ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2021-2022

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
της Μαρίας Τοπαλσάββα (Α.Μ.:ΜΔΙ 2048)

ΔΙΑΣΥΝΟΡΙΑΚΗ ΠΡΟΣΒΑΣΗ ΣΤΙΣ ΨΗΦΙΑΚΕΣ ΑΠΟΔΕΙΞΕΙΣ ΚΑΙ ΤΟ ΣΧΕΔΙΟ ΚΑΝΟΝΙΣΜΟΥ E-EVIDENCE

Επιβλέπουσα

Ευαγγελία Μήτρου

Πειραιάς, Ιούνιος, 2022

ΑΦΙΕΡΩΣΗ

Στη μητέρα μου Ιωάννα για την υποστήριξη της και την αγάπη της όλα αυτά τα χρόνια.

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.

Abstract

Today, criminal acts can be carried out rapidly over the Internet from the farthest corners of the globe and develop their criminal effects in many countries simultaneously. At the same time, electronic evidence that could lead to the discovery of the perpetrator or prove his guilt can be stored anywhere in the world. Thus, the cooperation of the Law Enforcement Authorities of all the countries of the world becomes more necessary than ever to deal with Cybercrime. Currently, the provisions of the International Cybercrime Convention are applicable to access to electronic evidence worldwide. At European Union (EU) level, the main "tool" of the Authorities is the European Investigation Mandate. However, the majority of internet companies - "giants" are based in the United States of America (USA). A Mutual Legal Assistance Agreement has been signed between the EU and the US since 2003 and has been implemented since 2010. Finally, the large volume of requests for assistance from European authorities to the US and the need for faster access to electronic evidence, mainly due to their volatile nature, have created a new model of cooperation: US law allows Service Providers to work directly with the Law Enforcement Authorities of other States, such as the EU States, but with some significant limitations. The need to establish effective institutions for cross-border co-operation, particularly in the field of electronic evidence in criminal matters, has recently led to intense discussions and negotiations, both at European and global level.

On 17 April 2018, the Commission adopted two legislative proposals: the Proposal for a Regulation on the European Submission Mandate and the European Mandate for the Keeping of Electronic Evidence in Criminal Matters and the Proposal for a Directive establishing harmonized rules for the appointment of legal representatives for the purpose of appointing legal representatives. evidence in criminal proceedings, which complements the above Regulation. Developments in the field of electronic evidence in criminal cases

preceded in the USA, where on March 23, 2018, the United States Congress passed the Clarifying Lawful Use of Overseas Data (CLOUD) Act, to clarify the legal use of data in the United States. abroad. Among other things, this law authorizes the US executive to enter into agreements with foreign governments, according to which foreign governments can gain quick access to the data, which is kept within the territory of the USA.

Thus paved the way for the start of negotiations between the US and the EU for the signing of a Mutual Assistance Agreement in the field of electronic evidence in criminal cases, negotiations, which officially began on June 6, 2019. Finally, globally, the same The European Council today authorized the European Commission to negotiate on behalf of the EU the Second Additional Protocol to the Council of Europe Convention on Cybercrime.

Ευχαριστίες

Ολοκληρώνοντας τις σπουδές μου στο Πρόγραμμα Μεταπτυχιακών Σπουδών (ΠΜΣ) «Δίκαιο και Τεχνολογίες Πληροφορικής και Επικοινωνιών» με την παράδοση της παρούσας εργασίας με θέμα «Διασυνοριακή Πρόσβαση στις Ψηφιακές αποδείξεις και το σχέδιο κανονισμού E-evidence». Τα συναισθήματα 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 σε μια δύσκολη περίοδο της πανδημίας του κορωνοιού.

Παρότι δεν είχαμε την ευκαιρία να απολαύσουμε την δια ζώσης εκπαίδευση και να αλληλεπιδράσουμε καθηγητές και μαθητές εντός του χώρου του Πανεπιστημίου νιώθω ευγνωμοσύνη και ιδιαίτερη τιμή που βρισκόμουν και εγώ ανάμεσα στα άτομα που συμμετείχαν σε αυτό το μεταπτυχιακό πρόγραμμα. Η ψηφιακή αίθουσα και η εξ' αποστάσεως εκπαίδευση έγιναν αναπόσπαστα στοιχεία για όλους μας αυτή την ακαδημαϊκή χρονιά και μας έφεραν πιο κοντά στην σύγχρονη τεχνολογία.

Έχοντας αποκομίσει πολλά εφόδια και καρπούς θα ήθελα να ευχαριστήσω θερμά τον Διευθυντή του Προγράμματος, Καθηγητή κ. Γκρίτζαλη Στέφανο αλλά και όλους τους διδάσκοντες του μεταπτυχιακούς προγράμματος για τις γνώσεις που μου μεταλαμπάδευσαν. Επίσης θερμές ευχαριστίες οφείλω στον κ. Αναστάσιο Παπαθανασίου, Αστυν. Υπ/ντη της Δ/νσης Δίωξης Ηλ. Εγκλήματος της ΕΛ.ΑΣ. για την βοήθεια και συνδρομή του ως προς την ευχερέστερη κατανόηση των διαδικασιών αναγνώρισης, συλλογής και κατάσχεσης ψηφιακών δεδομένων και διερεύνησης του εγκλήματος στον Κυβερνοχώρο.

Ιδιαίτερες ευχαριστίες οφείλω στην επιβλέπουσα για τη διπλωματική μου εργασία Καθηγήτρια κ.α Μήτρου Ευαγγελία για την πολύτιμη υποστήριξη και καθοδήγηση της στη διεκπεραίωση της διπλωματικής εργασίας.

Πίνακας περιεχομένων

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

Ελληνική

ΑΔΣΠΥ= Αμοιβαία Δικαστική Συνδρομή σε Ποινικές Υποθέσεις

Αρ.= Άρθρο

Αριθ.= Αριθμός

Αστ. Υπ/ντη= Αστυνομικός Υποδιευθυντής

Βλ. = Βλέπε

ΓΚΠΔ= Γενικός Κανονισμός Προσωπικών Δεδομένων

ΔΕΥ= Συμβούλιο Δικαιοσύνης και Εσωτερικών Υποθέσεων

Δ/νσης= Διεύθυνσης

ΕΑΔΠΑ= εκτέλεση των αποφάσεων δέσμευσης περιουσιακών ή αποδεικτικών στοιχείων στην ΕΈ

Ε.Ε= Ευρωπαϊκή Ένωση

Ε.Ε.Ε= Ευρωπαϊκή Εντολή Έρευνας

ΕΕΕυρΔ= Ελληνική Επιθεώρηση Ευρωπαϊκού Δικαίου

ΕΕΔ= Ευρωπαϊκή Επιτροπή Δεοντολογίας

Ε.Ε.Σ.Α= Ευρωπαϊκή Εντολή για τη συλλογή αντικειμένων, εγγράφων και στοιχείων σε ποινικές υποθέσεις

ΕΕΥ= Ευρωπαϊκή Εντολή Υποβολής Στοιχείων

ΕΚ= Ευρωπαϊκού Κοινοβουλίου

Εκδ.= Έκδοση/εις

ΕΛ.ΑΣ= Ελληνική Αστυνομία

Ε.Σ.Δ.Α= Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου

Ε.Υ.Π.= Εθνικής Υπηρεσίας Πληροφοριών

Ηλ. Εγκλήματος= Ηλεκτρονικού Εγκλήματος

Κλπ= Και λοιπά

Κ.=Κεφάλαιο

ΚΜ= Κράτος Μέλος

ΚΠΔ= Κώδικας Ποινικής Δικονομίας

Ν.= Νόμος

ό.π= όπως παραπάνω

παρ.= Παράγραφος

ΠοινΔικ= Ποινική Δικονομία

ΠοινΧρ= Ποινικά Χρονικά

Π.Δ= Προεδρικό Διάταγμα

ΠΚ= Ποινικός Κώδικας

ΠΜΣ= Πρόγραμμα Μεταπτυχιακών Σπουδών

π.χ= παραδείγματος χάρη

ΣΕΕ= Συνθήκη για την Ευρωπαϊκή Ένωση

σελ./σ.= σελίδα/ες

ΣΛΕΕ= Συνθήκη για την λειτουργία Ευρωπαϊκής Ένωσης

ΤΠ.= Τεχνολογία Πληροφοριών

ΤΣΡ= Τυποποιημένες Συμβατικές Ρήτρες

ΦΕΚ= Φύλλα Εφημερίδας της Κυβέρνησης

Ξένη

EU=European Union

EU-LISA= European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

GDPR=General Data Protection Regulation=Γενικός Κανονισμός Προστασίας Δεδομένων

IP=Internet Protocol

ISP= Internet Service Provider

P.p= Pages

USA=United States of America

ΕΙΣΑΓΩΓΗ

i) Τα Ηλεκτρονικά αποδεικτικά στοιχεία και η δυσκολία διασυνοριακής πρόσβασης σε αυτά

Ο διεθνής χαρακτήρας του διαδικτύου επιτρέπει σε μια εταιρεία παροχής υπηρεσιών να παρέχει τις υπηρεσίες της οπουδήποτε στον κόσμο και σε πολλά κράτη ταυτόχρονα, χωρίς όμως να έχει απαραίτητα την απαιτούμενη εταιρική παρουσία, προσωπικό ή εγκαταστάσεις στα κράτη αυτά. Πολλά από τα δεδομένα που παράγονται αποθηκεύονται ενώ κάποια άλλα δεν υφίστανται επεξεργασία αλλά ούτε και αποθηκεύονται. Το γεγονός αυτό οδηγεί με τη σειρά του στη δυσκολία των διωκτικών αρχών άλλων κρατών να αποκτούν πρόσβαση σε αυτά.

Βασικό χαρακτηριστικό των ηλεκτρονικών αποδεικτικών στοιχείων είναι ο ιδιαίτερα ευμετάβλητος χαρακτήρας τους, ο οποίος είναι και αυτός που τα διαφοροποιεί από τα συνηθισμένα «παραδοσιακά» αποδεικτικά στοιχεία. Επιπλέον, τα ηλεκτρονικά μέσα μεταφέρονται με μεγαλύτερη ταχύτητα από ένα κράτος σε ένα άλλο, από ήπειρο σε ήπειρο, μπορούν να τροποποιούνται και να διαγράφονται με μεγαλύτερη ευκολία. Τα ψηφιακά αποδεικτικά στοιχεία είναι «εύθραυστα», καθώς μπορούν επίσης να καταστραφούν από χρήστες άπειρους σε ζητήματα πρόσβασης και χειρισμού.[1] Τα αποδεικτικά στοιχεία πρέπει να εξεταστούν και να αξιολογηθούν αλλά τις περισσότερες φορές στα εγκλήματα στον κυβερνοχώρο δεν υπάρχουν φυσικές αποδείξεις στον τόπο τέλεσης τους.[2]

[1]Mitrakas, A.,Zaitch, D., "Law, Cybercrime and digital forensics: Trailling Digital Suspects", Kanellis P., Kiountouzis, E., Kolokontronis N.Drakoulis, M.(Eds), Digital Crime and Forensic Science in Cyberspace, London 2006, pp. 267-290 και Maria Karyda, Lilian Mitrou, "Internet Forensics: Legal and Technical issues", University of the Aegean, Deparntment of Information and Communication Systems Engineering, Karlovassi, Samos

[2]Nykodym N., Taylor, R.,Vilela, J., "Criminal Profiling and Insider cyber crime", Digital Investigation, Vol. 2 issue 4, 2005, pp. 261-265 και Maria Karyda, Lilian Mitrou, "Internet Forensics: Legal and Technical issues", University of the Aegean, Department of Information and Communication Systems Engineering, Karlovassi, Samos

Οι προαναφερόμενες δυσκολίες κατά τη διασυνοριακή πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία δυσκολεύουν, με τη σειρά τους, την αποτελεσματική έρευνα και δίωξη του εγκλήματος με το τρέχον νομικό σύστημα. Ο βασικός λόγος που οι έρευνες επί ψηφιακών εγκλημάτων δεν αποδίδουν έγκειται στην έλλειψη της δικαστικής συνεργασίας μεταξύ των δημοσίων αρχών, στην απουσία άμεσης συνεργασίας μεταξύ δημόσιων αρχών και παρόχων υπηρεσιών διαδικτύου και στην περιορισμένη πρόσβαση των δημοσίων αρχών σε ηλεκτρονικά αποδεικτικά στοιχεία.

