση όσον αφορά τον ορισμό των κατηγοριών των δεδομένων που ανταλλάσσονται στο πλαίσιο της δικαστικής συνεργασίας[181] και ο καθορισμός μιας σαφούς

---

[172] Βλ., άρθρο 2 περ. 9 εδάφιο τελευταίο, ο.π.

[173] Βλ, άρθρο 2 περ. 9 εδάφιο πρώτο, ο.π.

[174] Βλ. Γνωμοδότηση 23/2018 του Συμβουλίου Προστασίας Δεδομένων, ο.π.

[175] Βλ. Άρθρο 18 Σύμβασης της Βουδαπέστης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (CETS αριθ. 185)

[176] Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών

[177] Βλ. άρθρο 2 περ. Β' και γ', Οδηγία 2002/58/ΕΚ

[178] Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ, COM(2017) 10 final

[179] Βλ. άρθρο 4 παρ. 3 περ. Β' και γ' Πρότασης Κανονισμού για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες

[180] Katalin Ligeti/Gavin Robinson, Cross-Border Access to Electroinc Evidence: Policy and Legislative Challenges, in: Sergio Carrera/Valsamis Mitsilegas, Constitutionalising the Security Union - Effectiveness, Rule of Law and Rights in Countering Terrorism and Crime, σελ. 108

[181] Για την κατηγοριοποίηση των δεδομένων για τους σκοπούς των ποινικών διαδικασιών βλ. Claudia Warken, Classification of Electronic Data for Criminal Law Purposes, eucrim 4/2018, σελ. 226

ιεραρχίας μεταξύ κάθε κατηγορίας δεδομένων ανάλογα με τον βαθμό παρεμβατικότητας στην ιδιωτική ζωή ενός ατόμου[182].

Αξίζει να σταθούμε ιδιαίτερα στην επιλογή του Ευρωπαίου Νομοθέτη να υπαγάγει με ρητή νομοθετική πρόβλεψη τα "μεταδεδομένα" των ηλεκτρονικών επικοινωνιών στην κατηγορία των "δεδομένων πρόσβασης". Το Δικαστήριο της Ευρωπαϊκής Ένωσης έκρινε στην απόφασή του στις συνεκδικασθείσες υποθέσεις C-203/15 και C-698/15, Tele2 Sverige AB, ότι τα μεταδεδομένα, όπως τα "δεδομένα κίνησης" και τα "δεδομένα θέσης", παρέχουν τα μέσα για τον προσδιορισμό του προφίλ των προσώπων, περί των οποίων πρόκειται, πληροφορία εξίσου ευαίσθητη, υπό το πρίσμα του δικαιώματος του σεβασμού της ιδιωτικής ζωής, με το περιεχόμενο αυτό καθεαυτό των επικοινωνιών[183]. Συνεπώς, υποστηρίζεται βάσιμα ότι, με βάση την παραπάνω κρίση του ΔΕΕ, τα "μεταδεδομένα" των ηλεκτρονικών επικοινωνιών θα έπρεπε να κατατάσσονται στην κατηγορία των "δεδομένων περιεχομένου" και όχι των "δεδομένων πρόσβασης". Ο χαρακτηρισμός των μεταδεδομένων των ηλεκτρονικών επικοινωνιών ως "δεδομένων πρόσβασης" αντί "δεδομένων περιεχομένου" δεν έχει μόνο θεωρητική σημασία, καθώς συνεπάγεται, διαφορετική μεταχείριση των εν λόγω δεδομένων και λιγότερες εγγυήσεις σε σχέση με τα "δεδομένα περιεχομένου"[184].

Όπως ήδη αναφέρθηκε παραπάνω, η Πρόταση Κανονισμού διαχωρίζει τα δεδομένα και σε κατηγορίες ανάλογα με την παρέμβαση στα θεμελιώδη δικαιώματα του ατόμου. Η παρεμβατικότητα στην κατηγορία των "δεδομένων συναλλαγών" και τα "δεδομένων περιεχομένου" θεωρείται σαφώς μεγαλύτερη[185] και για τον λόγο αυτό αξιώνεται, ως πρόσθετη εγγύηση για την έκδοση ΕΕΥ που αφορά τέτοιου είδους δεδομένα, τη δυνατότητα λήψης παρόμοιου μέτρου για το ίδιο ποινικό αδίκημα σε ανάλογη κατάσταση στο εθνικό δίκαιο του

[182] Public Consultation on improving cross-border access to electronic evidence, BSA | The Software Alliance's supplemental position paper, October 2017

[183] Βλ. σχετική απόφαση ΔΕΕ της 21ης Δεκεμβρίου 2016, σκέψη 99

[184] Αξίζει να σημειωθεί ότι το ζήτημα του επιπέδου της παρεχόμενης προστασίας των "μεταδεδομένων" των ηλεκτρονικών επικοινωνιών απασχόλησε έντονα και την ελληνική έννομη τάξη. Βλ. σχετικά τις Γνωμοδοτήσεις ΕισΑΠ 09/2009 (Γ. Σανιδάς), 12/2009 (Ι. Τέντες), 09/2011 (Α. Κατσιρώδης), τις αποφάσεις ΑΠ 711/2011 (ΠοινΔικ 2012, 518), ΑΠ 203/2014 (ΠοινΧρ 2015, 103) και την αντίθετη ΣτΕ 1593/2016 (ΔιΜΕΕ 2016, 637, με σημ. Γ. Τσόλια). Για την αξιοποίηση των μεταδεδομένων γενικά βλ. Αναλυτικά Β. Κάτο, Ψηφιακά Πειστήρια, σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, εκδ. Νομική Βιβλιοθήκη, 2019, σελ. 63

[185] Dr. Stanislaw Tosza, The European Commission's Proposal on Cross-Border Access to E-Evidence, eucrim 4/2018, σελ. 214

Κράτους Έκδοσης. Η ρύθμιση αυτή όμως φαίνεται ότι, αντί να παρέχει πρόσθετες εγγυήσεις, ενθαρρύνει τα Κράτη-Μέλη, τα οποία δεν προβλέπουν τέτοια μέτρα, και κατά συνέπεια διαθέτουν υψηλότερο επίπεδο προστασίας στον τομέα των δεδομένων προσωπικού χαρακτήρα, να διευρύνουν τις εθνικές τους δυνατότητες, θεσπίζοντας παρόμοια μέτρα, ώστε να μπορούν να ζητούν την υποβολή δεδομένων συνδρομητή ή πρόσβασης και να εξασφαλίζεται, κατ' επέκταση, η δυνατότητα έκδοσης ΕΕΥ στοιχείων, μειώνοντας όμως έτσι το επίπεδο προστασίας των προσωπικών δεδομένων στην επικράτειά τους.

Επιπλέον, προκειμένου να εκδοθεί μια ΕΕΥ που αφορά -στα πιο ευαίσθητα- "δεδομένα συναλλαγών" ή "δεδομένα περιεχομένου" απαιτείται, όπως ήδη προαναφέρθηκε, το αδίκημα για το οποίο αυτή εκδίδεται, να τιμωρείται στο Κράτος Έκδοσης με στερητική της ελευθερίας ποινή με ανώτατο όριο τουλάχιστον 3 ετών[186]. Το όριο των τριών ετών περιορίζει το πεδίο εφαρμογής της νομικής πράξης στα σοβαρότερα εγκλήματα. Με τον τρόπο αυτό επιχειρείται η διασφάλιση του σεβασμού της αρχής της αναλογικότητας και των δικαιωμάτων των θιγόμενων προσώπων. Ωστόσο, μια σοβαρή επιφύλαξη που μπορεί να εκφραστεί είναι το γεγονός ότι δεν έχει εξευρεθεί ακόμη ένας κοινά αποδεκτός ορισμός του "σοβαρού εγκλήματος" εντός της ΕΕ, ούτε και έχει επιτευχθεί εναρμόνιση των ποινικών αδικημάτων που επισύρουν στερητική της ελευθερίας ποινή με ανώτατο όριο τουλάχιστον 3 έτη[187], με αποτέλεσμα την πιθανή πρόκληση ανισοτήτων στην αντιμετώπιση των Ευρωπαίων Πολιτών, όσον αφορά το δικαίωμα στην προστασία των προσωπικών δεδομένων τους, και κατά συνέπεια την καθιέρωση προστασίας δύο "ταχυτήτων" εντός της Ένωσης. Επιπλέον, με το ίδιο σκεπτικό, όπως παραπάνω, είναι πιθανό τα Κράτη - Μέλη να οδηγηθούν σε αυστηροποίηση των ποινών σε ολοένα και περισσότερα αδικήματα που προβλέπονται στο εθνικό τους δίκαιο, προκειμένου να πληρούνται οι ελάχιστες προϋποθέσεις έκδοσης ΕΕΥ στοιχείων (προβλεπόμενη ποινή με ανώτατο όριο μεγαλύτερο των 3 ετών). Η Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή επισημαίνει στη σχετική Γνωμοδότηση της[188]

[186] Βλ. άρθρο 5 παράγραφος 4 στοιχείο α' της Πρότασης Κανονισμού

[187] Για την έννοια του «σοβαρού ποινικού αδικήματος» βλ. ΔΕΕ, Προτάσεις του Γενικού Εισαγγελέα της 3ης Μαΐου 2018, Υπόθεση C-207/16 Ministerio Fiscal, παράγραφοι 95 επ. και ειδικά παράγραφο 98: "Επιπλέον, επισημαίνεται ότι, δεδομένου ότι υφίστανται σημαντικές διαφορές μεταξύ του εύρους των κυρώσεων που ισχύουν παραδοσιακά στα διάφορα κράτη μέλη, η σοβαρότητα ενός ποινικού αδικήματος δεν συνδέεται μόνο με τη βαρύτητα της σχετικής ποινής."

[188] Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής με θέματα «Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις», ΕΕ C 367/88 της 10.10.2018

ότι ο στόχος του περιορισμού της έκδοσης ΕΕΥ στις πιο σοβαρές μορφές εγκλημάτων θα μπορούσε να επιτευχθεί καλύτερα εφαρμόζοντας ποινή με ελάχιστο όριο τριών μηνών ως κατευθυντήρια γραμμή παρά ποινή με μέγιστο όριο τριών ετών[189].

Άλλη επιφύλαξη σχετίζεται με τη δυνατότητα έκδοσης ΕΕΥ στοιχείων που αφορούν "δεδομένα συνδρομητή" και "δεδομένα πρόσβασης" από τον εισαγγελέα, χωρίς προηγούμενο έλεγχο από δικαστική αρχή[190]. Ο εισαγγελέας μπορεί να ζητεί και να λαμβάνει "δεδομένα συνδρομητή" και "δεδομένα πρόσβασης" απευθείας από τους Παρόχους Υπηρεσιών, χωρίς να υπόκειται σε έλεγχο ούτε από δικαστική αρχή του Κράτους Έκδοσης, ούτε από δικαστική αρχή του Κράτους, όπου βρίσκονται τα ζητούμενα δεδομένα. Κατά συνέπεια, στις περιπτώσεις αυτές οδηγούμαστε σε διαδικασίες, στις οποίες εφαρμόζονται σημαντικά λιγότερες εγγυήσεις για τα "δεδομένα συνδρομητή" και τα "δεδομένα πρόσβασης".

Τέλος, ένας σημαντικός τεχνικός προβληματισμός που ανακύπτει σχετίζεται με την τύχη των ακατέργαστων δεδομένων[191]. Σύμφωνα με τον Κανονισμό, τα δεδομένα θα πρέπει να παρέχονται από τους Παρόχους στις Δημόσιες Αρχές του Κράτους Έκδοσης ανεξάρτητα από το αν είναι κρυπτογραφημένα ή όχι[192]. Ήδη σήμερα, πολλοί Πάροχοι Υπηρεσιών προσφέρουν για παράδειγμα τη δυνατότητα διενέργειας από άκρη σε άκρη[193] κρυπτογραφημένων κλήσεων και από άκρη σε άκρη αποστολής κρυπτογραφημένων μηνυμάτων με τη χρήση εφαρμογών κρυπτογράφησης πολύ υψηλού επιπέδου προστασίας[194]. Ωστόσο, δεν είναι καθόλου βέβαιο ότι οι Αρμόδιες Αρχές του Κράτους Έκδοσης διαθέτουν την απαραίτητη τεχνογνωσία και τους απαιτούμενους οικονομικούς πόρους, ώστε μετά την παραλαβή τους, να τα επεξεργαστούν

[189] Βλ. Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής, ο.π.

[190] Βλ., ο.π.

[191] Marco Stefan / Gloria González Fuster, Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters - State of the art and latest developments in the EU and the US, CEPS Paper in Liberty and Security in Europe, 07/2018, σελ. 32

[192] Αιτιολογική σκέψη (19) Πρότασης Κανονισμού

[193] Η κρυπτογράφηση από άκρη σε άκρη (end-to-end encryption) διασφαλίζει ότι η επικοινωνία μεταξύ των αποστολέων και των αποδεκτών δεν μπορεί να είναι προσβάσιμη από κανέναν ενδιάμεσο, ούτε από τους ανθρώπους της εταιρίας. Τα δεδομένα κρυπτογραφούνται από τον αποστολέα, πριν την αποστολή τους και «ταξιδεύουν» κρυπτογραφημένα μέχρι τον αποδεκτή τους, ο οποίος με τη χρήση του μοναδικού κάθε φορά «κλειδιού» του, είναι ο μοναδικός που μπορεί να τα αποκρυπτογραφήσει. Ακόμα δηλαδή και αν τα δεδομένα «υποκλαπούν», πριν φτάσουν στον αποδεκτή τους, είναι θεωρητικά αδύνατο να αποκρυπτογραφηθούν.

[194] Βλ. Για παράδειγμα τις εφαρμογές Viber και WhatsApp

κατάλληλα για τους σκοπούς της ποινικής διαδικασίας[195]. Έτσι, τίθεται σε αμφιβολία αν, και σε ποιό βαθμό θα είναι πρόσφορα αυτά να αξιοποιηθούν ως αποδεικτικά στοιχεία στην Ποινική Δίκη.

ii. Αναφορικά με τις διαβιβάσεις δεδομένων σε τρίτες χώρες

Άλλη μια επιφύλαξη γεννάται από την κατάργηση των κριτηρίων τοποθεσίας και πιο συγκεκριμένα αναφορικά με τις διαβιβάσεις δεδομένων προς τρίτες χώρες. Είναι γεγονός ότι τουλάχιστον στο εσωτερικό της ΕΕ έχουν επιτευχθεί υψηλά επίπεδα προστασίας των θεμελιωδών δικαιωμάτων του ανθρώπου. Ο Γενικός Κανονισμός Προστασίας Δεδομένων, η Αστυνομική Οδηγία[196] και η Οδηγία για την Προστασία των Προσωπικών Δεδομένων στις Ηλεκτρονικές Επικοινωνίες[197] -η οποία σημειωτέον πρόκειται σύντομα να αντικατασταθεί με τον Κανονισμό για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες[198]- προσφέρουν επαρκή προστασία στον τομέα των Προσωπικών Δεδομένων. Επιπλέον, με τις Οδηγίες 2010/64/ΕΕ[199], 2012/13/ΕΕ[200], 2013/48/ΕΕ[201], 2016/343[202], 2016/800[203] και 2016/1919[204] παρέχεται υψηλό

[195] Για τον προβληματισμό αυτό και για σχετικά χαρακτηριστικά παραδείγματα βλ. Ιδίως Α. Καργόπουλο, Ανακριτικές πράξεις επί ψηφιακών δεδομένων: δικαιικοί άξονες και προβληματισμοί, σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, εκδ. Νομική Βιβλιοθήκη, 2019, σελ. 212

[196] Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου, ΕΕ L 119/89 της 4.5.2016

[197] Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, ΕΕ L 201/37 της 31.7.2002

[198] Βλ. Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ, COM(2017) 10 final

[199] Οδηγία 2010/64/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Οκτωβρίου 2010 , σχετικά με το δικαίωμα σε διερμηνεία και μετάφραση κατά την ποινική διαδικασία, ΕΕ L 280/1 της 26.10.2010

[200] Οδηγία 2012/13/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 22ας Μαΐου 2012 , σχετικά με το δικαίωμα ενημέρωσης στο πλαίσιο ποινικών διαδικασιών, ΕΕ L 142/1 της 1.6.2012

[201] Οδηγία 2013/48/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 22ας Οκτωβρίου 2013 , σχετικά με το δικαίωμα πρόσβασης σε δικηγόρο στο πλαίσιο ποινικής διαδικασίας και διαδικασίας εκτέλεσης του ευρωπαϊκού εντάλματος σύλληψης, καθώς και σχετικά με το δικαίωμα ενημέρωσης τρίτου προσώπου σε περίπτωση στέρησης της ελευθερίας του και με το δικαίωμα επικοινωνίας με τρίτα πρόσωπα και με προξενικές αρχές κατά τη διάρκεια της στέρησης της ελευθερίας, ΕΕ L 294/1 της 6.11.2013

[202] Οδηγία (ΕΕ) 2016/343 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Μαρτίου 2016, για την ενίσχυση ορισμένων πτυχών του τεκμηρίου αθωότητας και του δικαιώματος παράστασης του κατηγορουμένου στη δίκη του στο πλαίσιο ποινικής διαδικασίας, ΕΕ L 65/1 της 11.3.2016

επίπεδο προστασίας των θεμελιωδών δικαιωμάτων στις ποινικές διαδικασίες. Με τα παραπάνω νομοθετικά κείμενα έχει επιτευχθεί σε μεγάλο βαθμό ομοιομορφία στις νομοθεσίες των Κρατών-Μελών και έχουν εξασφαλιστεί τα ελάχιστα επίπεδα διαδικαστικών εγγυήσεων σε συμμόρφωση με την ΕΣΔΑ. Συνεπώς, μπορεί δικαιολογημένα να υποστηριχθεί ότι οι συνέπειες της κατάργησης των κριτηρίων τοποθεσίας θα είναι πιθανότατα περιορισμένες, όταν τα αποδεικτικά στοιχεία ζητούνται εντός της ΕΕ. Οξύς προβληματισμός δημιουργείται όμως στην αντίστροφη περίπτωση, κατά την οποία αρχές τρίτων χωρών ζητούν δεδομένα από Παρόχους που είναι εγκατεστημένοι εντός της ΕΕ. Στο πλαίσιο αυτό, αρχές τρίτης χώρας, στην οποία εφαρμόζονται διαφορετικές και πιθανόν λιγότερες διαδικαστικές εγγυήσεις στον τομέα του Ποινικού Δικαίου, θα μπορούσαν να έχουν πρόσβαση σε δεδομένα, τα οποία προστατεύονται από πρόσθετες εγγυήσεις εντός της ΕΕ. Χαρακτηριστικό παράδειγμα αποτελεί η πρόσφατη Αμερικανική Cloud Act[205], η οποία υποχρεώνει τους Παρόχους που έχουν την έδρα τους στις ΗΠΑ να παρέχουν κάθε είδους δεδομένα στις αρμόδιες Αρχές, ακόμα και αν αυτά διατηρούνται σε τρίτες χώρες, όπως για παράδειγμα στην ΕΕ. Με τον τρόπο αυτό επιχειρείται παράκαμψη των προστατευτικών διατάξεων της Ευρωπαϊκής Νομοθεσίας[206] και δημιουργείται σύγκρουση των νομοθετικών συστημάτων ΕΕ και ΗΠΑ[207].

iii. Αναφορικά με τη μη εφαρμογή της "αρχής του διττού αξιοποίνου" και της "αρχής της ειδικότητας"

Μια άλλη επιφύλαξη σχετίζεται με την μη τήρηση της αρχής του διττού αξιοποίνου. Μια από τις συνέπειες της αρχής της αμοιβαίας αναγνώρισης είναι η βαθμιαία υποχώρηση της απαίτησης του διττού αξιοποίνου, η οποία παραδοσιακά ισχύει στο δίκαιο της διακρατικής συνεργασίας σε ποινικές υποθέσεις[208]. Είναι γεγονός ότι τα Κράτη-Μέλη της ΕΕ επιδεικνύουν

---

[203] Οδηγία (ΕΕ) 2016/800 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαΐου 2016, σχετικά με τις δικονομικές εγγυήσεις για τα παιδιά που είναι ύποπτοι ή κατηγορούμενοι στο πλαίσιο ποινικών διαδικασιών, ΕΕ L 132/1 της 21.5.2016