Ως ηλεκτρονικό αποδεικτικό στοιχείο ορίζεται «κάθε πληροφορία που λαμβάνεται από μια ηλεκτρονική συσκευή ή ψηφιακό μέσο, το οποίο χρησιμεύει για να αποδείξει την αλήθεια ενός γεγονότος».[3] Σύμφωνα με το Ν.4411/2016 προστέθηκε στο άρθρο 13 του προϊσχύοντος ΠΚ ο ορισμός των ψηφιακών δεδομένων ο οποίος παραμένει αυτούσιος στο νέο ΠΚ. *«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».*

Σαφής και ολοκληρωμένος ορισμός δίνεται στην Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις. 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*

[3]CYBEX, "The admissibility of electronic evidence in court- Fighting against high-tech crime-Study", 2006, available at: www.cybex.es

στοιχείων, τα οποία συνίστανται σε αποθηκευμένα δεδομένα συνδρομητή, δεδομένα πρόσβασης, δεδομένα συναλλαγών και δεδομένα περιεχομένου».[4]

Δεδομένου ότι η χρήση και ο χειρισμός των δεδομένων και των πληροφοριών που συλλέγονται από τα εργαλεία ανίχνευσης είναι στενά συνδεδεμένα με την προτυποποίηση, η Ευρωπαϊκή Επιτροπή υπογραμμίζει την ανάγκη για τη δημιουργία τεχνικών προτύπων έτσι ώστε να διασφαλιστεί ότι τα δεδομένα που συλλέγονται είναι σύμφωνα με τις απαιτήσεις της νομοθεσίας για τη χρήση των δεδομένων αυτών στις δικαστικές διαδικασίες.[5]

ii) Ο μη οπτικός χαρακτήρας των αποδείξεων

Η έρευνα και η ποινική δίωξη του πληροφορικού εγκλήματος απαιτεί τον έλεγχο στα δεδομένα που έχουν αποθηκευτεί σ' ένα σύστημα. Πολλά από αυτά δεν είναι εύκολα αναγνώσιμα έως και καθόλου, αλλά είναι συγκεντρωμένα σε ηλεκτρονικές συσκευές μνήμης, οι οποίες αναγνωρίζονται μόνο από τον υπολογιστή. Το πρόβλημα εμφανίζεται από τη στιγμή που οι αρμόδιες εισαγγελικές αρχές αντιμετωπίζουν την έλλειψη ορατών και κατανοήσιμων αποδείξεων, που προκαλούνται από την ανωνυμία, τη συμπίεση ή την κωδικοποίηση των ηλεκτρονικά αποθηκευμένων πληροφοριών. Οι πληροφορίες, τα αρχεία και τα δεδομένα μπορούν να κλαπούν εύκολα χωρίς καν να μετακινηθούν ή να έρθουν σε επαφή με τον παραβάτη. Η μη εξουσιοδοτημένη πρόσβαση γίνεται εφικτή μέσω του τηλεφώνου ή ενός τερματικού, μορφοποιημένου σε ένα ασταθές μοντέλο ηλεκτρονικών μηνυμάτων. Χαρακτηριστικό είναι κατά τους

[4]Βλ. Κανονισμό του Ευρωπαϊκού κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις (SWD(2018) 118 final και SWD(2018) 119 final, https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52018PC0225

[5]Commission of the European Communites, "Green Paper on detection technologies in the work of Law Enforcement", Customs and other Security Authorities- COM,2006,474(final) και Maria Karyda, Lilian Mitrou, "Internet Forensics: Legal and Technical Issues", University of the Aegean, Department of Information and Communication Systems Engineering, Karlovassi, Samos

Michalowski και Pfuhl πως «το πληροφορικό έγκλημα είναι έγκλημα χωρίς σωματικότητα (disembodied crime).[6]

Επιπλέον, σε άμεση συνάφεια βρίσκεται και το γεγονός ότι οι τροποποιήσεις στα προγράμματα ή τα δεδομένα δεν αφήνουν ίχνη, ανάλογα αυτών που αξιοποιούνται στα πλαίσια της κλασικής απόδειξης των παραδοσιακών εγκλημάτων. Για παράδειγμα, η ανάλυση χειρόγραφου δεν υφίσταται πλέον στις ηλεκτρονικές βάσεις δεδομένων, άρα και στις υποθέσεις των πληροφοριακών εγκλημάτων.

iii) Η εξάλειψη των αποδείξεων και κωδικοποίηση των αποδείξεων

Οι κακόβουλοι χρήστες στην προσπάθεια τους να αποφύγουν την ποινική δίωξη εξαφανίζουν κυρίως μέσω ρυθμίσεων στα λειτουργικά συστήματα ενός υπολογιστή τα αποδεικτικά στοιχεία που υπάρχουν.

Εκτός από τον μη οπτικό χαρακτήρα των αποδείξεων, κάποιος δράστης μπορεί να δυσκολέψει τις διαδικασίες έρευνας και ποινικής δίωξης προστατεύοντας τα δεδομένα μέσω κάποιων μηχανισμών ασφαλείας, όπως οι κωδικοί πρόσβασης και η κρυπτογράφηση. Χρησιμοποιώντας αυτές τις τεχνικές, ο hacker ή ο υπάλληλος κάποιας εταιρείας έχουν τη δυνατότητα να παρεμποδίσουν τον έλεγχο της διασυνοριακής μεταφοράς δεδομένων με μια κωδικοποιημένη τηλεφωνική κλήση διαρκείας μερικών δευτερολέπτων είναι σε θέση να ολοκληρώσει τη μη εξουσιοδοτημένη μεταβίβαση κεφαλαίων. Ακόμα και στο πεδίο των παραβιάσεων της ιδιωτικότητας, οι κρυπτογραφικές τεχνικές καθιστούν δύσκολο τον έλεγχο των αποθηκευμένων πληροφοριών.[7]

[6]Michalowski και Pfuhl, 1991, σ. 98

[7]Βλ. Γρ. Λάζος, «ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΕΓΚΛΗΜΑ», εντοπισμός-δίωξη πληροφορικού εγκλήματος, σελ.219

v) Η πρόκληση της διασυνοριακής ροής πληροφοριών και το εφαρμοστέο δίκαιο

Η παγκόσμια διάσταση του διαδικτύου έρχεται σε αντίθεση με την επιβολή του κανόνα δικαίου: τα εθνικά σύνορα, τα συνοριακά σημεία ελέγχου και τα εθνικά όργανα επιβολής. Πλην των περιπτώσεων διακρατικής συνεργασίας για τα συγκεκριμένα θέματα όπως π.χ η παιδική πορνογραφία, δεν υπάρχει κάποιο είδος διεθνούς αστυνομίας του Internet που να μπορεί κατασταλτικά να επιβάλει κυρώσεις ή να εξαναγκάσει σε εφαρμογή των κανόνων[8]. Στο πλαίσιο των Συνόδων Κορυφής του ΟΗΕ για την Κοινωνία της Πληροφορίας το διεθνές Forum για την διακυβέρνηση του Internet(Internet Governance Forum)[9]αν και αποτελεί την αρχή για ένα είδος υπερεθνικής επιβολής ρυθμίσεων, πολύ περισσότερο ασχολείται με την διευθέτηση των τεχνικών ζητημάτων και την εξαγγελία γενικών κατευθυντήριων γραμμών ενώ η ρύθμιση καθημερινών καταστάσεων, ακολουθεί. Οι εξακριβώσεις αυτές δεν πρέπει να οδηγούν στο συμπέρασμα ότι το δίκαιο είναι ανεπαρκές στο να καθοδηγήσει ένα υπερεθνικό μόρφωμα, μολαταύτα είναι δύσκολο να βρεθεί ο εφαρμοστέος κανόνας, του αρμόδιου δικαιοδοτικού οργάνου και να εφαρμοστούν οι αποφάσεις. Οι δυσκολίες αυτές ομολογουμένως προκύπτουν επειδή γίνεται προσπάθεια εφαρμογής παραδοσιακών κανόνων βασιζόμενους σε γεωγραφικά σύνορα επί ενός νέου επικοινωνιακού μέσου που δεν γνωρίζει σύνορα και γεωγραφικούς περιορισμούς και όχι επειδή δεν υπάρχουν κανόνες ή επειδή οι κανόνες αυτοί δήθεν είναι αναποτελεσματικοί.[10]

[8]Βλ. Γιώργος Ν. Γιαννόπουλος, Επικ. Καθηγητής στη Νομική Σχολή ΕΚΠΑ, «Εισαγωγή στη Νομική Πληροφορική», Μια πρώτη προσέγγιση της σχέσης δικαίου και νέων τεχνολογιών, Νομική Βιβλιοθήκη,σελ.170-171

[9]Βλ.http://www.intgovforum.org Το Forum παραμένει αναποτελεσματικό μέχρι σήμερα, αφού στην ουσία τα εθνικά κράτη είναι οι κύριοι αποφασιστικοί παράγοντες.

[10]Βλ. Γιώργος Ν. Γιαννόπουλος, ό.π

ΠΡΩΤΟ ΜΕΡΟΣ:ΔΙΑΣΥΝΟΡΙΑΚΗ ΠΡΟΣΒΑΣΗ ΣΤΙΣ ΨΗΦΙΑΚΕΣ ΑΠΟΔΕΙΞΕΙΣ

ΕΙΣΑΓΩΓΙΚΑ

ι)Διασυνοριακή ροή προσωπικών δεδομένων

Η οικονομική και κοινωνική ολοκλήρωση της ευρωπαϊκής ένωσης οδηγεί στην αύξηση της διασυνοριακής ροής δεδομένων προσωπικού χαρακτήρα μεταξύ όλων των πρωταγωνιστών της οικονομικής και κοινωνικής ζωής των κρατών μελών, ιδιώτες ή Δημόσιο.[11]

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα είναι ελεύθερη τόσο εντός των ορίων της Ε.Ε., λόγω της εναρμόνισης των εθνικών νομοθεσιών των κρατών μελών με τις ρυθμίσεις των σχετικών Κοινοτικών Οδηγιών, αρκεί βέβαια να τηρούνται οι σχετικοί όροι και προϋποθέσεις[12] όσο και προς χώρες μη μέλη της Ευρωπαϊκής Ένωσης υπό όρους.

Κατά κύριο λόγο η αποστολή προσωπικών δεδομένων σε μη κοινοτική χώρα καταρχήν απαγορεύεται και κατ' εξαίρεση επιτρέπεται σύμφωνα με τις εγγυήσεις και τους περιορισμούς που ορίζονται στον Γενικό Κανονισμό για την προστασία των προσωπικών δεδομένων (GDPR) και του αντίστοιχου εφαρμοστικού Ν.4624/2019, εφόσον σε κάθε περίπτωση προηγουμένως

[11]Βλ. Απόστολος Γέροντας, 2002, «Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, εκδόσεις Αντ.Ν.Σάκκουλα, σελ.218

[12]Θεόδωρος Σιδηρόπουλος, «Το δίκαιο του Διαδικτύου», Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη, σελ. 209

διακριβωθεί πως η εν λόγω χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας.[13]

Λαμβάνεται υπόψη γι' αυτό ιδίως η φύση των δεδομένων, ο σκοπός και η διάρκεια της επεξεργασίας, οι σχετικοί γενικοί και ειδικοί κανόνες δικαίου, οι κώδικες δεοντολογίας, τα μέτρα ασφαλείας για την προστασία δεδομένων προσωπικού χαρακτήρα, καθώς και το επίπεδο προστασίας των χωρών προέλευσης, διέλευσης και τελικού προορισμού των δεδομένων.

Η διαβίβαση δεδομένων σε Τρίτη χώρα μπορεί να επιτραπεί κατά περίπτωση, ακόμα και αν δεν έχει χορηγηθεί σχετική άδεια, εφόσον υπογραφεί μεταξύ των μερών (εξαγωγέα-εισαγωγέα δεδομένων) συμφωνία κατά το πρότυπο και με τους όρους που ορίζονται στην **Απόφαση 2001/497/ΕΚ** της Ευρωπαϊκής Επιτροπής «σχετικά με τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τις τρίτες χώρες δυνάμει του άρθρου 26 παρ.4 της Οδηγίας 95/46/ΕΚ[14]», εκτός και αν ο αποδέκτης των δεδομένων ενεργεί απλώς ως εκτελών την επεξεργασία, οπότε θεωρείται ότι ενεργεί αποκλειστικά για λογαριασμό του εξαγωγέα υπευθύνου επεξεργασίας. Με βάση αυτή σύμβαση, η οποία μπορεί να συμπληρωθεί περαιτέρω από τα Συμβαλλόμενα Μέρη, είναι δυνατή η εξαγωγή προσωπικών δεδομένων από ένα κράτος μέλος της ΕΕ, άρα και από τη Χώρα μας, προς τρίτο κράτος[15]. Σε αυτήν την περίπτωση πρέπει να συναφθεί και να υπογραφεί συμφωνία μεταξύ εξαγωγέα και εκτελούντα την επεξεργασία με βάση τους όρους που προβλέπονται στην **Απόφαση 2002/16/ΕΚ**[16] της Ευρωπαϊκής Επιτροπής «σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προς τις τρίτες χώρες σε

[13]Έως σήμερα μόνο η Ελβετία, η Ουγγαρία και ο Καναδάς έχουν κριθεί ότι παρέχουν ικανοποιητικά επίπεδα προστασίας, βλ. Αποφάσεις της Ευρωπαϊκής Επιτροπής 2000/518/ΕΚ (ΕΕL 215/1), 2000/519/ΕΚ (ΕΕL 215/4) και 2002/2/ΕΚ (ΕΕL 2/13) αντίστοιχα.
[14]ΕΕL 181/19
[15]Βλ. Ιωάννης Δημ.Ιγγλεζάκης, Δίκαιο Πληροφορικής, Γ΄ έκδοση, εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη σελ.295
[16]Περισσότερα αναφέρονται και εξηγούνται παρακάτω

εκτελούντες επεξεργασία εγκατεστημένους σε τρίτες χώρες βάσει της Οδηγίας 95/46/ΕΚ»[17].