[204] Οδηγία (ΕΕ) 2016/1919 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Οκτωβρίου 2016, σχετικά με τη δικαστική αρωγή για υπόπτους και κατηγορουμένους στο πλαίσιο ποινικών διαδικασιών και για καταζητούμενους σε διαδικασίες εκτέλεσης του ευρωπαϊκού εντάλματος σύλληψης, ΕΕ L 297/1 της 4.11.2016

[205] Βλ. Παρακάτω κεφάλαιο VI της παρούσης

[206] Βλ. Αναλυτικότερα EPDB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (annex)

[207] Sebastian Cording / Lena Götzinger, Der CLOUD Act aus europäischer Sicht, Computer Und Recht: Forum für die Praxis des Rechts der Datenverargeitung, Information und Automation, 10/2018, σελ. 636

[208] Α. Τζαννετής, Η Ευρωπαϊκή Εντολή Έρευνας, ΠοινΧρ 2/2018, σελ. 81

ολοένα μεγαλύτερη προθυμία συνεργασίας, ακόμη και αν τα ερευνητικά μέτρα αφορούν πράξεις οι οποίες δεν θεωρείται ότι συνιστούν αδίκημα στο εθνικό τους δίκαιο. Έτσι, το διττό αξιόποινο θεωρείται ολοένα και περισσότερο εμπόδιο στην ομαλή δικαστική συνεργασία[209]. Η μη τήρηση της αρχής του διττού αξιοποίνου έχει ως συνέπεια ο Πάροχος που έχει την έδρα του ή τον εκπρόσωπο του στο Κράτος Εκτέλεσης να εξαναγκάζεται από το Κράτος Έκδοσης να συμβάλει στην τιμώρηση μιας συμπεριφοράς, η οποία μπορεί να λαμβάνει χώρα στην επικράτεια του Κράτους Εκτέλεσης ελευθέρως και ατιμωρητί. Περαιτέρω, με βάση την εν λόγω ρύθμιση, το Κράτος Εκτέλεσης, στο οποίο έχει την έδρα του ή εκπροσωπείται ο Πάροχος Υπηρεσιών, είναι υποχρεωμένο για μια πράξη, που δεν είναι αξιόποινη κατά το εθνικό του δίκαιο, να ανέχεται την επιβολή επαχθών δικονομικών μέτρων κατά των πολιτών του, μέτρα, τα οποία δεν θα νομιμοποιούταν να λάβει το ίδιο, αν η αυτή ακριβώς συμπεριφορά είχε επιδειχθεί εντός της επικράτειάς του. Άμεση συνέπεια, λοιπόν, της μη εφαρμογής της αρχής του διττού αξιοποίνου είναι ότι ΕΕΔ στοιχείων οποιωνδήποτε δεδομένων, καθώς και ΕΕΥ "δεδομένων συνδρομητή" ή "δεδομένων πρόσβασης", όχι όμως και "δεδομένων συναλλαγών" και "δεδομένων περιεχομένου", επιτρέπεται να εκδίδονται για οποιοδήποτε ποινικό αδίκημα, ανεξάρτητα από το αν προβλέπονται ή όχι παρόμοια ποινικά αδικήματα σε άλλα Κράτη-Μέλη. Αξιοσημείωτη "παρενέργεια" της μη εφαρμογής της αρχής του διττού αξιοποίνου αποτελεί, για παράδειγμα, η υποχρέωση των Παρόχων Υπηρεσιών του Κράτους Εκτέλεσης να εκτελούν τις εντολές, που προέρχονται από Κράτη Έκδοσης και αφορούν ποινικό αδίκημα που μπορεί να καταλογιστεί σε νομικό πρόσωπο στο Κράτος Έκδοσης ή για το οποίο μπορεί να τιμωρηθεί νομικό πρόσωπο στο κράτος αυτό[210], ακόμα κι αν στο Κράτος Εκτέλεσης δεν νοείται ποινική ευθύνη των νομικών προσώπων, όπως ισχύει στη χώρα μας[211].

Μια άλλη "κλασσική" αρχή στο πεδίο της δικαστικής συνεργασίας σε ποινικές υποθέσεις που τείνει να απεμπολήσει το σύγχρονο Ευρωπαϊκό Ποινικό Δίκαιο είναι η αρχή της ειδικότητας. Αυτή εκφράζεται στην Απόφαση-Πλαίσιο 2002/584/ΔΕΥ του Συμβουλίου της 13ης Ιουνίου 2002 για το Ευρωπαϊκό Ένταλμα Σύλληψης, η οποία ενσωματώθηκε στην Ελληνική έννομη τάξη με τον Ν. 3251/2004. Σύμφωνα με το άρθρο 34 παρ. 1 «ο εκζητούμενος που έχει

[209] Γνωμοδότηση 23/2018 του Συμβουλίου Προστασίας Δεδομένων, ο.π.
[210] Βλ. άρθρο 3 παρ. 2 εδ. 2 Πρότασης Κανονισμού
[211] Βλ. σχετικά Δημήτριος Νταφόπουλος/Παναγιώτης Σάικας/Μαρία Σαΐτη, Ποινική ευθύνη νομικών προσώπων και επιχειρήσεων – Σύγχρονες εξελίξεις, Pro Justitia 1/2018, σελ. 344

προσαχθεί στον αρμόδιο εισαγγελέα εφετών δεν διώκεται, ούτε καταδικάζεται, ούτε στερείται με άλλον τρόπο της ελευθερίας του για αξιόποινη πράξη, η οποία τελέστηκε πριν από την προσαγωγή του και είναι διαφορετική από εκείνη για την οποία είχε εκδοθεί το ευρωπαϊκό ένταλμα σύλληψης». Όμοια ρύθμιση καθιερωνόταν στο άρθρο 14 της από 13 Δεκεμβρίου 1957 Ευρωπαϊκής Συμβάσεως Εκδόσεως, που κυρώθηκε από την Ελλάδα με το νόμο 4165/1961, και επίσης υπάρχει στο άρθρο 440 σε συνδυασμό με άρθρα 438 εδ. ε' και 445 του νΚΠΔ[212]. Η αρχή αυτή απαντάται επίσης στο άρθρο 13 παρ. 10 της Ευρωπαϊκής Σύμβασης περί Αμοιβαίας Συνδρομής επί Ποινικών Υποθέσεων του 1959, όπως επίσης και στο άρθρο 20 παρ. 10 του Δεύτερου Πρόσθετου Πρωτοκόλλου της. Ωστόσο, τόσο η Οδηγία για την ΕΕΕ[213] όσο και η Πρόταση Κανονισμού δεν περιέχουν καμία διάταξη που να προβλέπει την αρχή της ειδικότητας. Στην προκειμένη περίπτωση, η αρχή της ειδικότητας θα είχε την έννοια ότι τα αποδεικτικά στοιχεία ή οι πληροφορίες που αποκτήθηκαν μέσω της διεθνούς συνεργασίας σε ποινικές υποθέσεις δεν μπορούν να χρησιμοποιηθούν για σκοπούς άλλους από αυτούς, για τους οποίους ζητήθηκε η συνεργασία. Η αρχή αυτή συνδέεται άμεσα με την προβληματική των αποδεικτικών απαγορεύσεων και την αξιοποίηση των "τυχαίων ευρημάτων"[214].

iv. Αναφορικά με την επάρκεια της δικαστικής προστασίας

Η προβλεπόμενη έννομη προστασία, όσον αφορά τους Αποδέκτες των εντολών, που επιτυγχάνεται μέσω των διαδικασιών ελέγχου των άρθρων 15 και 16 της Πρότασης Κανονισμού, αφορά μόνο τις ΕΕΥ στοιχείων, με την αιτιολογία ότι οι ΕΕΔ στοιχείων δεν έχουν ως αποτέλεσμα τη γνωστοποίηση δεδομένων και ότι, ως εκ τούτου, δε θα πρέπει να γεννιούνται ανησυχίες[215]. Έτσι όμως, οι Πάροχοι στερούνται το δικαίωμα αποτελεσματικής έννομης προστασίας, όταν πρόκειται για ΕΕΔ στοιχείων. Επιπρόσθετα, στο άρθρο 17, όπου προβλέπεται η έννομη προστασία των υπόπτων, των κατηγορουμένων αλλά και τρίτων, των οποίων τα δεδομένα συλλέγονται, δεν διατίθενται επίσης ειδικά μέσα έννομης προστασίας όταν πρόκειται για ΕΕΔ στοιχείων, με την ίδια, ως άνω αιτιολογία, ότι δηλαδή η τελευταία από μόνη της δεν

[212] Α. Καραφλός, Ανακύπτοντα νομικά ζητήματα κατά την πρακτική εφαρμογή του ευρωπαϊκού εντάλματος σύλληψης, ΠοινΧρ 2013/90

[213] Júlio Barbosa e Silva, The speciality rule in cross-border evidence gathering and in the European Investigation Order—let's clear the air, ERA Forum, Volume 19, Issue 3, March 2019, σελ. 485

[214] Βλ. Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, εκδ. Νομική Βιβλιοθήκη, 2019, σελ. 258 και από εκεί σχετικές παραπομπές

[215] Βλ. Αιτιολογική Έκθεση Πρότασης Κανονισμού

προβλέπει τη γνωστοποίηση δεδομένων, με την εξαίρεση των περιπτώσεων, στις οποίες την ακολουθεί ΕΕΥ στοιχείων ή άλλη πράξη ΑΔΣ, που αποσκοπεί στη γνωστοποίηση. Η θέση αυτή όμως αποδεικνύεται μάλλον προβληματική, όταν, για παράδειγμα, ο Πάροχος είχε υποχρέωση εκ του νόμου να διαγράψει ή να περιορίσει την επεξεργασία των δεδομένων, των οποίων ζητήθηκε η διατήρηση μέσω της ΕΕΔ στοιχείων. Όταν λοιπόν τα δεδομένα αυτά, τα οποία έπρεπε να διαγραφούν ή να περιοριστεί η επεξεργασία τους, διατηρούνται δυνάμει μιας ΕΕΔ στοιχείων, αντίθετα με την σχετική νομοθετική πρόβλεψη, υπάρχει σαφής παραβίαση των δικαιωμάτων των υποκειμένων, των οποίων τα δεδομένα διατηρούνται και συγκεκριμένα των δικαιωμάτων τους στην προστασία των δεδομένων προσωπικού χαρακτήρα και του σεβασμού της ιδιωτικής και οικογενειακής ζωής. Ειδικότερα, στην περίπτωση που μετά την ΕΕΔ στοιχείων ακολουθήσει ΕΕΥ στοιχείων ή άλλη πράξη ΑΔΣ, τότε η προθεσμία διατήρησης των στοιχείων των 60 ημερών δύναται να επεκτείνεται για αόριστο χρονικό διάστημα[216], χωρίς να τίθεται ένα ανώτατο όριο διατήρησης.

VI. Η Νομοθετική Πορεία

Σήμερα, τόσο η Πρόταση Κανονισμού όσο και η Πρόταση Οδηγίας εκκρεμούν στο στάδιο της πρώτης ανάγνωσης[217], σύμφωνα με τη συνήθη νομοθετική διαδικασία[218]. Στο Ευρωπαϊκό Κοινοβούλιο αναμένεται η έκθεση της αρμόδιας Επιτροπής Πολιτικών Ελευθεριών, Δικαιοσύνης και Εσωτερικών Υποθέσεων (LIBE), προτού το Κοινοβούλιο καθορίσει τη θέση του. Ταυτόχρονα διεξήχθησαν προπαρασκευαστικές εργασίες στο Συμβούλιο. Στη συνεδρίαση της 7ης Δεκεμβρίου 2018, που συμπληρώθηκε από τη Συνεδρίαση της 6ης Ιουνίου 2019, το Συμβούλιο κατέληξε στη γενική προσέγγισή του αναφορικά με τον Κανονισμό[219]**.** Όσον αφορά την Οδηγία, το Συμβούλιο κατέληξε στην γενική προσέγγισή του στη Συνεδρίαση της 8ης Μαρτίου 2019[220]. Σύμφωνα με τις παραπάνω γενικές προσεγγίσεις, τόσο στην Πρόταση Κανονισμού όσο και στην Πρόταση Οδηγίας σημειώνονται πολλές και σημαντικές τροποποιήσεις που δίνουν απάντηση σε πολλούς από τους παραπάνω προβληματισμούς[221]. Έτσι,

[216] Βλ. άρθρο 10, παρ. 1 και 2 Πρότασης Κανονισμού
[217] Βλ. άρθρο 294 παρ. 3-6 Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης
[218] Βλ. άρθρα 289 και 294, ο.π.
[219] 10206/19, 11 June 2019
[220] 7348/19, 11 March 2019
[221] Για παράδειγμα, με το προστεθέν άρθρο 12b υπό τον τίτλο "Speciality principle" προβλέπεται ρητά η αρχή της ειδικότητας

το Συμβούλιο είναι έτοιμο να ξεκινήσει τριμερείς διαπραγματεύσεις επί του συνόλου της δέσμης για τα ηλεκτρονικά αποδεικτικά στοιχεία μόλις το Κοινοβούλιο εγκρίνει τη θέση του, κάτι που δεν αναμενόταν να συμβεί πριν από τις πρόσφατες Ευρωεκλογές της 26ης Μαΐου 2019[222].

[222] Δελτίο Τύπου του Συμβουλίου της ΕΕ της 8/3/2019

Β. Η Συμφωνία Αμοιβαίας Δικαστικής Συνδρομής μεταξύ ΕΕ και ΗΠΑ

i. Η υπόθεση States v. Microsoft Corp.

Τον Δεκέμβριο του 2013, αμερικανικές ομοσπονδιακές αρχές επιβολής του Νόμου ζήτησαν από αμερικανικό επαρχιακό δικαστήριο της Νέας Υόρκης την έκδοση ενός εντάλματος, σύμφωνα με την παράγραφο 2703 του νόμου για τα Αποθηκευμένα Δεδομένα Επικοινωνιών (Stored Communications Act - SCA)[223], με το οποίο θα υποχρεωνόταν η Microsoft να παρέχει όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου, καθώς και άλλες πληροφορίες που αφορούσαν έναν συγκεκριμένο λογαριασμό πελάτη που τηρούσε η ίδια και υπήρχαν βάσιμες υποψίες ότι χρησιμοποιήθηκε για διακίνηση ναρκωτικών ουσιών. Το ένταλμα εκδόθηκε, αλλά μετά την επίδοσή του διαπιστώθηκε ότι τα ζητούμενα δεδομένα ήταν αποθηκευμένα σε διακομιστή της Microsoft στην Ιρλανδία. Η Microsoft αμφισβήτησε το ένταλμα με την αιτιολογία ότι ένα ένταλμα που εκδίδεται σύμφωνα με τον νόμο για Αποθηκευμένα Δεδομένα Επικοινωνιών (Stored Communications Act - SCA) δεν μπορεί να υποχρεώσει Αμερικανικές εταιρίες να υποβάλουν δεδομένα που βρίσκονται αποθηκευμένα σε διακομιστές εκτός της επικράτειας των ΗΠΑ. Η εταιρία προσέφυγε στο Περιφερειακό Δικαστήριο της Νέας Υόρκης, όπου ηττήθηκε σε πρώτο βαθμό, με την απόφαση να αποφαίνεται ότι η φύση του εντάλματος που εκδίδεται σύμφωνα με τον νόμο για Αποθηκευμένα Δεδομένα Επικοινωνιών (Stored Communications Act - SCA) δεν υπόκειται σε τοπικούς περιορισμούς. Η Microsoft άσκησε έφεση κατά της παραπάνω απόφασης και δικαιώθηκε από το αρμόδιο Εφετείο της Νέας Υόρκης, το οποίο επιλήφθηκε της υπόθεσης και ακύρωσε το επίμαχο ένταλμα. Αξίζει να σημειωθεί ότι σε παρόμοιες περιπτώσεις το ίδιο Εφετείο είχε διατάξει άλλες εταιρίες (π.χ. Google) να συμμορφωθούν με παρόμοια εντάλματα, εφόσον μπορούσαν να έχουν πρόσβαση στα ζητούμενα δεδομένα από την επικράτεια των ΗΠΑ, ανεξάρτητα από την τοποθεσία αποθήκευσης των δεδομένων. Το Υπουργείο Δικαιοσύνης των ΗΠΑ προσέφυγε κατά της απόφασης του Εφετείου της Νέας Υόρκης στο Ανώτατο Δικαστήριο, το οποίο συμφώνησε να εξετάσει την υπόθεση τον Οκτώβριο του 2017. Πριν από την έκδοση της σχετικής απόφασης του Ανωτάτου Δικαστηρίου επενέβη ο Νομοθέτης

[223] Ο νόμος για τα Αποθηκευμένα Δεδομένα Επικοινωνιών (Stored Communications Act - SCA) αποτελεί μέρος του νόμου περί Ηλεκτρονικών Επικοινωνιών και Προστασίας της Ιδιωτικής Ζωής του 1986 (Electronic Communications and Privacy Act 1986 — ECPA)

με την θέσπιση του νόμου Clarifying Lawful Overseas Use of Data Act (CLOUD Act), επιλύοντας οριστικά δια της νομοθετικής οδού το ζήτημα, που είχε ανακύψει.

ii. Οι εξελίξεις στον τομέα των ηλεκτρονικών αποδεικτικών μέσων σε ποινικές υποθέσεις στις ΗΠΑ και ο νόμος CLOUD Act

Έτσι, στις 23 Μαρτίου 2018 εκδόθηκε από το Κογκρέσο των Ηνωμένων Πολιτειών της Αμερικής ο Νόμος Clarifying Lawful Use of Overseas Data (CLOUD) Act, για την αποσαφήνιση της νόμιμης χρήσης δεδομένων στο εξωτερικό. Ο στόχος ήταν διπλός, αφενός η αποσαφήνιση της πρόσβασης των Αμερικανικών αρχών επιβολής του Νόμου σε δεδομένα που βρίσκονται στο εξωτερικό και αφετέρου η δημιουργία ενός μηχανισμού για τις αλλοδαπές κυβερνήσεις, ώστε να έχουν πρόσβαση σε δεδομένα που είναι αποθηκευμένα στις ΗΠΑ[224]. Μέχρι τότε, ο Νόμος για τα Αποθηκευμένα Δεδομένα Επικοινωνιών (Stored Communications Act) του 1986[225] απαγόρευε τη γνωστοποίηση δεδομένων περιεχομένου, ενώ τα δεδομένα που δεν αφορούν το περιεχόμενο μπορούσαν να παρέχονται σε προαιρετική βάση[226]. Ο Νόμος CLOUD τροποποιεί τον νόμο για τα Αποθηκευμένα Δεδομένα Επικοινωνιών (SCA) του 1986, και προβλέπει πλέον την υποχρέωση των Παρόχων Υπηρεσιών των ΗΠΑ[227] να συμμορφώνονται με εντολές Αρχών των ΗΠΑ για γνωστοποίηση τόσο δεδομένων περιεχομένου όσο και δεδομένων που δεν αφορούν το περιεχόμενο, και επιπρόσθετα ανεξάρτητα από τον τόπο αποθήκευσης των δεδομένων αυτών, συμπεριλαμβανομένης της Ευρωπαϊκής Ένωσης[228]. Ταυτόχρονα, ο Νόμος εξουσιοδοτεί την εκτελεστική εξουσία των ΗΠΑ να συνάπτει συμφωνίες με ξένες κυβερνήσεις, σύμφωνα με τις οποίες οι ξένες κυβερνήσεις μπορούν να αποκτήσουν ταχεία πρόσβαση στα δεδομένα, που διατηρούνται εντός της επικράτειας των ΗΠΑ[229]. Έτσι,

[224] Jennifer Daskal, Unpacking the CLOUD Act, eucrim 4/2018, σελ. 220

[225] Stored Communications Act (SCA), 18 U.S.C. Chapter 121 §§ 2701–2712. Ο Νόμος Stored Communications Act (SCA), εμπεριέχεται στον Δεύτερο Τίτλο του Νόμου Electronic Communications and Privacy Act (ECPA), ο οποίος προστατεύει τις προφορικές, τις τηλεφωνικές και τις ηλεκτρονικές επικοινωνίες

[226] Αξίζει να σημειωθεί ότι το δίκαιο των Η.Π.Α. επιτρέπει στους παρόχους υπηρεσιών που είναι εγκατεστημένοι στις ΗΠΑ να συνεργάζονται απευθείας με τις Ευρωπαϊκές Δημόσιες Αρχές για δεδομένα που όμως δεν αφορούν το περιεχόμενο. Ωστόσο, η συνεργασία αυτή είναι προαιρετική.