Τα βασικά σημεία της **Απόφασης 2001/497/ΕΚ** είναι τα εξής:

Α) τα συμβαλλόμενα μέρη θα πρέπει να αναφέρουν τις κατηγορίες προσωπικών δεδομένων και τους σκοπούς για τους οποίους αυτά διαβιβάζονται,

β)αναγνωρίζεται ότι τα πρόσωπα στα οποία αναφέρονται τα δεδομένα μπορούν να επικαλούνται ευθέως τις διατάξεις της σύμβασης, παρ'ότι δεν είναι οι ίδιοι συμβαλλόμενοι,

γ)ο εξαγωγέας δεδομένων αναλαμβάνει ορισμένες υποχρεώσεις, ιδίως ότι θα ενημερώσει τα πρόσωπα στα οποία αναφέρονται τα δεδομένα είναι ευαίσθητα, δ)αντίστοιχα, ο εισαγωγέας δεδομένων αναλαμβάνει υποχρεώσεις, μεταξύ των οποίων ότι θα τηρεί τις αρχές που αναφέρονται στο Παράρτημα 2,[18]

ε)τα συμβαλλόμενα μέρη υπέχουν ευθύνη απέναντι στα πρόσωπα στα οποία αναφέρονται τα δεδομένα, εάν αυτά υποστούν ζημία συνεπεία παραβίασης ορισμένων κρίσιμων διατάξεων της σύμβασης.

Απόφαση Υπ'αριθ. 2002/16/ΕΚ

Η Απόφαση 2001/497 συμπληρώνεται με την υπ'αριθ. Απόφαση 2002/16 Απόφαση η οποία έχει αναφερθεί και πιο πάνω, «σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε εκτελούντες επεξεργασία σε τρίτες χώρες, βάσει της οδηγίας 95/46/ΕΚ και η οποία περιέχει ορισμένες εναλλακτικές ρήτρες. Στη συνέχεια, εκδόθηκε η υπ'αριθ.2004/915 Απόφαση της Επιτροπής, με την οποία

[17]EEL 6/52,10.1.2002

[18]Συγκεκριμένα: περιορισμός του σκοπού, ποιότητα των δεδομένων, αναλογικότητα. Διαφάνεια, ασφάλεια και εμπιστευτικότητα, δικαιώματα πρόσβασης, διόρθωσης και κλειδώματος, περιορισμοί διαδοχικών διαβιβάσεων, ειδικές κατηγορίες δεδομένων, άμεση προώθηση προϊόντων και αυτοματοποιημένες αποφάσεις.

τροποποιήθηκε η υπ'αριθ.2002/16 Απόφαση και η οποία επίσης παραθέτει μια εναλλακτική δέσμη συμβατικών ρητρών, οι οποίες είναι περισσότερο «φιλικές» προς τον επιχειρησιακό κόσμο, καθώς οι ρήτρες που περιείχε η υπ'αριθ. 2001/497 Απόφαση επικρίθηκαν για το λόγο ότι επιβάρυναν υπέρμετρα τις επιχειρήσεις.

Η κύρια διαφορά της εν λόγω Απόφασης σε σχέση με την υπ'αριθ. 2001/497 είναι ότι η πρώτη περιλαμβάνει ένα σύστημα ευθύνης σύμφωνα με το οποίο ο εξαγωγέας των δεδομένων και ο εισαγωγέας των δεδομένων θα είναι αντίστοιχα υπεύθυνοι έναντι των προσώπων στα οποία αναφέρονται τα δεδομένα για τυχόν παραβιάσεις των συμβατικών τους υποχρεώσεων. Επίσης, ο εξαγωγέας των δεδομένων είναι επίσης υπεύθυνος εάν δεν καταβάλει εύλογες προσπάθειες για να εξασφαλίσει ότι ο εισαγωγέας των δεδομένων είναι σε θέση να ανταποκριθεί στις υποχρεώσεις του που προκύπτουν από τις συμβατικές ρήτρες και το υποκείμενο των δεδομένων μπορεί να στραφεί εναντίον του στην περίπτωση αυτή.

Απόφαση Υπ'αριθ. 2010/87/ΕΕ

Η διαβίβαση προσωπικών δεδομένων σε εκτελούντες της επεξεργασία σε τρίτες χώρες εκδόθηκε με την ανωτέρω απόφαση της Επιτροπής.[19] Σε αυτήν καθορίζονται τα ελάχιστα πληροφοριακά στοιχεία που οφείλουν τα συμβαλλόμενα μέρη στη σύμβαση που διέπει τη διαβίβαση και επιπλέον, περιέχει ειδικότητες τυποποιημένες συμβατικές ρήτρες σχετικά με την υπεργολαβία επεξεργασίας από έναν εκτελούντα επεξεργασία σε τρίτη χώρα (εισαγωγέα δεδομένων) των υπηρεσιών επεξεργασίας που παρέχει σε άλλους εκτελούντες επεξεργασίας (υπεργολάβους επεξεργασίας) εγκατεστημένους σε τρίτες χώρες. Υπεύθυνος απέναντι στο υποκείμενο δεδομένων είναι ο εξαγωγέας δεδομένων κατ' εξαίρεση μόνο δικαιούται να ασκήσει αυτό αγωγή κατά του εισαγωγέα δεδομένων εξαιτίας αθέτησης εκ

[19] ΕΕ L 39/5, 12.2.2010

μέρους του τελευταίου ή του υπεργολάβου επεξεργασίας κάποιας από τις υποχρεώσεις που προβλέπονται στις ρήτρες, σε περίπτωση που ο εξαγωγέας δεδομένων έπαυσε να υφίσταται από πραγματική ή νομική άποψη ή κατέστη αφερέγγυος. Τέλος, υπογραμμίζεται ότι η σύμβαση πρέπει να διέπεται από το δίκαιο του κράτους μέλους στο οποίο είναι εγκατεστημένος ο εξαγωγέας δεδομένων και το οποίο επιτρέπει σε δικαιούχο τρίτο να ζητήσει την εκτέλεση της σύμβασης.

ιι)Διεύρυνση της υποχρέωσης ενημέρωσης της Ευρωπαϊκής Επιτροπής από την Αρχή

Σύμφωνα με το άρθρο 25 παρ.4 του Ν.3471/2006, η υποχρέωση ενημέρωσης της Ευρωπαϊκής Επιτροπής από την Αρχή διευρύνεται και καταλαμβάνει και τις άδειες που χορηγεί η Αρχή για διασυνοριακή διαβίβαση προσωπικών δεδομένων, όταν μετά από ενέργειες της (η Αρχή) διαπιστώνει ότι ο υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις.[20]

Πρόκειται για την εναρμόνιση του Ν.2472/1997 προς τη διάταξη του άρθρου 26 παρ.3 εδ.α' της Οδηγίας 95/46. Σύμφωνα με το ίδιο άρθρο όμως, αν διατυπωθεί από άλλο κράτος μέλος ή την Επιτροπή ένσταση δεόντως αιτιολογημένη όσον αφορά την προστασία της ιδιωτικής ζωής και των θεμελιωδών δικαιωμάτων και ελευθεριών των προσώπων, η Επιτροπή θεσπίζει τα κατάλληλα μέτρα με τη διαδικασία που αναφέρεται στο άρθρο 31 παρ.2. Στη συνέχεια τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να συμμορφωθούν με την απόφαση της Επιτροπής.

Σκοπός λοιπόν της διεύρυνσης της υποχρέωσης της Αρχής είναι η παροχή δυνατότητας στα άλλα κράτη να ενημερώνονται για τις τυχόν άδειες που έχουν χορηγηθεί, μέσω του «μητρώου» που τηρεί η Ευρωπαϊκή Επιτροπή έτσι ώστε να μπορούν να ασκούν το παραπάνω δικαίωμα τους για υποβολή

[20]Βλ. Παναγιώτης Δ. Αρμαμέντος και Βασίλης Α. Σωτηρόπουλος, Προσωπικά δεδομένα, ερμηνεία κατ' άρθρο, οι τροποποιήσεις του Ν.2472/1997 απ' τους Ν. 3471/2006 και 3625/2007, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη, σελ.106

ένστασης.[21] Έτσι, αυτό έχει ως αποτέλεσμα την επίτευξη καλύτερης προστασίας και διαφύλαξης των προσωπικών δεδομένων.

Κατά συνέπεια, αν συντρέξουν οι όροι του άρθρου 26 παρ.3 της Οδηγίας, η Επιτροπή έχει τη δυνατότητα να ακυρώσει κατ' αποτέλεσμα με απόφαση της την άδεια της Αρχής. Τέλος, είναι σημαντικό να τονιστεί πως μια τέτοια απόφαση μπορεί στη συνέχεια να ελεγχθεί και δικαστικά με προσφυγή στο Δ.Ε.Κ από κράτος μέλος στο οποίο υπάγεται η Αρχή της οποίας η απόφαση ακυρώθηκε.

Α. ΔΙΚΑΣΤΙΚΗ ΣΥΝΕΡΓΑΣΙΑ

Α.1 Σύμβαση της Βουδαπέστης για το Έγκλημα στον Κυβερνοχώρο

Το γεγονός πως τα ηλεκτρονικά συστήματα επεξεργασίας δεδομένων προσωπικού χαρακτήρα αποτελούν ολοένα και περισσότερο είτε στόχο είτε εργαλείο εγκληματικών δραστηριοτήτων, δημιουργεί την ανάγκη ή καλύτερα την απαίτηση νέων διατάξεων του ποινικού δικαίου για την αντιμετώπιση της συγκεκριμένης πρόκλησης. Έτσι, το Συμβούλιο της Ευρώπης εξέδωσε διεθνή νομική πράξη, τη Σύμβαση της Βουδαπέστης, προκειμένου να αντιμετωπιστεί το ζήτημα των εγκληματικών πράξεων που διαπράττονται κατά και μέσω των ηλεκτρονικών δικτύων.[22]

Η Σύμβαση για το έγκλημα στον Κυβερνοχώρο εξακολουθεί να αποτελεί τη σημαντικότερη διεθνή συνθήκη που άπτεται των παραβιάσεων της νομοθεσίας μέσω του διαδικτύου ή άλλων δικτύων πληροφοριών. Επιβάλλει στα συμβαλλόμενα μέρη την υποχρέωση να προσαρμόζουν την ποινική νομοθεσία τους για την καταπολέμηση του hacking και των άλλων

[21]Βλ. Παναγιώτης Δ. Αρμαμέντος και Βασίλης Α. Σωτηρόπουλος, ό.π, σελ.106-107

[22]Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (2001), Σύμβαση για το έγκλημα στον κυβερνοχώρο, CETS αριθ.185, Βουδαπέστη, 23 Νοεμβρίου 2001, τέθηκε σε ισχύ την 1η Ιουλίου 2004, Η Σύμβαση υπογράφηκε από τα περισσότερα μέλη του Ευρωπαϊκού Συμβουλίου, τις ΗΠΑ, τον Καναδά, την Νότια Αφρική, την Ιαπωνία και στη συνέχεια προστέθηκαν και άλλα μέλη ενώ ακόμα και σήμερα εισέρχονται συνεχώς νέα.

παραβιάσεων ασφαλείας, μεταξύ των οποίων και οι παραβιάσεις των πνευματικών δικαιωμάτων, η απάτη με χρήση ηλεκτρονικών υπολογιστών, η παιδική πορνογραφία και άλλες παράνομες δραστηριότητες στον κυβερνοχώρο.[23]

Στόχος της Σύμβασης είναι η 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.[24] Ενώ επίσης στοχεύει και στο να θέσει τις βάσεις για άμεση και αποτελεσματική διεθνή συνεργασία για το ηλεκτρονικό έγκλημα.[25] Το πρόσθετο πρωτόκολλο στη Σύμβαση αφορά την ποινικοποίηση της ρατσιστικής και ξενοφοβικής προπαγάνδας μέσω των δικτύων ηλεκτρονικών υπολογιστών.[26]

Η Σύμβαση δεν αποσκοπεί ουσιαστικά στην προώθηση της προστασίας των δεδομένων προσωπικού χαρακτήρα όμως ποινικοποιεί δραστηριότητες οι οποίες είναι πιθανό να παραβιάζουν το δικαίωμα του υποκειμένου των δεδομένων στην προστασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Επιπρόσθετα, επιβάλλει στα συμβαλλόμενα μέρη την υποχρέωση να θεσπίσουν νομοθετικά μέτρα τα οποία θα επιτρέπουν στις οικείες εθνικές αρχές να υποκλέπτουν δεδομένα κίνησης και περιεχομένου.[27] Ακόμη, επιτάσσει στα συμβαλλόμενα μέρη να προβλέπουν, κατά την εφαρμογή της Σύμβασης, επαρκές επίπεδο προστασίας των δικαιωμάτων και των ελευθεριών του ανθρώπου, περιλαμβανομένων των δικαιωμάτων που

[23]Βλ. Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, έκδοση 2018, σελ.353
[24]Βλ. Κ. Βλαχόπουλος, «Ηλεκτρονικό Έγκλημα», 2007, εκδ. Νομική Βιβλιοθήκη, σελ. 137
[25]Βλ. Κ. Βλαχόπουλος, ό.π
[26]Βλ. Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, έκδοση 2018, σελ.353
[27]Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών(2001), Σύμβαση για το Έγκλημα στον Κυβερνοχώρο, CETS αριθμ.185, Βουδαπέστη,23 Νοεμβρίου 2001,άρθρα 20 και 21

κατοχυρώνονται με την ΕΣΔΑ, όπως το δικαίωμα προστασίας των προσωπικών δεδομένων[28].