[227] Marco Stefan / Gloria González Fuster, Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters - State of the art and latest developments in the EU and the US, CEPS Paper in Liberty and Security in Europe, 07/2018

[228] §2713 Electronic Communications and Privacy Act 1986 (ECPA) που προστέθηκε με την Pub. L. 115–141, div. V, § 103(a)(1), Mar. 23, 2018, 132 Stat. 1214

[229] Pub. L. 115–141, div. V, § 105, Mar. 23, 2018, 132 Stat. 1217

άνοιξε ο δρόμος για την έναρξη των διαπραγματεύσεων μεταξύ ΗΠΑ και ΕΕ στον τομέα των ηλεκτρονικών αποδεικτικών μέσων σε ποινικές υποθέσεις.

iii. Οι κινήσεις της ΕΕ για την επίτευξη συμφωνίας Αμοιβαίας Δικαστικής Συνδρομής

Η ψήφιση του Νόμου CLOUD Act έχει άμεσες επιπτώσεις για την ΕΕ και οδήγησε σε ραγδαίες εξελίξεις εντός της Ένωσης. Όπως προαναφέρθηκε, ο νέος Νόμος δίνει τη δυνατότητα στις Αμερικανικές Αρχές να ζητούν δεδομένα, ακόμα και δεδομένα περιεχομένου, από τους Παρόχους Υπηρεσιών που έχουν την έδρα τους στις ΗΠΑ, ανεξάρτητα από τον τόπο, όπου βρίσκονται αποθηκευμένα τα δεδομένα, ακόμα και αν αυτά βρίσκονται στην ΕΕ και αφορούν Ευρωπαίους πολίτες. Έτσι, ο Νόμος CLOUD Act έρχεται σε σύγκρουση με την Ευρωπαϊκή Νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα[230], και συγκεκριμένα με τον Γενικό Κανονισμό Προστασίας Δεδομένων, ο οποίος στο άρθρο 48 απαγορεύει διαβιβάσεις ή κοινοποιήσεις δεδομένων σε τρίτες χώρες, που βασίζονται σε αποφάσεις δικαστηρίων ή αποφάσεις διοικητικών αρχών των χωρών αυτών και απαιτούν από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία να διαβιβάσει ή να κοινοποιήσει δεδομένα προσωπικού χαρακτήρα Ευρωπαίων πολιτών. Οι παραπάνω αποφάσεις, σύμφωνα με το ίδιο άρθρο, μπορούν να αναγνωρισθούν ή να είναι εκτελεστές καθ' οιονδήποτε τρόπο, μόνο εάν βασίζονται σε διεθνή συμφωνία, όπως σύμβαση αμοιβαίας δικαστικής συνδρομής, που ισχύει μεταξύ της αιτούσας τρίτης χώρας και της Ένωσης ή κράτους μέλους, με την επιφύλαξη άλλων λόγων διαβίβασης. Σύμφωνα με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων και Ευρωπαίο Επόπτη Προστασίας Δεδομένων[231], επί του παρόντος δεν υπάρχει τέτοιου είδους συμφωνία αμοιβαίας δικαστικής συνδρομής μεταξύ ΕΕ και ΗΠΑ, η οποία να πληρεί τα κριτήρια του άρθρου 48 του Γενικού Κανονισμού Προστασίας Δεδομένων. Επιπλέον, υπό τον φόβο ότι πολλά Κράτη-Μέλη της ΕΕ θα σπεύσουν να επιτύχουν διμερείς σχετικές συμφωνίες με τις ΗΠΑ, γεγονός που πιθανότατα θα δημιουργήσει καθεστώς πολυνομίας και θα οδηγήσει σε διάσπαση του νομοθετικού πλαισίου εντός της ΕΕ, η Ευρωπαϊκή Επιτροπή κινήθηκε με χαρακτηριστική ταχύτητα. Έτσι, στις 5 Φεβρουαρίου 2019 εξέδωσε Σύσταση για Απόφαση του Συμβουλίου που εγκρίνει την έναρξη διαπραγματεύσεων με σκοπό τη σύναψη συμφωνίας μεταξύ της ΕΕ και των

[230] Βλ. EPDB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection και EPDB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (annex)
[231] Βλ. Ο.π.

ΗΠΑ σχετικά με τη διασυνοριακή πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία στο πλαίσιο της δικαστικής συνεργασίας σε ποινικές υποθέσεις[232]. Με το άρθρο 1 της Σύστασης η Επιτροπή εξουσιοδοτείται να διαπραγματευθεί, εξ ονόματος της Ένωσης, συμφωνία μεταξύ της Ένωσης και των ΗΠΑ σχετικά με τη διασυνοριακή πρόσβαση των δικαστικών αρχών, στο πλαίσιο ποινικών διαδικασιών, σε ηλεκτρονικά αποδεικτικά στοιχεία που τηρούνται από Πάροχο Υπηρεσιών. Το πλαίσιο αυτό θα εξασφαλίσει την έγκαιρη πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία συντομεύοντας σε 10 ημέρες το χρονικό διάστημα για την παροχή των ζητούμενων δεδομένων, διαδικασία που επί του παρόντος διαρκεί κατά μέσο όρο 10 μήνες[233]. Την 6η Ιουνίου 2019 το Συμβούλιο υιοθέτησε την παραπάνω Σύσταση[234] σηματοδοτώντας ουσιαστικά την έναρξη των διαπραγματεύσεων.

[232] Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 5.2.2019, COM(2019) 70 final

[233] Βλ. Recommendation for a Council Decision, ο.π., σελ. 1

[234] Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 12 June 2019, 10128/19

Γ. Το Δεύτερο Πρόσθετο Πρωτόκολλο της Σύμβασης της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο

Την ίδια στιγμή σε διεθνές επίπεδο, οι συζητήσεις λαμβάνουν χώρα στο πλαίσιο των διαπραγματεύσεων σχετικά με το δεύτερο Πρόσθετο Πρωτόκολλο της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο[235]. Το άρθρο 46 παράγραφος 1 της Σύμβασης προβλέπει ότι τα Συμβαλλόμενα Μέρη διαβουλεύονται περιοδικά, όταν αυτό χρειάζεται, με σκοπό να διευκολυνθεί: α) η αποτελεσματική χρήση και εφαρμογή της Σύμβασης, όπως επίσης και ο εντοπισμός τυχόν προβλημάτων αυτής, καθώς και τα αποτελέσματα κάθε δήλωσης ή επιφύλαξης έχει γίνει δυνάμει της Σύμβασης, β) η ανταλλαγή πληροφοριών για σημαντικές νομικές, πολιτικές ή τεχνολογικές εξελίξεις πάνω στο θέμα του εγκλήματος στον Κυβερνοχώρο και της συλλογής αποδεικτικών στοιχείων σε ηλεκτρονική μορφή και γ) η εξέταση πιθανών συμπληρώσεων και τροποποιήσεων της Σύμβασης. Τον Ιούνιο του 2017, η Επιτροπή της Σύμβασης για το Έγκλημα στον Κυβερνοχώρο ενέκρινε τους όρους εντολής για την κατάρτιση Δεύτερου Πρόσθετου Πρωτοκόλλου της Σύμβασης κατά την περίοδο από τον Σεπτέμβριο του 2017 έως τον Δεκέμβριο του 2019. Σύμφωνα με τους όρους εντολής, το Δεύτερο Πρόσθετο Πρωτόκολλο μπορεί να περιλαμβάνει τα ακόλουθα στοιχεία:

α) διατάξεις για αποτελεσματικότερη αμοιβαία δικαστική συνδρομή, ιδίως:

- απλουστευμένο καθεστώς για την υποβολή αιτημάτων αμοιβαίας δικαστικής συνδρομής για πληροφορίες σχετικά με συνδρομητές,
- διεθνείς εντολές υποβολής στοιχείων / διαταγές επίδειξης,
- άμεση συνεργασία μεταξύ των δικαστικών αρχών όσον αφορά αιτήματα αμοιβαίας δικαστικής συνδρομής,
- κοινές έρευνες και κοινές ομάδες έρευνας,
- αιτήματα διατυπωμένα στην αγγλική γλώσσα,
- ακρόαση μαρτύρων, θυμάτων και εμπειρογνωμόνων μέσω ηχητικής διάσκεψης/εικονοδιάσκεψης,
- διαδικασίες για επείγουσες περιστάσεις αμοιβαίας δικαστικής συνδρομής (MLA),

[235] Σύμβαση της Βουδαπέστης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (CETS αριθ. 185)

β) διατάξεις που προβλέπουν την άμεση συνεργασία με παρόχους υπηρεσιών σε άλλες δικαιοδοσίες όσον αφορά τα αιτήματα παροχής πληροφοριών σχετικά με συνδρομητές, αιτήματα διατήρησης και αιτήματα έκτακτης ανάγκης,

γ) σαφέστερο πλαίσιο και ισχυρότερες διασφαλίσεις για τις υφιστάμενες πρακτικές διασυνοριακής πρόσβασης στα δεδομένα,

δ) διασφαλίσεις, συμπεριλαμβανομένων των απαιτήσεων προστασίας δεδομένων.