Η Σύμβαση συνοδεύεται από την Επεξηγηματική της Έκθεση, ένα κείμενο ιδιαίτερα κατανοητό και επεξηγηματικό το οποίο εξαίρει την αξία της Πληροφορίας και των Τεχνολογιών Πληροφορικής και Επικοινωνίας, αναγνωρίζει τη σημασία που θα διαδραματίσουν στο μέλλον, ενώ ταυτόχρονα αναδεικνύει τα προβλήματα που δημιουργούνται με τα νέα δεδομένα και τονίζει την επιτακτική ανάγκη νομοθετικής ρύθμισης του νεοεμφανιζόμενου χώρου που αποκαλεί «Κυβερνοχώρο». Τόσο η Σύμβαση της Βουδαπέστης όσο και η Επεξηγηματική Έκθεση αποτελούν πρωταρχικά για την εποχή εκείνη κείμενα τα οποία βρίσκουν εφαρμογή ως και σήμερα. Ωστόσο πρόσφατα έχει εκδοθεί το Δεύτερο Πρόσθετο Πρωτόκολλο της Σύμβασης για το Έγκλημα στον Κυβερνοχώρο (Σύμβαση της Βουδαπέστης), το οποίο αφορά την ενίσχυση της συνεργασίας και την αποκάλυψη ηλεκτρονικών αποδεικτικών στοιχείων.

Α.2. Θεσμοί διεθνούς συνεργασίας της Σύμβασης της Βουδαπέστης

Α.2.1 Κατεπείγουσα διατήρηση αποθηκευμένων δεδομένων υπολογιστών

Στο άρθρο 29 της Σύμβασης καθιερώνεται ένας μηχανισμός ο οποίος καθιστά διαθέσιμα τα μέτρα που δύναται να λαμβάνονται σε εθνικό σε διασυνοριακό επίπεδο. Κάθε Συμβαλλόμενο μέρος μπορεί να ζητήσει από ένα άλλο ή να εξασφαλίσει την κατεπείγουσα διατήρηση δεδομένων που είναι αποθηκευμένα σε ένα σύστημα υπολογιστή, το οποίο βρίσκεται στην επικράτεια του άλλου. Το αιτούν Συμβαλλόμενο Μέρος υποβάλλει αίτηση αμοιβαίας συνδρομής με σκοπό την έρευνα ή την πρόσβαση, κατάσχεση, εξασφάλιση ή αποκάλυψη των δεδομένων. Το χρονικό διάστημα που δίνεται

[28] Ό.π., άρθρο 15 παρ.1. Τα συμβαλλόμενα μέρη δεν είναι υποχρεωμένα να προσχωρήσουν στη Σύμβαση 108 προκειμένου να είναι σε θέση να προσχωρήσουν στη Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο.

προκειμένου να γίνει η αίτηση από το αιτούν Συμβαλλόμενο Μέρος με σκοπό να γίνουν-επιτευχθούν τα ανωτέρω είναι τουλάχιστον εξήντα ημέρες. Η αίτηση διατήρησης που υποβάλλεται πρέπει να περιλαμβάνει την αρχή που ζητεί τη διατήρηση, το έγκλημα που αποτελεί το αντικείμενο της ποινικής έρευνας ή δίωξης και συνοπτική περιγραφή των συναφών πραγματικών περιστατικών, τα προς διατήρηση αποθηκευμένα δεδομένα υπολογιστή και τη 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.[29]

Η διατήρηση των δεδομένων υπολογιστή είναι ένα περιορισμένο, προσωρινό μέτρο, προορισμένο να εκτελείται ταχύτατα. Τα δεδομένα έχουν ευμετάβλητο χαρακτήρα τα οποία όπως έχει ξαναειπωθεί μπορούν να διαγραφούν εύκολα, να μεταβληθούν ή να μετακινηθούν. Τα παραπάνω αφενός καθιστούν αδύνατο τον εντοπισμό του δράστη ενός εγκλήματος και αφετέρου κάνουν πιο επιτακτική την ανάγκη λήψης ταχύτερων μέτρων προς τη διατήρηση των δεδομένων. Για το τελευταίο, τα Συμβαλλόμενα Μέρη συμφώνησαν ότι απαιτείται ένας μηχανισμός για να εξασφαλιστεί η διαθεσιμότητα αυτών των δεδομένων εν όψει της επικείμενης, περισσότερο χρονοβόρας και περίπλοκης διαδικασίας εκτέλεσης μιας «παραδοσιακής» αίτησης αμοιβαίας δικαστικής συνδρομής, η οποία μπορεί να απαιτήσει εβδομάδες ή μήνες για να εκτελεστεί.[30] Η εν λόγω διαδικασία αποκτά περισσότερο ενδιαφέρον καθώς πέρα του γεγονότος πως εξασφαλίζει ταχύτητα, αποδεικνύεται και προστατευτική για το Υποκείμενο των

[29]Σύμφωνα με παράγραφο 1 του άρθρου 29 της Σύμβασης της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο.
[30]Βλ.Explanatory Report to the Convention on Cybertime, σελ. 50

δεδομένων καθώς το μόνο που απαιτεί είναι η διατήρηση από κάποιον τρίτο που τα έχει ήδη στη κατοχή του.

Α.2.3 Κατεπείγουσα γνωστοποίηση διατηρηθέντων δεδομένων κίνησης

Σύμφωνα με το άρθρο 30 της Σύμβασης τα μέτρα δύναται να λαμβάνονται σε εθνικό επίπεδο, δυνάμει του άρθρου 17 της Σύμβασης. Ένα Συμβαλλόμενο Μέρος μπορεί να ζητά από το Συμβαλλόμενο Μέρος στο οποίο υπέβαλλε την αίτηση δεδομένα κίνησης. Κάτι τέτοιο είναι δυνατό να οδηγήσει στον εντοπισμό του δράστη ενός εγκλήματος όμως υπάρχει και μια περίπτωση αυτό να μην είναι εύκολα εφικτό. Η περίπτωση αυτή, η οποία συναντάται και στη πράξη είναι όταν η επικοινωνία λαμβάνει χώρα μέσω Διαδικτύου και λόγω του διεθνούς χαρακτήρα του, τα δεδομένα του 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, για τη 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 είναι διαθέσιμη ανεξαρτήτως της συμμετοχής ενός ή περισσοτέρων παρόχων υπηρεσιών στη διαβίβαση αυτών των επικοινωνιών, το Συμβαλλόμενο 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 διαβιβάστηκε η επικοινωνία αυτή.[31] Επιπλέον, η γνωστοποίηση των δεδομένων κίνησης μπορεί να απορριφθεί, εάν η αίτηση, αφορά πολιτικό

[31]Σύμφωνα με το άρθρο 29 της Σύμβασης της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο

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 συμφέροντα του.[32]

Α.2.4 Αμοιβαία συνδρομή σχετικά με την πρόσβαση σε αποθηκευμένα δεδομένα υπολογιστή

Κάθε συμβαλλόμενο Μέρος μπορεί να ζητήσει από ένα άλλο Συμβαλλόμενο Μέρος να ερευνήσει ή με παρόμοιο τρόπο να αποκτήσει πρόσβαση, να κατάσχει ή με παρόμοιο τρόπο να εξασφαλίσει ή να αποκαλύψει δεδομένα που είναι αποθηκευμένα σε ένα σύστημα υπολογιστή που βρίσκεται στην επικράτεια του Συμβαλλόμενου Μέρους, προς το οποίο απευθύνεται η αίτηση, περιλαμβανομένων των δεδομένων που έχουν διατηρηθεί κατ' εφαρμογή του άρθρου 29.[33] Ακόμα, 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.[34]

Το ζήτημα του κατά πόσο θα πρέπει να επιτρέπεται σε ένα Συμβαλλόμενο Μέρος να αποκτά πρόσβαση μονομερώς σε δεδομένα ηλεκτρονικού υπολογιστή τα οποία είναι αποθηκευμένα σε άλλο Συμβαλλόμενο Μέρος χωρίς να υποβάλει αίτημα αμοιβαίας συνδρομής προβλημάτισε τους συντάκτες της Σύμβασης. Μολαταύτα οι συντάκτες κατέληξαν να συμπεριλάβουν στο άρθρο 32 της Σύμβασης μόνο καταστάσεις

[32]Βλ. άρθρο 30 παρ.2 της Σύμβασης της Βουδαπέστης για το Έγκλημα στον Κυβερνοχώρο
[33]Σύμφωνα με άρθρο 31 της Σύμβασης της Βουδαπέστης για το Έγκλημα στον Κυβερνοχώρο
[34]Βλ. άρθρο 31 παρ. 3 σε συνδυασμό με παρ.2 και άρθρο 23 της Σύμβασης της Βουδαπέστης για το Έγκλημα στον Κυβερνοχώρο

κατά τις οποίες η μονομερή πρόσβαση είναι επιτρεπτή. Συγκεκριμένα και σύμφωνα με το άρθρο 32 κάθε Συμβαλλόμενο Μέρος χωρίς να έχει εξουσιοδοτηθεί από το άλλο Συμβαλλόμενο Μέρος μπορεί να έχει πρόσβαση σε αποθηκευμένα δεδομένα υπολογιστή που είναι διαθέσιμα στο κοινό(ανοιχτή πηγή) ασχέτως της γεωγραφικής θέσης των δεδομένων ή να αποκτήσει πρόσβαση ή να λάβει μέσω ενός συστήματος υπολογιστή στην επικράτεια του δεδομένα υπολογιστή που είναι αποθηκευμένα σε άλλο Συμβαλλόμενο Μέρος, εάν το Συμβαλλόμενο Μέρος λάβει τη νόμιμη και οικειοθελή συναίνεση του προσώπου που έχει νόμιμη εξουσία να γνωστοποιεί τα δεδομένου του υπολογιστή του στο Συμβαλλόμενο Μέρος. Ένα παράδειγμα αυτής της περίπτωσης είναι τα μηνύματα του ηλεκτρονικού ταχυδρομείου (e-mails) ενός ατόμου τα οποία μπορούν να αποθηκεύονται από έναν πάροχο υπηρεσιών σε άλλο Συμβαλλόμενο Μέρος ή ένα άτομο μπορεί να αποθηκεύει σκόπιμα δεδομένα σε άλλο Συμβαλλόμενο Μέρος.

Συμπερασματικά, οι πάροχοι υπηρεσιών εφόσον έχουν την νόμιμη εξουσία που αναφέρθηκε παραπάνω και αναφέρεται στο άρθρο 32 της Σύμβασης μπορούν είτε να αποκαλύψουν τα δεδομένα στις Αρχές επιβολής του Νόμου είτε να τους επιτρέψουν την πρόσβαση σε αυτά αποσκοπώντας, ως εκ τούτου, στην περαιτέρω ενίσχυση της συνεργασίας στον τομέα του κυβερνοεγκλήματος και της συλλογής ηλεκτρονικών αποδεικτικών στοιχείων για κάθε ποινικό αδίκημα στο πλαίσιο συγκεκριμένων ποινικών ερευνών ή διώξεων. Σύμφωνα με την Επιτροπή της Σύμβασης για το Κυβερνοέγκλημα, οι πάροχοι υπηρεσιών δε φαίνεται να έχουν την νόμιμη εξουσία, ώστε να υποβάλουν δεδομένα των χρηστών τους, καθώς αυτοί μόνο διατηρούν τα δεδομένα αυτά, τα οποία όμως δεν τους ανήκουν.[35] Αυτό το οποίο πρέπει να γίνει κατανοητό στη συγκεκριμένη περίπτωση είναι πως η συγκεκριμένη διάταξη βρίσκει εφαρμογή μόνο στις περιπτώσεις όπου τα

[35]Βλ.Cybertime 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)

δεδομένα υπολογιστή είναι αποθηκευμένα σε άλλο Συμβαλλόμενο Μέρος και σε καμία περίπτωση όταν αυτά είναι αποθηκευμένα σε τρίτο μη Συμβαλλόμενο Μέρος.