Έτσι, ταυτόχρονα με την από 5 Φεβρουαρίου 2019 Σύστασή της, σχετικά με τη συμφωνία αμοιβαίας δικαστικής συνδρομής μεταξύ ΕΕ και ΗΠΑ, η Ευρωπαϊκή Επιτροπή εξέδωσε την ίδια ημέρα, Σύσταση για Απόφαση του Συμβουλίου για την έγκριση της συμμετοχής σε διαπραγματεύσεις σχετικά με Δεύτερο Πρόσθετο Πρωτόκολλο της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο[236]. Το άρθρο 1 της Σύστασης εξουσιοδοτεί την Επιτροπή να διαπραγματευτεί, εξ ονόματος της Ένωσης, το Δεύτερο Πρόσθετο Πρωτόκολλο της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο. Το πλεονέκτημα μιας τέτοιας συμφωνίας είναι ότι θα μπορούσε να εφαρμοστεί σε ολόκληρη την υφήλιο. Επί του παρόντος, τα συμβαλλόμενα μέρη της Σύμβασης ανέρχονται σε 62, συμπεριλαμβανομένων 26 Κρατών-Μελών της ΕΕ[237]. Την 6η Ιουνίου 2019 το Συμβούλιο υιοθέτησε και την παραπάνω Σύσταση[238]. Οι διαπραγματεύσεις αναμένεται να διεξαχθούν ταυτόχρονα με τη συμφωνία αμοιβαίας δικαστικής συνδρομής μεταξύ ΕΕ και ΗΠΑ και παρότι οι δύο διαδικασίες θα διεξαχθούν με διαφορετικούς ρυθμούς, αφορούν αλληλένδετα ζητήματα και οι δεσμεύσεις που θα αναληφθούν στο πλαίσιο της μιας διαπραγμάτευσης ενδέχεται να έχουν άμεσο αντίκτυπο και στην άλλη.

[236] Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), 5.2.2019, COM(2019) 71 final

[237] Βλ. Recommendation for a Council Decision, ο.π., σελ. 1

[238] Council Decision authorising the European Commisson to participate, on behalf of the European Union, in negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime, 12 June 2019, 10129/19

ΕΠΙΛΟΓΟΣ

Οι διασυνοριακές ροές δεδομένων αυξάνονται ταυτόχρονα, με τον ίδιο φρενήρη ρυθμό, με τον οποίο αυξάνεται η χρήση των κοινωνικών δικτύων, των υπηρεσιών ηλεκτρονικού ταχυδρομείου, των υπηρεσιών διαδικτυακής επικοινωνίας, των υπηρεσιών αποθήκευσης δεδομένων σε υποδομές νεφοϋπολογιστικής και άλλων καινοτόμων επιφυών υπηρεσιών, που παρέχονται μέσω του Διαδικτύου. Έτσι, σε έναν συνεχώς αυξανόμενο αριθμό ποινικών υποθέσεων, οι Αρχές επιβολής του Νόμου χρειάζονται ταχεία πρόσβαση σε ηλεκτρονικά αποδεικτικά μέσα, τα οποία δεν είναι δημόσια, όπως για παράδειγμα στο περιεχόμενο μιας συνομιλίας στο Facebook, στα προσωπικά στοιχεία του κατόχου μιας διεύθυνσης ηλεκτρονικού ταχυδρομείου, στο περιεχόμενο μιας κλήσης που πραγματοποιήθηκε μέσω WhatsApp, στα αρχεία που διατηρεί αποθηκευμένα ένας χρήστης στο Google Drive κ.α..

Ασφαλώς η αναχαίτιση και η εξάλειψη του Κυβερνοεγκλήματος αποτελεί το μεγαλύτερο στοίχημα για τις Αρχές επιβολής του Νόμου στην ψηφιακή εποχή, δε θα πρέπει ωστόσο ο στόχος αυτός να επιδιώκεται με οποιοδήποτε κόστος. Τα θεμελιώδη δικαιώματα, όπως το δικαίωμα στο σεβασμό της ιδιωτικής και οικογενειακής ζωής, το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα κ.α., θα πρέπει να λαμβάνονται πολύ σοβαρά υπόψη. Τα νομοθετικά μέτρα, τα οποία πρόκειται να ληφθούν στο μέλλον θα πρέπει επίσης να σέβονται, τόσο την αρχή της αναγκαιότητας όσο και την αρχή της αναλογικότητας, η οποία αποτελεί ακρογωνιαίο λίθο της Ευρωπαϊκής Νομοθεσίας. Από την άλλη, η άμεση λήψη αποτελεσματικών μέτρων θα οδηγήσει στην αύξηση του αισθήματος ασφάλειας, που αισθάνονται οι πολίτες σήμερα.

Δεδομένου του διεθνούς χαρακτήρα του Διαδικτύου απαιτείται η όσο το δυνατόν μεγαλύτερη συμμετοχή κρατών από όλο τον κόσμο στις διαπραγματεύσεις και η ευρύτερη αποδοχή των νομοθετικών μέτρων από ολοένα και περισσότερα κράτη της υφηλίου. Η λήψη ενιαίων μέτρων σε παγκόσμια κλίμακα θα δημιουργήσει ομοιομορφία στα δίκαια των κρατών ανά τον κόσμο, κάτι που αναμένεται να δημιουργήσει ασφάλεια δικαίου και να ενισχύσει την οικουμενική διασυνοριακή συνεργασία των κρατών.

Έχω την ενδόμυχη πεποίθηση ότι σήμερα η Ευρωπαϊκή Ένωση κινείται προς την σωστή κατεύθυνση, καταφέρνοντας να «ισορροπήσει» επαρκώς ανάμεσα στην ανάγκη για άμεση λήψη αποτελεσματικών μέτρων στο πεδίο των ηλεκτρονικών αποδεικτικών μέσων σε ποινικές διαδικασίες και στην παρεμβατικότητα, την οποία συνεπάγονται τα μέτρα αυτά στα θεμελιώδη δικαιώματα. Βέβαια, οι συζητήσεις για την αναζήτηση της «χρυσής τομής» ανάμεσα στην αποτελεσματικότητα των νομοθετικών μέτρων και της προστασίας των θεμελιωδών δικαιωμάτων αναμένεται να συνεχιστούν και να κορυφωθούν το επόμενο διάστημα.

Βιβλιογραφία

i. Ελληνική Βιβλιογραφία

1. Furnell St., (2006), Κυβερνοέγκλημα, Εκδόσεις Παπαζήση
2. Jougleux P., (2016), Ευρωπαϊκό δίκαιο του διαδικτύου, Εκδόσεις Σάκκουλα: Αθήνα - Θεσσαλονίκη
3. Βλαχόπουλος Κ., (2007), Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη
4. Γιαννόπουλος Γ., (2018), Εισαγωγή στη Νομική Πληροφορική, Νομική Βιβλιοθήκη
5. Δαλακούρας Θ., (2018), Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη
6. Δαλακούρας Θ., (2019), Ο νέος Κώδικας Ποινικής Δικονομίας, Νομική Βιβλιοθήκη
7. Ζέκος Γ., (2017), Διαδίκτυο, Η/Υ & Τηλεπικοινωνίες στο Ελληνικό Δίκαιο, Εκδόσεις Σάκκουλα: Αθήνα - Θεσσαλονίκη
8. Ιγγλεζάκης Ι., (2018), Δίκαιο Πληροφορικής, Εκδόσεις Σάκκουλα: Αθήνα - Θεσσαλονίκη
9. Καράκωστας Ι., (2009), Δίκαιο και Ίντερνετ, Εκδόσεις Π.Ν. Σάκκουλας
10. Κιούπης Δ., (1999), Ποινικό Δίκαιο και Internet, Εκδόσεις Αντ. Ν. Σάκκουλα
11. Κριθαράς Θ., (2009), Ποινικό Δίκαιο και Διαδίκτυο, Νομική Βιβλιοθήκη
12. Λαχανά, Κ. - Χ. (διδακτορική διατριβή), (2017), Η κατά το ελληνικό δίκαιο ποινική προστασία των προσωπικών δεδομένων στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις: προκλήσεις και προοπτικές, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Τμήμα Νομικής
13. Μεταξάκης Ε., (2017), Μπίτκοϊν (bitcoin), κρυπτοχρήμα και κυβερνοέγκλημα, Αντ. Ν. Σάκκουλα: Αθήνα - Θεσσαλονίκη
14. Νούσκαλης Γ., (2006), Ποινική προστασία προσωπικών δεδομένων, Εκδόσεις Σάκκουλα: Αθήνα - Θεσσαλονίκη

15. Παναγιωτακόπουλος Χρ., (2018), Η ηθική στο διαδίκτυο και το ηλεκτρονικό έγκλημα, Εκδόσεις Παπαζήση

16. Παπακωνσταντίνου Ε., (2010), Δίκαιο πληροφορικής, Εκδόσεις Σάκκουλα: Αθήνα - Θεσσαλονίκη

17. Σφακιανάκης Ε., Μακρυπούλιας Ι. (2016). Τα κλειδιά του διαδικτύου : Το διαδίκτυο από το Α ως το Ω. All About Internet

18. Σφακιανάκης Ε., (2016)., Ο Κώδικας του Διαδικτύου, All About Internet

ii. Ελληνική Αρθρογραφία

1. Girginov A., Εκτέλεση της Ευρωπαϊκής Εντολής Έρευνας στη Βουλγαρία, Ποινική Δικαιοσύνη, 12/2018

2. Αγγελής Ι ., Διαδίκτυο και ποινικό δίκαιο , Έγκλημα στον Κυβερνοχώρο , Ποινικά Χρονικά, 8/2000.

3. Αγγελής Ι., Ηλεκτρονικό έγκλημα και απονομή της ποινικής δικαιοσύνης, Ποινική Δικαιοσύνη, 8-9/2005

4. Αγγελής Ι., Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convection on Cyber-crime), Ποινική Δικαιοσύνη 12/2001

5. Αγγελόπουλος Δ. – Πάσχος Ι., Κατάσχεση - Ανάλυση ψηφιακών πειστηρίων, Ποινική Δικαιοσύνη, 4/2003

6. Αναστασόπουλος Δ., Η προστασία της ιδιωτικότητας κατά το άρθρο 8 της ΕΣΔΑ στο ψηφιακό περιβάλλον, Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας, 3/2012

7. Ανδρεάδης-Παπαδημητρίου Π., Η πορνογραφία ανηλίκων στην εποχή του υπολογιστικού νέφους. Σκέψεις με αφορμή το Ν 4267/2014, Ποινική Δικαιοσύνη, 5/2015

8. Βαγενά Ε., Το νέο θεσμικό πλαίσιο για την καταπολέμηση του κυβερνοεγκλήματος Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας, 1/2017

9. Δασκαλόπουλος Στ., Ευρωπαϊκή Εντολή Έρευνας (Ε.Ε.Ε.): Ο νέος θεσμός Δικαστικής Συνεργασίας επί ποινικών υποθέσεων εντός της Ευρωπαϊκής Ένωσης, Ποινικά Χρονικά, 2/2018

10. Δημόπουλος Χ., Έκδοση εγκληματιών: Ευρωπαϊκή Εντολή Έρευνας (Μέρος Β΄), Ποινική Δικαιοσύνη, 6/2018