Α.2.5 Δικαστική συνδρομή για την συλλογή δεδομένων κίνησης σε πραγματικό χρόνο

Το γεγονός πως βασικά δεδομένα κίνησης ενδέχεται πολλές φορές να έχουν διαγραφεί αυτόματα από έναν πάροχο υπηρεσιών, πριν καν προλάβουν οι Αρχές να ζητήσουν τη διατήρηση τους, δυσκολεύει εκ των πραγμάτων τους ερευνητές να ανιχνεύσουν μια επικοινωνία στην πηγή της ακολουθώντας το ίχνος μέσω αρχείων ιστορικού προηγούμενων μεταδόσεων. Σύμφωνα με το άρθρο 33 της Σύμβασης τα Συμβαλλόμενα Μέρη θα παρέχουν αμοιβαία συνδρομή για τη συλλογή σε πραγματικό χρόνο δεδομένων κίνησης σχετικά με συγκεκριμένες επικοινωνίες στην επικράτεια τους που διαβιβάζονται μέσω ενός συστήματος υπολογιστή, τηρούμενων των διατάξεων της παραγράφου 2, η εν λόγω συνδρομή θα διέπεται από τους όρους και τις διαδικασίες που προβλέπονται από το εσωτερικό δίκαιο. Επιπλέον, βάση της παρ. 2 του άρθρου 33 κάθε Συμβαλλόμενο Μέρος θα παρέχει παρόμοια συνδρομή τουλάχιστον αναφορικά με αδικήματα για τα οποία επιτρέπεται, η συλλογή δεδομένων κίνησης σε πραγματικό χρόνο σε παρόμοιες υποθέσεις σύμφωνα με το εσωτερικό δίκαιο.

Συμπερασματικά, είναι πολύ σημαντικό για τους ερευνητές σε κάθε Συμβαλλόμενο Μέρος να έχουν τη δυνατότητα να λαμβάνουν δεδομένα κίνησης σε πραγματικό χρόνο, σχετικά με επικοινωνίες που διέρχονται από ένα σύστημα ηλεκτρονικών υπολογιστών σε άλλα κράτη.[36]

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

Α.2.6 Αμοιβαία συνδρομή σχετικά με την άρση απορρήτου δεδομένων περιεχομένου

Με βάση το άρθρο 34 της Σύμβασης της Βουδαπέστης τα Συμβαλλόμενα Μέρη μπορούν να παρέχουν αμοιβαία συνδρομή για την συλλογή ή καταγραφή σε πραγματικό χρόνο δεδομένων περιεχομένου σχετικά με συγκεκριμένες επικοινωνίες στην επικράτεια τους, που διαβιβάζονται μέσω ενός συστήματος υπολογιστή, στον βαθμό που επιτρέπεται από ισχύουσες συμβάσεις και το εσωτερικό τους δίκαιο. Σημειώνεται επίσης, πως εξαιτίας του υψηλού βαθμού παρεμβατικότητας στην άρση του περιεχομένου, ο βαθμός αμοιβαίας συνδρομής σχετικά με την άρση του απορρήτου δεδομένων περιεχομένου περιορίζεται και παρέχεται μόνο στο βαθμό που αυτό επιτρέπεται από τις ισχύουσες συνθήκες και νόμους των Συμβαλλόμενων Μερών.

Α.2.7 Δικαστική Συνδρομή

Όσον αφορά τη διασυνοριακή πρόσβαση σε δεδομένα για σκοπούς έρευνας, **βάσει της Οδηγίας 2013/40/ΕΕ,** ο ευρωπαίος νομοθέτης υιοθέτησε μια εντελώς διαφορετική προσέγγιση. Συγκεκριμένα, ισχυρή είναι η άποψη πως δεν υπάρχουν ειδικοί κανόνες σχετικά με τους τρόπους και τους όρους πρόσβασης σε δεδομένα σε άλλη χώρα ενώ παράλληλα η συνεργασία, ο συντονισμός και η προσέγγιση του ποινικού δικαίου φαίνεται να αποτελούν τις κύριες επιλογές της οδηγίας **2013/40/ΕΕ** σχετικά με τις επιθέσεις κατά των συστημάτων πληροφοριών όσον αφορά τις επιθέσεις με διασυνοριακή διάσταση.

Η σύμβαση εισάγει την υποχρέωση ενός κράτους μέλους να ενημερώνει την Επιτροπή, όταν αποφασίζει να εξετάσει το ζήτημα της δικαιοδοσίας του για αδίκημα που διαπράχθηκε εκτός του εδάφους του. Η ανταλλαγή πληροφοριών ρυθμίζεται στο άρθρο 13 και συνίσταται στην καθιέρωση και

χρήση λειτουργικών εθνικών σημείων επαφής και στην υποχρέωση θέσπισης διαδικασιών για την αντιμετώπιση επειγόντων αιτημάτων συνδρομής.

Η απόφαση πλαίσιο **2009/948/ΔΕΥ** επικεντρώνεται στην πρόληψη καταστάσεων κατά τις οποίες το ίδιο πρόσωπο μπορεί να υποβληθεί σε παράνομες εγκληματικές πράξεις σε διαφορετικά κράτη μέλη.[37] Στην εν λόγω απόφαση προτείνεται η υλοποίηση της διαδικασίας να γίνεται από ενα κράτος ή η αναφορά στην Eurojust. Με αυτόν τον τρόπο θα αποφευχθούν οι δυσμενείς συνέπειες που προκύπτουν από παράλληλες διαδικασίες. Σημαντικό είναι να τονιστεί πως ενώ η ανταλλαγή πληροφοριών μεταξύ αρμόδιων αρχών και η απάντηση σε αιτήσεις που υποβάλλονται από αρμόδιες αρχές άλλου κράτους μέλους θεωρούνται υποχρέωση των κρατών μελών δεν διατίθεται μια συνολική ρύθμιση για τη διασυνοριακή συνεργασία, δοθέντος ότι τα κράτη-μέλη που στηρίζονται τη Σύμβαση για την εγκληματικότητα στον κυβερνοχώρο απέφυγαν τη λεπτομερή ρύθμιση και επέλεξαν μια "εποικοδομητική ασάφεια" ώστε να μπορούν να αντιμετωπίσουν διαφορετικές καταστάσεις.

Σε αυτό το σημείο σημαντική εξίσου είναι και η τοποθέτηση της ΕΕ η οποία μεταξύ άλλων προωθεί τη συντονισμένη συνεργασία μεταξύ των κρατών-μελών, η οποία με το καιρό ενισχύεται και βελτιώνεται. Παρ' ολαυτά και ειδικά κυρίως λόγω των δυσχερειών των διαδικασιών αμοιβαίας δικαστικής συνδρομής, οι ερευνητές μερικές φορές προχωρούν σε δραστηριότητες έρευνας εξ αποστάσεως σε ξένο έδαφος χωρίς την επίσημη εξουσιοδότηση. Ένα επιπλέον μειονέκτημα των διαδικασιών της αμοιβαίας δικαστικής συνδρομής είναι πως υποβαθμίζουν τις απαιτήσεις για την απόκτηση και διαφύλαξη ηλεκτρονικών αποδεικτικών στοιχείων.

Τον Ιούνιο του 2013, πραγματοποιήθηκε δημόσια ακρόαση στο Στρασβούργο για να συζητηθούν τα πιθανά στοιχεία ενός πρόσθετου

[37]Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou , The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

πρωτοκόλλου και έγιναν οι ακόλουθες πέντε προτάσεις: **διασυνοριακή πρόσβαση με συγκατάθεση χωρίς περιορισμό στα αποθηκευμένα δεδομένα "σε άλλο μέρος"· διασυνοριακή πρόσβαση χωρίς συγκατάθεση, αλλά με έγκυρα διαπιστευτήρια · διασυνοριακή πρόσβαση χωρίς συγκατάθεση σε απαιτητικές ή άλλες περιστάσεις · επέκταση της έρευνας χωρίς τον περιορισμό «στην επικράτειά του» στο άρθρο 19.3 · και η εξουσία διάθεσης ως συνδετικού νομικού παράγοντα.** Οι βασικές επικρίσεις, πάνω σε αυτές τις προτάσεις αφορούσαν τις απαιτήσεις προστασίας της ιδιωτικής ζωής και της έννοιας της συγκατάθεσης ενός υποκειμένου δεδομένων αντί του υπεύθυνου επεξεργασίας δεδομένων. Οι πτυχές που σχετίζονται με την προστασία των δεδομένων είναι ακόμη πιο δύσκολες, δεδομένου ότι τα συμβαλλόμενα μέρη της Σύμβασης για την εγκληματικότητα στον κυβερνοχώρο εκτείνονται και πέρα από την επικράτεια του Συμβουλίου της Ευρώπης.[38]

Προβληματισμό επίσης, δημιούργησε και η νομιμότητα της έγκρισης πρόσβασης σε διασυνοριακό επίπεδο, η αμφισβητούμενη ερμηνεία των όρων όπως «καλή τη πίστει ή σε επιτακτικές περιστάσεις» και «η εξουσία διάθεσης δεδομένων» στο πλαίσιο της διασυνοριακής πρόσβασης.[39] Τα συμβατικά κείμενα που αφορούν σε ποινικές υποθέσεις και συνδέουν τα κράτη μέλη της Ευρωπαϊκής Ένωσης είναι τα κάτωθι: 1) Η Ευρωπαϊκή Σύμβαση περί Εκδόσεως Εγκληματιών της 13-12-1957, και το από 20-4-1959 συμπλήρωμά της, η Ευρωπαϊκή Σύμβαση περί Αμοιβαίας Δικαστικής Συνδρομής επί ποινικών υποθέσεων, καθώς και τα δύο πρόσθετα πρωτόκολλά της. 2) Τμήματα της Συνθήκης Schengen της 14 -6-1985. 3) Η Ευρωπαϊκή Σύμβαση της 29-5-2000 για την Αμοιβαία Δικαστική Συνδρομή σε Ποινικές Υποθέσεις (ΑΔΣΠΥ/ΕΕ) και το πρόσθετο πρωτόκολλό της, που όμως δεν την έχει κυρώσει η Ελλάδα. 4) Η Απόφαση-Πλαίσιο 2002/584/JI της 13-6-2002 για το

[38] https://ccdcoe.org/transborder-data-access-quo-vadis-council-europe.html
[39] https://www.coe.int/en/web/corruption, Council of Europe, Article: Economic Crime and Cooperation Division

Ευρωπαϊκό Ένταλμα Σύλληψης. 5) Η Απόφαση-πλαίσιο 2003/577/ΔΕΥ του Συμβουλίου της 22/7/ 2003 σχετικά με την εκτέλεση των αποφάσεων δέσμευσης περιουσιακών ή αποδεικτικών στοιχείων στην ΕΈ (ΕΑΔΠΑ). 6) Η Απόφαση-Πλαίσιο 2008/978/ JI για την Ευρωπαϊκή Εντολή για τη συλλογή αντικειμένων, εγγράφων και στοιχείων σε ποινικές υποθέσεις (ΕΕΣΑ). 7) Η Οδηγία 2010/64/EU για το δικαίωμα διερμηνείας και μετάφρασης σε ποινικές διαδικασίες. 8) Η Οδηγία 2012/13/EU για το δικαίωμα πληροφόρησης σε ποινικές διαδικασίες. 9) Η Οδηγία 2013/48/EU για το δικαίωμα πρόσβασης σε δικηγόρο και το δικαίωμα επικοινωνίας των στερημένων της ελευθερίας τους. 10) Τέλος, σημαντικό σταθμό πρόκειται να αποτελέσει η Οδηγία 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 3-4-2014, περί Ευρωπαϊκής Εντολής Έρευνας σε ποινικές υποθέσεις, η οποία πρόκειται να αρχίσει να ισχύει από την 22/5/2017.[40]

Οι αιτήσεις δικαστικής συνδρομής διαβιβάζονται από κάποιο δικαστή ή εισαγγελέα ενός κράτους μέλους (ΚΜ) σε δικαστή ή εισαγγελέα άλλου κράτους μέλους[41] και σύμφωνα με όσα ορίζονται και στον Κώδικα Ποινικής Δικονομίας. Το 2000, τα κράτη μέλη της Ευρωπαϊκής Ένωσης υπέγραψαν Σύμβαση για την αμοιβαία δικαστική συνδρομή επί ποινικών υποθέσεων προς συμπλήρωση και διευκόλυνση της εφαρμογής αυτών των συμβάσεων. **Η σύμβαση του 2000 ενισχύθηκε το 2001 από Πρωτόκολλο**, το οποίο επικεντρώνεται στην αμοιβαία νομική συνδρομή για πληροφορίες σχετικά με τραπεζικούς λογαριασμούς ή τραπεζικές συναλλαγές.