11. Καϊάφα – Γκμπάντι Μ., Ποινικό δίκαιο και καταχρήσεις της Πληροφορικής, Αρμενόπουλος, 7/2007

12. Καραφλός Α., Ανακύπτοντα νομικά ζητήματα κατά την πρακτική εφαρμογή του ευρωπαϊκού εντάλματος σύλληψης, Ποινικά Χρονικά, 1/2013

13. Καραγκούνη Δ., Η επιβολή περιορισμών στα μέσα κοινωνικής δικτύωσης μετά τον νέο γερμανικό Νόμο περί Βελτίωσης της Επιβολής της Νομοθεσίας στα Κοινωνικά Δίκτυα (Netzwerkdurchsetzungsgesetz) - Επίθεση στην ελευθερία έκφρασης ή αναγκαίο μέσο καταπολέμησης της διαδικτυακής εγκληματικότητας;, Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας, 3/2018

14. Κατσιρώδης Α., Ο Νέος Κανονισμός Προσωπικών Δεδομένων και η ποινική προστασία αυτών, Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας, 2/2018

15. Λαχανά Κ.-Χ., Εξερευνώντας διαχρονικά τη μετάβαση από το παρελθόν στο παρόν status της προληπτικής διατήρησης δεδομένων εντός των ευρωπαϊκών δικαιοταξιών Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας, 3/2013

16. Μήτρου Λ., Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος, Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας, 4/2015

17. Μανιάτης Α., Δικαστική των Ηλεκτρονικών Υπολογιστών, Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας, 4/2011

18. Μεταξάκης Ε., Η ποινική προστασία του Ν 2472/1997 δεν εκτείνεται μόνο σε «κρυφά» προσωπικά δεδομένα, Πειραϊκή Νομολογία, 3/2017

19. Μπουρμάς Γ., Η νομιμότητα των ερευνών σε ηλεκτρονικά δίκτυα και δεδομένα στις περιπτώσεις εγκλημάτων στον Κυβερνοχώρο, Ποινική Δικαιοσύνη, 5/2019

20. Μυλωνόπουλος Χρ., Χωρεί έκδοση στις ΗΠΑ για νομιμοποίηση κρυπτονομισμάτων (bitcoin) προερχομένων από εγκληματική δραστηριότητα;, Ποινικά Χρονικά, 3/2018

21. Νούσκαλης Γ., Η ποινική προστασία προσωπικών δεδομένων μετά τον Κανονισμό 679/2016 και το σχετικό ελληνικό νομοσχέδιο. Ορισμένες πρώτες σκέψεις και επισημάνσεις, Ποινική Δικαιοσύνη, 3/2018

22. Νταφόπουλος Δ./ Σάικας Π./ Σαΐτη Μ., Ποινική ευθύνη νομικών προσώπων και επιχειρήσεων – Σύγχρονες εξελίξεις, Pro Justitia 1/2018

23. Παπαπροδρόμου Γ., Ο ρόλος της Δίωξης Ηλεκτρονικού Εγκλήματος στην πρόληψη και την αντιμετώπιση του κυβερνο-εγκλήματος, Εγκληματολογία, 1/2017

24. Παναγοπούλου-Κουτνατζή Φ., Διαδίκτυο των πραγμάτων (Internet of Things-IoT): Αποικισμός της καθημερινής ζωής ή νέα τεχνολογική πρόκληση;, Δίκαιο Μέσων Ενημέρωσης & Επικοινωνίας, 3/2014

25. Παπαδόπουλος Μ. – Ευγενίδη Π., Νεφοϋπολογιστική (cloud computing) και προστασία προσωπικών δεδομένων, Δίκαιο Μέσων Ενημέρωσης & Επικοινωνίας, 2/2016.

26. Παπαθανασίου Α. / Γέρμανος Γ., Το φαινόμενο του crime-as-a-service για βίαια εγκλήματα στο Σκοτεινό Διαδίκτυο (Dark Web), Εγκληματολογία, 1/2017

27. Πιπύρο Κ./Μήτρου Λ., Κυβερνοεπίθεση ή κυβερνοπόλεμος;, Δίκαιο Μέσων Ενημέρωσης & Επικοινωνίας, 2/2018

28. Σπινέλλη Κ., Εισαγωγικές παρατηρήσεις από τη συντονίστρια της Β΄ Συνεδρίας: Ηλεκτρονικά εγκλήματα και τρομοκρατία, Εγκληματολογία, 1/2017

29. Σπυρόπουλος Φ., Η διασπορά ψευδών ειδήσεων στην εποχή των "fake news". Ανάλυση του άρθρου 191 ΠΚ ενώπιον των σύγχρονων (τεχνολογικών) προκλήσεων, Ποινική Δικαιοσύνη, 3/2019

30. Τζαννετής Α., Η Ευρωπαϊκή Εντολή Έρευνας, Ποινικά Χρονικά, 2/2018

31. Τζώρτζη Β., Προστασία δεδομένων προσωπικού χαρακτήρα: οι σημαντικότερες αλλαγές από τον Γενικό Κανονισμό, Εφαρμογές Δημοσίου Δικαίου, 2-3/2017

32. Τομαράς Κ., Είναι πράγματι παράνομα αποδεικτικά μέσα τα μηνύματα κινητού τηλεφώνου (SMS);, Εφαρμογές Αστικού Δικαίου & Πολιτικής Δικονομίας, 7/2018

33. Φαραντούρης Ν., Σύγχρονες εγκληματικές δράσεις στο Διαδίκτυο - Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του Hacking και του φαινομένου της μόλυνσης με ιούς, Ποινική Δικαιοσύνη, 2/2003

iii. Ελληνικά Νομοθετικά Κείμενα

1. Αιτιολογική Έκθεση, Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις, COM(2018) 225 final

2. Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, Το ευρωπαϊκό θεματολόγιο για την ασφάλεια, COM(2015) 185 final

3. Απόφαση-Πλαίσιο 2008/978/ΔΕΥ του Συμβουλίου, της 18ης Δεκεμβρίου 2008, σχετικά με το ευρωπαϊκό ένταλμα συγκέντρωσης αποδεικτικών στοιχείων προς λήψη αντικειμένων, εγγράφων και δεδομένων για χρήση σε ποινικές διαδικασίες

4. 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

5. Απόφαση-Πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου, της 28ης Μαΐου 2001, "για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών", ΕΕ L 149/1 της 2.6.2001

6. Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής με θέματα «Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις», ΕΕ C 367/90 της 10.10.2018

7. Γνωμοδότηση 23/2018 του Συμβουλίου Προστασίας Δεδομένων σχετικά με τις προτάσεις της Επιτροπής για την Ευρωπαϊκή Εντολή Υποβολής και την Ευρωπαϊκή Εντολή Διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις [άρθρο 70 παράγραφος 1 στοιχείο β)] της 26ης Σεπτεμβρίου 2018

8. Δελτίο Τύπου του Συμβουλίου της ΕΕ της 8/3/2019

9. Νόμος 4411/2016 (ΦΕΚ Α' 142/3-8-2016), Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών - Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις

10. Νόμος 3917/2011, ΦΕΚ Α' 22/21-2-2011

11. Νόμος 4489/2017 (ΦΕΚ 140/Α/21-9-2017)

12. 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 119/1 της 4.5.2016

13. Κοινή δράση 98/428/ΔΕΥ της 29ης Ιουνίου 1998 που θεσπίστηκε από το Συμβούλιο βάσει του άρθρου Κ.3 της συνθήκης για την Ευρωπαϊκή Ένωση, για τη δημιουργία ευρωπαϊκού δικαστικού δικτύου

14. Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018 για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών, ΕΕ L 321/36 της 17.12.2018

15. Οδηγία (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Σεπτεμβρίου 2015 για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας των πληροφοριών, ΕΕ, L 241/1 της 17.9.2015

16. Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, ΕΕ L 194/1 της 19.7.2016

17. Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου, ΕΕ L 119/89 της 4.5.2016

18. Οδηγία (ΕΕ) 2019/713 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, "για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών και την αντικατάσταση της απόφασης-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου", ΕΕ L 123/18 της 10.5.2019

19. Οδηγία 2011/92/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 2011, σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου, ΕΕ L 335/1 της 17.12.2011

20. Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ΕΕ L 218/8 της 14.8.2013

21. 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

22. Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών

23. Οδηγία (ΕΕ) 2017/541 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2017, για την καταπολέμηση της τρομοκρατίας και την αντικατάσταση της απόφασης-πλαισίου 2002/475/ΔΕΥ του Συμβουλίου και για την τροποποίηση της απόφασης 2005/671/ΔΕΥ του Συμβουλίου, ΕΕ L 88/6 της 31.3.2017

24. Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου, ΕΕ L 119/89 της 4.5.2016

25. Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, ΕΕ L 201/37 της 31.7.2002

26. Οδηγία 2010/64/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Οκτωβρίου 2010 , σχετικά με το δικαίωμα σε διερμηνεία και μετάφραση κατά την ποινική διαδικασία, ΕΕ L 280/1 της 26.10.2010

27. Οδηγία 2012/13/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 22ας Μαΐου 2012 , σχετικά με το δικαίωμα ενημέρωσης στο πλαίσιο ποινικών διαδικασιών, ΕΕ L 142/1 της 1.6.2012

28. Οδηγία 2013/48/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 22ας Οκτωβρίου 2013 , σχετικά με το δικαίωμα πρόσβασης σε δικηγόρο στο πλαίσιο ποινικής διαδικασίας και διαδικασίας εκτέλεσης του ευρωπαϊκού εντάλματος σύλληψης, καθώς και σχετικά με το δικαίωμα ενημέρωσης τρίτου προσώπου σε περίπτωση στέρησης της ελευθερίας του και με το δικαίωμα επικοινωνίας με τρίτα πρόσωπα και με προξενικές αρχές κατά τη διάρκεια της στέρησης της ελευθερίας, ΕΕ L 294/1 της 6.11.2013

29. Οδηγία (ΕΕ) 2016/343 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Μαρτίου 2016, για την ενίσχυση ορισμένων πτυχών του τεκμηρίου αθωότητας και του δικαιώματος παράστασης του κατηγορουμένου στη δίκη του στο πλαίσιο ποινικής διαδικασίας, ΕΕ L 65/1 της 11.3.2016

30. Οδηγία (ΕΕ) 2016/800 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαΐου 2016, σχετικά με τις δικονομικές εγγυήσεις για τα παιδιά που είναι ύποπτοι ή κατηγορούμενοι στο πλαίσιο ποινικών διαδικασιών, ΕΕ L 132/1 της 21.5.2016

31. Οδηγία (ΕΕ) 2016/1919 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Οκτωβρίου 2016, σχετικά με τη δικαστική αρωγή για υπόπτους και κατηγορουμένους στο πλαίσιο ποινικών διαδικασιών και για καταζητούμενους σε διαδικασίες εκτέλεσης του ευρωπαϊκού εντάλματος σύλληψης, ΕΕ L 297/1 της 4.11.2016

32. Περίληψη της Εκτίμησης Επιπτώσεων που συνοδεύει το έγγραφο Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις και Πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον ορισμό νόμιμων εκπροσώπων με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών, SWD(2018) 119 final

33. Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες), 10.1.2017, COM(2017) 10 final

34. Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις, COM(2018) 225 final

35. Πρόταση Οδηγίας σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον ορισμό νόμιμων εκπροσώπων με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών, COM(2018) 226 final

36. Σύμβαση της Βουδαπέστης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (CETS αριθ. 185)

37. Συμφωνία μεταξύ της Ευρωπαϊκής Ένωσης και της Ιαπωνίας για την Αμοιβαία Δικαστική Συνδρομή επί ποινικών υποθέσεων, ΕΕ L 39/19 της 12.2.2010

iv. Ξενόγλωσση βιβλιογραφία

1. Casey, E., 2011, Digital Evidence and Computer Crime, Academic Press

2. Clough, J., 2010, Principles of Cybercrime, Cambridge University Press

3. Mason, S., 2012, Electronic Evidence, LexisNexis

4. Millard, C., 2013, Cloud Computing Law, OUP

5. Summers, S., et. Al., 2014, The Emergence of EU Criminal Law: Cybercrime and the regulation of the Information Society, Hart Publishing

6. Walden, I., 2016, Computer crimes and digital investigations, Oxford

7. Biasiotti M., Mifsud Bonnici J., Cannataci J., Turchi F. (eds) Handling and Exchanging Electronic Evidence Across Europe. Law, Governance and Technology Series, vol 39. Springer, Cham, 2018

8. Kostoris R. (eds) Handbook of European Criminal Procedure. Springer, Cham

9. Synodinou TE., Jougleux P., Markou C., Prastitou T. (eds) EU Internet Law. Springer, Cham

10. Rafaraci T., Belfiore R. (eds) EU Criminal Justice. Springer, Cham

ν. Ξενόγλωσση Αρθρογραφία

1. Paul de Hert, Vagelis Papakonstantinou, The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for, Computer Law & Security Review, Volume 25, Issue 5, 2009

2. Thomas Marquenie, The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework, Computer Law & Security Review: The International Journal of Technology Law and Practice, 2017

3. Catherine Jasserand, Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?, Computer Law & Security Report 34(1), 2017

4. Mireille Caruana, The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement, International Review of Law Computers & Technology, September 2017

5. Paul de Hert, Vagelis Papakonstantinou, The New Police and Criminal Justice Data Protection Directive: A First Analysis, New Journal of European Criminal Law, 7(1), 2016

6. B.J. Koops and M. Goodwin, "Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities International Law", in Tilburg Law School Research Paper No. 5/2016, 2014

7. L. Buono, The genesis of the European Union's new proposed legal instrument(s) on e-evidence, ERA Forum 3/19, σελ. 307

8. B. Jerman Blažič/T. Klobučar, Advancement in Cybercrime Investigation – The New European Legal Instruments for Collecting Cross-border E-evidence σε Information Technology and Systems - Proceedings of ICITS 2019, σελ. 871-877

9. Dr. Stanislaw Tosza, The European Commission's Proposal on Cross-Border Access to E-Evidence, eucrim 4/2018, σελ. 215

10. Sebastian Cording / Lena Götzinger, Der CLOUD Act aus europäischer Sicht, Computer Und Recht: Forum für die Praxis des Rechts der Datenverargeitung, Information und Automation, 10/2018, σελ. 636

11. Júlio Barbosa e Silva, The speciality rule in cross-border evidence gathering and in the European Investigation Order—let's clear the air, ERA Forum, Volume 19, Issue 3, March 2019, σελ. 485

12. Jennifer Daskal, Unpacking the CLOUD Act, eucrim 4/2018, σελ. 220

13. Marco Stefan / Gloria González Fuster, Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters - State of the art and latest developments in the EU and the US, CEPS Paper in Liberty and Security in Europe, 07/2018

14. Katalin Ligeti/Gavin Robinson, Cross-Border Access to Electroinc Evidence: Policy and Legislative Challenges, in: Sergio Carrera/Valsamis Mitsilegas, Constitutionalising the Security Union - Effectiveness, Rule of Law and Rights in Countering Terrorism and Crime, σελ. 108

15. Claudia Warken, Classification of Electronic Data for Criminal Law Purposes, eucrim 4/2018, σελ. 226

vi. Ξενόγλωσσα Νομοθετικά Κείμενα

1. Council of the European Union, Handbook on the practical application of the EU-U.S. Mutual Legal Assistance and Extradition Agreements, Brussels, 25 March 2011, 8024/11

2. Council of the European Union, Review of the 2010 EU-US MLA Agreement - Examination of draft texts, Brussels, 7 April 2016, 7403/16

3. Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 12 June 2019, 10128/19

4. Council Decision authorising the European Commisson to participate, on behalf of the European Union, in negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime, 12 June 2019, 10129/19

5. Prof. Martin BÖSE, An assessment of the Commission's proposals on electronic evidence (Study Requested by the LIBE committee), September 2018

6. Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 5.2.2019, COM(2019) 70 final

7. Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), 5.2.2019, COM(2019) 71 final

8. Cybercrime Convention Committee (T-CY), T-CY Guidance Note # 3, Transborder access to data (Article 32), adopted by the 12th Plenary of the T-CY on 2–3 December 2014, T-CY (2013)7 E

9. Commission, Staff Working Document, 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 Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD (2018) 118 final, 17 April 2018

10. Explanatory Report to the Convention on Cybercrime

11. E-CODEX, Criminal Justice – Mutual Legal Assistance

12. Council of the European Union, Review of the 2010 EU-US MLA Agreement - Examination of draft texts, Brussels, 7 April 2016, 7403/16

13. Agreement on mutual legal assistance between the European Union and the United States of America, EE L 181/34 της 19.7.2003

14. Presidency Conclusions of the Tampere European Council, 15 and 16 October 1999

15. European Commission, Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the

United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Brussels, 5.2.2019 COM(2019) 70 final

16. Eurojust / Europol, Common challenges in combating cybercrime, 7021/17

17. EPDB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (annex)

18. Sergio Carrera/Gloria González Fuster/Elspeth Guild/Valsamis Mitsilegas, Access to Electronic Data by Third-Country Law Enforcement Authorities Challenges to EU Rule of Law and Fundamental Rights, Centre for European Policy Studies (CEPS), Brussels, 2015

19. Collaborative Project EVIDENCE, "European Informatics Data Exchange Framework for Courts and Evidence", D3.1 Overview of existing legal framework in the EU Member States

20. Koops & Goodwin, Cyberspace, the cloud, and cross-border criminal investigation, 2014

21. Opinion of the T-CY on the competent authority for issuing a preservation request under Articles 29 and 35 Budapest Convention, 28 November 2017, T-CY (2017)18

22. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken – NetzDG

23. Statement of the Article 29 Working Party, 29 November 2017, Data protection and privacy aspects of cross-border access to electronic evidence

24. Meijers Committee, CM1809 Comments on the proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters, 18 July 2018

25. Council of Bars and Law Societies of Europe (CCBE), CCBE position on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, 19/10/2018
26. Public Consultation on improving cross-border access to electronic evidence, BSA | The Software Alliance's supplemental position paper, October 2017

27. Electronic Communications and Privacy Act 1986 (ECPA)

28. Stored Communications Act – SCA

29. Clarifying Lawful Overseas Use of Data Act (CLOUD Act)

vii. Νομολογία

1. ΓνωμΕισΑΠ 09/2009

2. ΓνωμΕισΑΠ 12/2009

3. ΓνωμΕισΑΠ 09/2011

4. Εγκύκλιο ΕισΑΠ 2/22-5-2019, ΠοινΔικ 5/2019, σελ. 644

5. ΑΠ 711/2011 (ΠοινΔικ 2012, 518)

6. ΑΠ 203/2014 (ΠοινΧρ 2015, 103)

7. ΣτΕ 1593/2016 (ΔιΜΕΕ 2016, 637, με σημ. Γ. Τσόλια)

8. Απόφαση ΔΕΕ της 21ης Δεκεμβρίου 2016C-203/15 και C-698/15, Tele2 Sverige AB

9. Προτάσεις του Γενικού Εισαγγελέα της 3ης Μαΐου 2018, Υπόθεση C-207/16 Ministerio Fiscal

10. States v. Microsoft Corp.

Κυρώσεις για λογοκλοπή

Η λογοκλοπή είναι ένα πολύ σοβαρό παράπτωμα. Με απόφαση με το άρθ. 7.2 του Κανονισμού «σε περιπτώσεις λογοκλοπής ή παράλειψης αναφοράς στη μεταπτυχιακή Διπλωματική Εργασία, η ελάχιστη κύρωση, μετά από απόφαση της ΕΔΕ, είναι η υποχρέωση του φοιτητή να επιλέξει άλλον επιβλέποντα καθηγητή με διαφορετικό θέμα Διπλωματικής και να επαναλάβει το τρίτο εξάμηνο με ανάλογες πρόσθετες οικονομικές υποχρεώσεις, ενώ μέγιστη κύρωση μπορεί να είναι η οριστική διαγραφή του από το Πρόγραμμα. Εάν έχει ήδη αποφοιτήσει, ανακαλείται το Μεταπτυχιακό Δίπλωμα Ειδίκευσης και προωθείται το θέμα στο Δικαστικό Γραφείο του Πανεπιστημίου για την έναρξη των ανάλογων νομικών διαδικασιών».