Με βάση τη σύμβαση του 2000, παρέχεται αμοιβαία συνδρομή για*: 1. ποινικές διαδικασίες, 2. διαδικασίες που κινούνται από διοικητικές αρχές όταν η απόφαση μπορεί να δικαιολογήσει προσφυγή ενώπιον ποινικού δικαστηρίου, 3. διαδικασίες που αφορούν αδικήματα ή παραβάσεις τα οποία συνεπάγονται*

[40]Αναλυτικότερα περί Ευρωπαϊκής Εντολής Έρευνας παρακάτω, Διονύσιος Δ. Σπινέλλης, Η δικαστική συνεργασία σε ποινικές υποθέσεις στην Ευρώπη και ειδικότερα η ευρωπαϊκή εντολή έρευνας, Ιανουάριος 2016

[41]https://e-justice.europa.eu/content_request_for_judicial_assistance-91-el.do, Διαδικτυακή πύλη της Ευρωπαϊκής Ένωσης, Δικαστήριο της Ευρωπαϊκής Ένωσης

ευθύνη νομικού προσώπου (εταιρείας ή φορέα, όχι «προσώπου») στο αιτούν κράτος μέλος. Η συνεργασία δύναται να πραγματοποιείται είτε μέσω «αυθόρμητης» ανταλλαγής πληροφοριών είτε κατόπιν αιτήματος κράτους μέλους. Ο γενικός κανόνας είναι ότι οι αιτήσεις θα πρέπει να διαβιβάζονται απευθείας μεταξύ των δικαστικών αρχών που είναι κατά τόπον αρμόδιες για την υποβολή και τη διεκπεραίωσή τους και να επιστρέφονται δια της αυτής οδού. Το κράτος μέλος προς το οποίο απευθύνεται η αίτηση οφείλει να συμμορφώνεται προς τις διατυπώσεις και τις διαδικασίες που υπέδειξε ρητά το αιτούν κράτος μέλος. Για τη καλύτερη δυνατή συνεργασία μεταξύ των αρχών επιβολής του νόμου, των δικαστικών αρχών και των λοιπών αρχών, η Σύμβαση του 2000 προβλέπει την χρήση τεχνολογικών εργαλείων όπως η εικονοδιάσκεψη, η τηλεφωνική συνδιάλεξη και η παρακολούθηση των τηλεπικοινωνιών.

Έπειτα, με το Πρωτόκολλο του 2001 τα κράτη μέλη συνεργάζονται όλο και περισσότερο χρησιμοποιώντας μέσα τα οποία εφαρμόζουν την αρχή της αμοιβαίας αναγνώρισης κατά την οποία οι δικαστικές αρχές (δικαστήρια, δικαστές, εισαγγελείς) ενός κράτους μέλους αναγνωρίζουν τις αποφάσεις των δικαστικών αρχών άλλου κράτους μέλους ως ισοδύναμες εκείνων που λαμβάνονται στο κράτος τους.

Β. ΤΟ ΔΙΚΤΥΟ 24/7

Κάθε Συμβαλλόμενο Μέρος ορίζει ένα σημείο επαφής, το οποίο θα είναι διαθέσιμο σε εικοσιτετράωρη βάση, επτά μέρες 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 τη συλλογή των αποδεικτικών στοιχείων σε

ηλεκτρονική μορφή για ένα ποινικό αδίκημα.[42] 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 συμβούλων, τη διατήρηση των δεδομένων, σύμφωνα με τα άρθρα 29 και 30, τη συλλογή αποδεικτικών στοιχείων, τη παροχή νομικής ενημέρωσης και τον εντοπισμό των υπόπτων.

Ακόμα, το σημείο επαφής κάθε Συμβαλλόμενου Μέρους είναι να επικοινωνεί σε κατεπείγουσα βάση με το σημείο επαφής ενός άλλου Συμβαλλόμενου Μέρους. Εάν το σημείο επαφής που ορίστηκε από το 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 6 του Ν.4411/2016[43], η Ελληνική Δημοκρατία ορίζει ως σημείο επαφής για την εκπλήρωση των σκοπών του παραπάνω άρθρου της Σύμβασης «Δίκτυο 24/7» τη Διεύθυνση Δίωξης του Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας υπό την εποπτεία Εισαγγελέα Εφετών.

Γ. ΟΔΗΓΙΑ 2014/41/ΕΕ

Οι διατάξεις της **Οδηγίας 2014/41/ΕΕ,** οι οποίες σημειωτέον ενσωματώθηκαν στο εθνικό μας δίκαιο με τον Ν.4489/2017 αποτελούν μια

[42]Σύμφωνα με άρθρο 35 της Σύμβασης

[43]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 Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης –πλαισίου 2005/22/ΔΕΥ του Συμβουλίου, ρυθμίσεις Σωφρονιστικής και εγκληματικής πολιτικής και άλλες διατάξεις.

πρόοδο στον τομέα της ασφάλειας και της απονομής δικαιοσύνης στην ΕΕ η οποία διευκόλυνε τη δικαστική συνεργασία σχετικά με τα διασυνοριακά εγκλήματα ενώ παράλληλα αντικατέστησε τα διάφορα προηγούμενα νομικά κείμενα που ρύθμιζαν θέματα δικαστικής συνδρομής με ένα ενιαίο κείμενο. Επιπλέον, κάποιες μόνο εξαιρέσεις προβλέπονται από ειδικές ρυθμίσεις ενώ συνάμα στο κανονιστικό πλαίσιο της Οδηγίας ενισχύεται η θέση του κράτους που δίνει την εντολή. Ταυτόχρονα αναγνωρίζει και στο κράτος εκτέλεσης σημαντικούς λόγους να αρνηθεί την αιτούμενη δικαστική συνδρομή ανάγοντας έτσι το συμπέρασμα πως εν μέρει τουλάχιστον, διατηρεί και αυτή η οδηγία την απαίτηση του διπλού αξιοποίνου. Αναμφίβολα, το κράτος εντολής έχει τον κύριο λόγο για τον καθορισμό του επιτρεπτού πλαισίου εκτέλεσης των ερευνών ενώ επίσης η ρύθμιση αυτή των σχετικών ζητημάτων δικαιολογείται από το γεγονός ότι το αποτέλεσμα των ανακριτικών ενεργειών θα χρησιμοποιηθεί σε ποινική διαδικασία του κράτους αυτού (του κράτους εντολής).

Τα κυριότερα ζητήματα που ενδιαφέρουν κατά τη μεταφορά των διατάξεων της Οδηγίας στο Ελληνικό Δίκαιο αφορούν την τήρηση ενός υψηλού βαθμού δικονομικών εγγυήσεων. Σχετικά με την διαδικασία της έκδοσης και εκτέλεσης της ΕΕΕ[44] γίνεται προσπάθεια να επιταχυνθεί με δυο τουλάχιστον τρόπους:

Πρώτον, προβλέπεται ότι η εκτέλεση της ΕΕΕ θα πρέπει να γίνεται "το ταχύτερο", και αφετέρου προβλέπονται ειδικές προθεσμίες δηλαδή 30 ημέρες για ν' αποφασίσει το κράτος εκτέλεσης για την εκτέλεση της ΕΕΕ (ά. 12 παρ. 3) και 90 ημέρες για να πραγματοποιηθεί η εκτέλεση του ανακριτικού μέτρου (ά. 12 παρ. 4). Στην πράξη, για διάφορους λόγους, οι προθεσμίες συχνά δεν τηρούνται. Η πρόβλεψη αυτή, όμως, στόχο έχει να ασκήσει σε κάποιο βαθμό

[44]Παρακάτω δίνονται περισσότερα στοιχεία και λεπτομέρειες για την Ευρωπαϊκή Εντολή Έρευνας(ΕΕΕ).

πίεση για την επιτάχυνση των διαδικασιών.[45] Η ανταλλαγή δεδομένων δημιουργεί προβλήματα σχετικά με την ποινική διαδικασία, γι' αυτό σχεδιάστηκε το «έργο της απόδειξης»-"the evidence project". Η ανταλλαγή είναι αδήριτη ανάγκη να είναι αμεσότερη ιδίως για τις αντιτρομοκρατικές επιχειρήσεις με σκοπό την αντιμετώπιση παγκόσμιων εγκλημάτων γι' αυτό λοιπόν η Ευρωπαϊκή Ένωση πρέπει να αναπτύξει ένα καλύτερο μέσο προς αυτή τη κατεύθυνση. Ταυτόχρονα, μια ασφαλής και αξιόπιστη ανταλλαγή πληροφοριών και ηλεκτρονικών αποδεικτικών στοιχείων σχετικά με εγκλήματα αποτελεί σημαντικό στοιχείο για την προώθηση της δικαστικής συνεργασίας σε ποινικές υποθέσεις καθώς και για την αποτελεσματική και συνεπή εφαρμογή της αμοιβαίας δικαστικής συνδρομής της Ευρωπαϊκής Ένωσης και των διαδικασιών ευρωπαϊκής διερεύνησης.[46] Η πρόκληση είναι να διευκολυνθεί η ανταλλαγή ηλεκτρονικών αποδεικτικών στοιχείων στο πλαίσιο της Ευρωπαϊκής Ένωσης, καθιστώντας δυνατή την επίτευξη βελτιωμένης διεθνούς συνεργασίας στον εγκληματικό τομέα, με την ενσωμάτωση ειδικού πλαισίου διαδικασιών δικαστικής συνδρομής που θα επιτρέπουν καλύτερη συνεργασία και αμεσότητα μεταξύ των εισαγγελέων και των υπηρεσιών επιβολής του νόμου των κρατών-μελών. Για την ενίσχυση της δικαστικής συνεργασίας στον ποινικό τομέα είναι σημαντικό να εξεταστούν οι υφιστάμενες διαδικασίες δικαστικής συνδρομής, όπως προαναφέρθηκαν και τα νέα σύνορα της ευρωπαϊκής εντολής έρευνας. Το γεγονός παρολαυτά πως δεν υπάρχουν καθολικά μέσα που να αφορούν και να συμπεριλαμβάνουν μια άμεση συνεργασία επηρεάζουν αρνητικά τις δυνατότητες ταχείας και αποτελεσματικής μεταφοράς ηλεκτρονικών αποδεικτικών στοιχείων.

Προς αυτή τη κατεύθυνση και για τον σκοπό αυτό, οι Υπουργοί του Συμβουλίου Δικαιοσύνης και Εσωτερικών Υποθέσεων τον Ιούνιο του 2016

[45]Διονύσιος Δ. Σπινέλλης, Η δικαστική συνεργασία σε ποινικές υποθέσεις στην Ευρώπη και ειδικότερα η ευρωπαϊκή εντολή έρευνας, Ιανουάριος 2016

[46]A proposed electronic evidence exchange across the European Union By Maria Angela Biasiotti

πρότειναν να γίνει μεταρρύθμιση σχετικά με τις διαδικασίες αυτές προκειμένου να υπάρξει άμεση ανταλλαγή ηλεκτρονικών αποδεικτικών στοιχείων. Η προσέγγιση μιας τέτοιας μεταρρυθμιστικής προσπάθειας θα μπορούσε να είναι είτε αποκεντρωμένη είτε κεντρική. Συγκεκριμένα, θα μπορούσε η κεντρική πύλη της ΕΕ να λειτουργεί ως κέντρο επεξεργασίας αιτήσεων αμοιβαίας δικαστικής συνδρομής με μία κεντρική εγκατάσταση αποθήκευσης ψηφιακών αποδεικτικών στοιχείων ή θα μπορούσε να υιοθετηθεί μια εφαρμογή αναφοράς για τις αιτήσεις, η οποία θα εγκαθίσταται χωριστά στα κράτη-μέλη, παρέχοντας αναφορά για τη μονάδα αποθήκευσης.[47] Όσον αφορά τη συνεργασία μεταξύ των αρχών επιβολής του νόμου και των παρόχων, η Επιτροπή περιέγραψε τις κυριότερες ανησυχίες σχετικά με τη διαφάνεια της διαδικασίας, την αξιοπιστία των ενδιαφερομένων, τον εντοπισμό και την επαφή των αρμόδιων παρόχων υπηρεσιών, τη γνησιότητα και τη νομιμότητα ενός αιτήματος από μια αρχή, την άνιση μεταχείριση των αρχών σε όλα τα κράτη-μέλη και το παραδεκτό των αποδεικτικών στοιχείων σε μια ακροαματική διαδικασία. Μάλιστα η Επιτροπή έδωσε ιδιαίτερη έμφαση στο ζήτημα της πολυπλοκότητας που δημιουργείται από τις διαφορετικές κι ενίοτε αντιφατικές προσεγγίσεις των κρατών-μελών στο πεδίο των ερευνών.[48]

Δ. ΔΙΑΒΙΒΑΣΗ ΑΝΑΓΚΑΙΑ ΣΤΟ ΠΛΑΙΣΙΟ ΕΚΤΕΛΕΣΗΣ ΣΥΜΒΑΣΗΣ

Με την τροποποίηση της επιτρεπόμενης διασυνοριακής διαβίβασης για λόγους εκτέλεσης σύμβασης, ο **Ν. 3471/2006** αφαίρεσε από το άρθρο 9παρ.2 την προϋπόθεση της φυσικής ή νομικής αδυναμίας παροχής συγκατάθεσης

[47]A proposed electronic evidence exchange across the European Union By Maria Angela Biasiotti

[48]Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, 2017

του υποκειμένου των δεδομένων.[49] Αποτέλεσμα της τροποποίησης είναι η καλύτερη εναρμόνιση προς το άρθρο 26παρ.1 (β) και (γ) της Οδηγίας, κατά το οποίο επιτρέπεται κατ' εξαίρεση διαβίβαση σε τρίτη χώρα όταν:

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

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

Η Ομάδα Εργασίας, στο έγγραφο WP12 για την προστασία προσωπικών δεδομένων του άρθρου 29 της Οδηγίας, ανέφερε ότι αν και το πεδίο εφαρμογής των παρεκκλίσεων που αφορούν την εκτέλεση της σύμβασης φαίνεται αρκετά ευρύ, η εφαρμογή τους στην πράξη είναι μάλλον περιορισμένη από την «αναγκαιότητα».[50] Με το έγγραφο WP114 η Ομάδα Εργασίας τονίζει πως ανεξάρτητα από τη γενικότερη ερμηνεία του άρθρου 26 παρ.1, το κριτήριο της αναγκαιότητας μπορεί να περιορίσει τον αριθμό των περιπτώσεων στις οποίες βρίσκουν εφαρμογή οι εξαιρέσεις του άρθρου 26 παρ.1 της Οδηγίας.[51]

Ε. ΕΥΡΩΠΑΪΚΗ ΕΝΤΟΛΗ ΈΡΕΥΝΑΣ

[49]Βλ. Παναγιώτης Δ. Αρμαμέντος και Βασίλης Α.Σωτηρόπουλος, «Προσωπικά δεδομένα, Ερμηνεία κατ' άρθρο, Οι τροποποιήσεις του Ν.2472/1997 απ' τους Ν.3471/2006 και 3625/2007», Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη

[50]Σχέδιο εγγράφου εργασίας «Διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες: Εφαρμογή των άρθρων 25 και 26 της οδηγίας της ΕΕ για την προστασία των δεδομένων», ΓΔ XV D/5025/98, διαθέσιμο στην ιστοθέση http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_el.pdf.

[51]Οι εξαιρέσεις αναφέρονται στην έννοια της «αναγκαιότητας», δηλ. στο άρθρο 26 παρ.1 στοιχεία (β) έως (ε)

i) Περίληψη

Έπειτα από πολλές συζητήσεις και διαβουλεύσεις θεσπίστηκε με την Οδηγία 2014/41/ΕΕ η «ευρωπαϊκή εντολή έρευνας» (ΕΕΕ), ως μέσο συνεργασίας μεταξύ των κρατών μελών της ΕΕ σε ποινικές υποθέσεις (στο εξής «Οδηγία για την ΕΕ). Η παρούσα υιοθετήθηκε στις 3 Απριλίου του 2014 και στις 21 Σεπτεμβρίου 2017 ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν.4489/2017. Με αυτή αντικαταστάθηκε σε μεγάλο βαθμό το προϊσχύσαν νομικό πλαίσιο για τη συγκέντρωση και διαβίβαση αποδεικτικών μέσων για την ποινική δίκη –ιδίως μέσω της «μικρής δικαστικής συνδρομής»–, επειδή ήταν υπερβολικά πολύπλοκο και περιορισμένα αποτελεσματικό. Η ΕΕΕ σηματοδοτεί το πέρασμα σε μια αναπτυγμένη ενωσιακή ωριμότητα δικαστικής συνεργασίας μεταξύ των κρατών μελών της ΕΕ52.

Η ΕΕΕ βασίζεται στην αρχή της αμοιβαίας αναγνώρισης των δικαστικών αποφάσεων και διαταγών (άρθρ. 82§1 ΣΛΕΕ) και εκδίδεται από δικαστική αρχή του «κράτους έκδοσης» με σκοπό ιδίως την εκτέλεση ενός ή περισσοτέρων ερευνητικών μέτρων στο «κράτος εκτέλεσης». Η Οδηγία για την ΕΕΕ αποσκοπεί στην αντικατάσταση του «υπερβολικά κατακερματισμένου» πλαισίου για την συγκέντρωση αποδεικτικών στοιχείων από ένα σύστημα που βασίζεται μεν στην αρχή της αμοιβαίας αναγνώρισης, λαμβάνει δε υπόψιν και την ευελιξία του παραδοσιακού μοντέλου αμοιβαίας δικαστικής συνδρομής με άξονα την απλούστευση και επιτάχυνση της συλλογής και ανταλλαγής αποδείξεων εντός της ΕΕ[53]. Η ΕΕΕ ανοίγει κατά συνέπεια νέους ορίζοντες στον τομέα της μικρής δικαστικής συνδρομής και ενισχύει τη συνεργασία των αρχών των καρτών μελών προσφέροντας αρκετές δυνατότητες αλληλεπίδρασης. Η κατάργηση των συνοριακών ελέγχων εντός της ΕΕ έχει διευκολύνει σημαντικά την ελεύθερη

[52]Βλ. Δασκαλόπουλου Στ., Η Ευρωπαϊκή Εντολή Έρευνας (Ε.Ε.Ε.): Ο νέος θεσμός Δικαστικής Συνεργασίας επί ποινικών υποθέσεων εντός της Ευρωπαϊκής Ένωσης, ΠοινΧρ 2018, σελ. 173.
[53]Βλ. Προοίμιο της Οδηγίας για την ΕΕΕ, αρ. 5-6

κυκλοφορία των πολιτών της Ένωσης, έχει, όμως, διευκολύνει και τις διασυνοριακές δραστηριότητες των εγκληματιών.[54]

Η Οδηγία για την ΕΕΕ αποτελεί το πρώτο νομοθετικό μέτρο που υιοθετήθηκε μετά τη θέση σε ισχύ της Συνθήκης της Λισαβόνας, η οποία κατήργησε το νομικό εργαλείο της απόφασης-πλαίσιο και καθιέρωσε την αρχή της αμοιβαίας αναγνώρισης ως θεμέλιο της δικαστικής συνεργασίας στις ποινικές υποθέσεις.

ii) Ορισμός

Ως Ευρωπαϊκή Εντολή Έρευνας(ΕΕΕ) ορίζεται η δικαστική απόφαση την οποία εκδίδει ή επικυρώνει δικαστική αρχή κράτους έκδοσης με σκοπό την εκτέλεση ενός ή περισσότερων συγκεκριμένων ερευνητικών μέτρων σε άλλο κράτος μέλος ως κράτος εκτέλεσης για τη λήψη αποδεικτικών στοιχείων δυνάμει των διατάξεων του παρόντος Νόμου και της Οδηγίας 2014/41/ΕΕ, ή/και τη λήψη αποδεικτικών στοιχείων ευρισκομένων ήδη στην κατοχή των αρμόδιων αρχών του κράτους εκτέλεσης.[55] Την έκδοση ΕΕΕ δικαιούται να αιτηθεί ο ύποπτος ή ο κατηγορούμενος, ή ο δικηγόρος εξ ονόματός του, στο πλαίσιο των δικαιωμάτων υπεράσπισης που προβλέπει το δίκαιο και η ποινική δικονομία της Δημοκρατίας, ο Γενικός Εισαγγελέας της Δημοκρατίας, ο Αρχηγός Αστυνομίας, ο Διευθυντής του Τμήματος Τελωνείων, ο Έφορος Φορολογίας, ο ποινικός ανακριτής, εξουσιοδοτημένος δυνάμει των διατάξεων του εδαφίου (2) του άρθρου 4 του περί Ποινικής Δικονομίας Νόμου.[56]

---

[54]Επίσημος Ιστότοπος της Ευρωπαϊκής Ένωσης https://ejustice.europa.eu/92/EL/european_investigation_order_mutual_legal_assistance_and_joint_investigation_teams

[55]Άρθρο 1 παρ.1 Ο περί της Ευρωπαϊκής Εντολής Έρευνας σε Ποινικές Υποθέσεις Νόμος του 2017 (181(Ι)/2017)

[56]Άρθρο 1 παρ.3 ό.π

Η οδηγία για την ευρωπαϊκή εντολή έρευνας σε ποινικές υποθέσεις εκδόθηκε στις 3 Απριλίου 2014, τα δε κράτη μέλη της ΕΕ όφειλαν να τη μεταφέρουν στο εθνικό τους δίκαιο έως τις 22 Μαΐου 2017. Η Δανία και η Ιρλανδία δεν δεσμεύονται από την εν λόγω πράξη.

Η ευρωπαϊκή εντολή έρευνας βασίζεται στην αμοιβαία αναγνώριση, γεγονός που σημαίνει ότι η αρχή εκτέλεσης υποχρεούται να αναγνωρίσει το αίτημα του άλλου κράτους και να μεριμνήσει για την εκτέλεσή του. Η ευρωπαϊκή εντολή έρευνας εκτελείται κατά τον ίδιο τρόπο και με την ίδια διαδικασία ως εάν το οικείο ερευνητικό μέτρο είχε διαταχθεί από αρχή του κράτους εκτέλεσης. Ευρωπαϊκή εντολή έρευνας μπορεί επίσης να εκδοθεί για τη συγκέντρωση αποδεικτικών στοιχείων που υπάρχουν ήδη.

Η οδηγία δημιουργεί ένα ενιαίο και ολοκληρωμένο πλαίσιο για τη συγκέντρωση αποδεικτικών στοιχείων. Στα σχετικά ερευνητικά μέτρα είναι δυνατόν να περιλαμβάνονται, για παράδειγμα, η εξέταση μαρτύρων, παρακολουθήσεις τηλεφωνικών συνδιαλέξεων, μυστικές έρευνες και έρευνες για τη συγκέντρωση στοιχείων σχετικά με τραπεζικές συναλλαγές.

Οι αρχές έκδοσης μπορούν να καταφύγουν στη χρήση ευρωπαϊκής εντολής έρευνας μόνο αν το σχετικό ερευνητικό μέτρο είναι:

- απαραίτητο,
- αναλογικό και
- επιτρεπτό σε παρόμοιες εγχώριες υποθέσεις.

Η ευρωπαϊκή εντολή έρευνας εκδίδεται στη βάση τυποποιημένου εντύπου και μεταφράζεται στην επίσημη γλώσσα του κράτους μέλους εκτέλεσης ή σε οποιαδήποτε άλλη γλώσσα την οποία έχει υποδείξει το κράτος μέλος εκτέλεσης.

Σύμφωνα με τη νέα οδηγία, τα ερευνητικά μέτρα πρέπει να εκτελούνται από το κράτος μέλος εκτέλεσης με την ταχύτητα και την προτεραιότητα που θα δινόταν για παρόμοια εγχώρια υπόθεση.

Η οδηγία τάσσει συναφώς προθεσμίες (ανώτατο όριο 30 ημερών για τη λήψη της απόφασης για την αναγνώριση και εκτέλεση της αίτησης, και 90 ημερών από τη λήψη της προαναφερθείσας απόφασης για την ουσιαστική εκτέλεση της αίτησης).[57]

iii) Αρμόδιες Αρχές Έκδοσης και Εκτέλεσης

Στο άρθρο 7 παρ. 2 ορίζονται οι προϋποθέσεις υπό τις οποίες μπορεί να εκδοθεί ΕΕΕ από την αρχή έκδοσης. Προϋπόθεση για την έκδοση ΕΕΕ είναι η τήρηση της αρχής της αναλογικότητας. Ειδικότερα, πρέπει το αιτούμενο ερευνητικό μέτρο –όχι το αποδεικτικό αποτέλεσμα καθαυτό- να είναι, πρώτον, αναγκαίο, δηλαδή το μόνο πρόσφορο για την επίτευξη του επιδιωκόμενου σκοπού ή το λιγότερο επαχθές, και δεύτερον, εν στενή εννοία αναλογικό με τους σκοπούς της διαδικασίας. Επομένως, η αρμόδια αρχή έκδοσης πρέπει πριν από την έκδοση της ΕΕΕ να προβαίνει σε έλεγχο αναλογικότητας του αιτούμενου μέτρου στην συγκεκριμένη περίπτωση. Η στάθμιση θα γίνεται κατά κύριο λόγο μεταξύ των σκοπών της διαδικασίας και της προστασίας των δικαιωμάτων του ερευνώμενου προσώπου. Στο πλαίσιο αυτό θα λαμβάνεται υπόψη, ιδίως, η βαρύτητα του εγκλήματος, η αποδεικτική ανάγκη για τη δίωξη του εγκλήματος, ο βαθμός προσβολής των εννόμων συμφερόντων και δικαιωμάτων του ερευνώμενου προσώπου, το ύψος των απαιτούμενων πόρων για την εκτέλεση του αιτούμενου μέτρου, η ύπαρξη άλλων λιγότερο επαχθών μέτρων κ.α. Περαιτέρω προϋπόθεση για

[57] https://ejustice.europa.eu/92/EL/european_investigation_order_mutual_legal_assistance_and_joint_investigation_teams, Ευρωπαϊκή Εντολή Έρευνας, Αμοιβαία Δικαστική Συνδρομή και Κοινές Ομάδες Έρευνας

την έκδοση ΕΕΕ είναι η διαθεσιμότητα του αιτούμενου ερευνητικού μέτρου κατά το εσωτερικό δίκαιο. Εξετάζεται δηλαδή υποθετικά αν θα ήταν δυνατή κατά το ελληνικό δίκαιο η διενέργεια του μέτρου αυτού σε αντίστοιχη εσωτερική υπόθεση υπό τις συγκεκριμένες περιστάσεις και προϋποθέσεις. Ωστόσο, η έλλειψη εναρμόνισης του περιεχομένου των εννοιών «αναλογικότητα», «αναγκαιότητα» και «διαθεσιμότητα» σε επίπεδο ΕΕ, καθιστά δύσκολο τον ουσιαστικό έλεγχο συνδρομής τους.

Σκοπός της καθιέρωσης ελέγχου αναλογικότητας και διαθεσιμότητας του ερευνητικού μέτρου είναι η αποτροπή καταστρατήγησης του εσωτερικού δικαίου με την διενέργεια ανακριτικών πράξεων, που δεν επιτρέπονται κατά το εσωτερικό δίκαιο του κράτους έκδοσης της ΕΕΕ, σε κράτος-μέλος όπου αυτές επιτρέπονται, και κατ' επέκταση η αποτροπή του forum-shopping[58].

Στο άρθρο 11 παρ. 5 προβλέπεται η δυνατότητα συνδρομής των αρμόδιων αρχών έκδοσης της ΕΕΕ κατά την εκτέλεση των ερευνητικών μέτρων στο κράτος-εκτέλεσης. Η συνδρομή θα γίνει προς υποστήριξη των αρμόδιων ελληνικών αρχών, υπό την προϋπόθεση ότι: α) έχει υποβληθεί αντίστοιχο αίτημα από τις αρχές του κράτους έκδοσης, β) οι αρχές του κράτους έκδοσης θα μπορούσαν να συνδράμουν στην εκτέλεση των ερευνητικών μέτρων που αναφέρονται στην ΕΕΕ και σε παρόμοια εσωτερική υπόθεση, και γ) η εν λόγω συνδρομή δεν αντιτίθεται στις θεμελιώδεις αρχές του ελληνικού δικαίου ούτε βλάπτει τα ουσιώδη συμφέροντα εθνικής ασφαλείας. Υποστηρίζεται ότι ακόμα κι αν πληρούνται οι παραπάνω προϋποθέσεις, οι αρχές εκτέλεσης μπορεί να αρνηθούν το αίτημα των αρχών έκδοσης. Ορθότερο είναι να γίνει δεκτό ότι οι αρχές εκτέλεσης μπορούν να αρνηθούν το αίτημα αυτό μόνο αν δεν πληρούται η ως άνω υπό γ) αρνητική προϋπόθεση. Οι αρχές του κράτους έκδοσης που παρίστανται κατά την εκτέλεση της ΕΕΕ στην Ελλάδα υπόκεινται στο ελληνικό δίκαιο κατά την εκτέλεση της ΕΕΕ και δεν διαθέτουν κατ' αρχήν εξουσία εκτέλεσης ερευνητικών μέτρων στο ελληνικό έδαφος. Ο

[58] https://en.wikipedia.org/wiki/Forum_shopping, Ερμηνεία Forum Shopping

περιορισμός της δράσης των αρχών έκδοσης κατά την παρουσία τους στο ελληνικό έδαφος αποσκοπεί όχι μόνο στη διασφάλιση της εθνικής κυριαρχίας του κράτους-εκτέλεσης, αλλά και στην αποτροπή της πιθανότητας η συλλογή των αποδείξεων να κριθεί ως μη παραδεκτή από τα δικαστήρια του κράτους έκδοσης. Αρνητικά αξιολογείται η απουσία πρόβλεψης σχετικά με την δυνατότητα παράστασης δικηγόρου των υπό διερεύνηση προσώπων, καθώς υποβαθμίζει το ρόλο και τη σημασία της υπεράσπισης του υπόπτου ή του κατηγορουμένου σε διασυνοριακές υποθέσεις.

Πέραν όμως από την παραπάνω δυνατότητα, καθιερώνεται ευρύτατη υποχρέωση συνεργασίας και μάλιστα σε προληπτικό επίπεδο, προκειμένου να διασφαλιστεί η αποτελεσματικότερη δυνατή δικαστική συνδρομή. Στο πλαίσιο αυτό προβλέπεται: α) η δυνατότητα διαβούλευσης μεταξύ των αρμόδιων αρχών σχετικά με την πλήρωση των προϋποθέσεων έκδοσης ή εκτέλεσης της ΕΕΕ, β) η δυνατότητα της αρχής εκτέλεσης να ζητήσει περισσότερες πληροφορίες από την αρχή έκδοσης, γ) η υποχρέωση ενημέρωσης της αρχής έκδοσης από την αρχή εκτέλεσης για οποιοδήποτε ζήτημα αφορά την λήψη της ΕΕΕ, την πορεία εκτέλεσης, αποφάσεις σχετικά με την εκτέλεση, ιδίως δε αν η αρχή εκτέλεσης δεν μπορεί να εκτελέσει το αιτούμενο ερευνητικό μέτρο, ή θεωρεί ότι υπάρχει λόγος άρνησης εκτέλεσης, ή καθυστερεί να τηρήσει τις οριζόμενες από το νόμο προθεσμίες κ.α.

υ) Περιεχόμενο ΕΕΕ

Η ΕΕΕ ως δικαστική απόφαση, διαβιβάζεται από το κράτος έκδοσής της στο κράτος εκτέλεσης. Για τη διευκόλυνση και να επιτάχυνση της διαδικασίας δικαστικής συνεργασίας, το άρθρο 5 της Οδηγίας αλλά και το Παράρτημα Α αυτής, στο οποίο το άρθρο 5 ρητά παραπέμπει, προβλέπουν τη συγκεκριμένη μορφή και το ελάχιστο περιεχόμενο μίας ΕΕΕ. Ειδικότερα, το άρθρο 5 της Οδηγίας απαριθμεί τις εξής πληροφορίες ως τις ελάχιστες που

πρέπει να περιέχει κάθε ΕΕΕ: «*α) στοιχεία σχετικά με την αρχή έκδοσης και, κατά περίπτωση, την αρχή επικύρωσης, β) το αντικείμενο και τους λόγους έκδοσης της ΕΕΕ, γ) τις απαραίτητες διαθέσιμες πληροφορίες για το ή τα ενδιαφερόμενα πρόσωπα, δ) περιγραφή της αξιόποινης πράξης που αποτελεί αντικείμενο έρευνας ή διαδικασίας και των ισχυουσών διατάξεων του ποινικού δικαίου του κράτους έκδοσης, ε) περιγραφή του ή των ερευνητικών μέτρων που ζητούνται και των αποδεικτικών στοιχείων που πρέπει να συγκεντρωθούν*». Η ΕΕΕ λοιπόν συμπληρώνεται από το προτυπωμένο έντυπο του Παραρτήματος Α της Οδηγίας 2014/14/ΕΕ και υπογράφεται από την Αρχή Έκδοσης, η οποία πιστοποιεί την ακρίβεια του περιεχομένου της. Η Αρχή Έκδοσης μπορεί να διαβιβάζει τις ΕΕΕ μέσω συστήματος τηλεπικοινωνιών του Ευρωπαϊκού Δικαστικού Συμβουλίου (ΕΕΔ) που δημιουργήθηκε με την κοινή δράση 98/428/ΔΕΥ του Συμβουλίου[59].

Η επιλογή της ποσότητας των λεπτομερειών εναπόκειται φυσικά στον εθνικό νομοθέτη κάθε κράτους μέλους που θα καθορίσει πιο συγκεκριμένα ποια ακριβώς στοιχεία είναι αναγκαία. Στο άρθρο 8 του Ν. 4489/2017 αποτυπώνεται η επιλογή του Έλληνα νομοθέτη, ο οποίος όρισε ως ελάχιστα απαραίτητα στοιχεία τα εξής: «*α) το όνομα, τη διεύθυνση, τους αριθμούς τηλεφώνου και τηλεομοιοτυπίας, καθώς και, αν υπάρχει, τη διεύθυνση ηλεκτρονικού ταχυδρομείου της δικαστικής αρχής που εξέδωσε ή επικύρωσε την ΕΕΕ, β) το αντικείμενο και τους λόγους έκδοσης της ΕΕΕ, γ) τα στοιχεία ταυτότητας και την ιθαγένεια του υπόπτου ή κατηγορουμένου, αν δε αυτός είναι ανήλικος ή ανίκανος προς δικαιοπραξία, τα στοιχεία ταυτότητας και την ιθαγένεια του αντιπροσώπου ή του επιτρόπου του, δ) περιγραφή της αξιόποινης πράξης που αποτελεί αντικείμενο έρευνας ή διαδικασίας, καθώς και των σχετικών ποινικών διατάξεων που την τυποποιούν, ε) περιγραφή του ή των*

[59]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

αιτούμενων ερευνητικών μέτρων που πρέπει να ληφθούν και των αποδεικτικών στοιχείων που πρέπει να συγκεντρωθούν».

Η διατύπωση του ελληνικού νόμου δεν απέχει ιδιαίτερα από τη διατύπωση της Οδηγίας, συγκεκριμενοποιεί όμως ποια στοιχεία της αρχής έκδοσης, καθώς και του ατόμου, το οποίο αφορά η διαδικασία, είναι απαραίτητα. Ωστόσο, χρειάζεται πράξη διευκρίνισης των όσων αναφέρονται στην ΕΕΕ αναφορικά με την αξιόποινη πράξη που φέρεται να τέλεσε ο ύποπτος ή ο κατηγορούμενος, αλλά και για το αιτούμενο ερευνητικό μέτρο και αυτό διότι υπάρχουν διαφορές ανάμεσα στις ποινικές νομοθεσίες των κρατών σε συνδυασμό με τον διαφορετικό βαθμό βεβαιότητας σχετικά με την τέλεση αξιόποινης πράξης που απαιτείται σε κάθε στάδιο της ποινικής διαδικασίας. Η ανάγκη αυτή δε εμφανιζόταν σπάνια και στο παλαιό καθεστώς, με αποτέλεσμα την καθυστέρηση στην παροχή δικαστικής συνδρομής.[60] Συγκεκριμένα, εφόσον οι αρχές του κράτους εκτέλεσης μπορούν να συμβουλευθούν[61] τις αρχές έκδοσης «σχετικά με τη σημασία εκτέλεσης της ΕΕΕ» όταν έχουν αμφιβολίες για την συμμόρφωση του κράτους έκδοσης με την αρχή της αναλογικότητας, θα είναι αναμφισβήτητα δυνατό και εφικτό να επικοινωνήσουν με τις αρχές έκδοσης ζητώντας λεπτομέρειες για την αξιόποινη πράξη και το ερευνητικό μέτρο που πρέπει να εκτελεσθεί.

ΣΤ. ΣΥΜΦΩΝΙΕΣ ΜΕΤΑΞΥ ΕΕ ΚΑΙ ΗΠΑ

Ουσιαστικά μεταξύ της ΕΕ και των ΗΠΑ συνάφθηκε μια συμφωνία η οποία καθορίζει τους όρους που αφορούν την παροχή αμοιβαίας δικαστικής συνδρομής σε ποινικές υποθέσεις μεταξύ της ΕΕ και των ΗΠΑ.

[60] Bachmaier Winter L., Transnational Evidence, ό.π., σελ. 51.

[61] Σύμφωνα με το άρθρο 9 παρ. 6 της Οδηγίας αλλά και με ένα επιχείρημα εκ του μείζονος στο έλασσον, στηριζόμενο στο άρθρο 6 παρ. 3 της Οδηγία

Σκοπός είναι η ενίσχυση της συνεργασίας μεταξύ των χωρών της ΕΕ και των ΗΠΑ, συμπληρωματικά με τις διμερείς συνθήκες που έχουν συναφθεί μεταξύ των χωρών της ΕΕ και των ΗΠΑ. Με την απόφαση συνάπτεται εξ ονόματος της ΕΕ η συμφωνία με τις ΗΠΑ σχετικά με την αμοιβαία δικαστική συνδρομή.

Συγκεκριμένα τα βασικά σημεία της συγκεκριμένης συμφωνίας είναι τα ακόλουθα:

Οι χώρες της ΕΕ και οι ΗΠΑ εφαρμόζουν τους όρους της εν λόγω συμφωνίας-πλαισίου στις διμερείς συνθήκες αμοιβαίας δικαστικής συνδρομής. Εν απουσία τέτοιας συνθήκης, η ΕΕ και οι ΗΠΑ αναλαμβάνουν να εξασφαλίσουν την εφαρμογή της συμφωνίας. Σε περίπτωση που οι υφιστάμενες διμερείς συνθήκες μεταξύ των χωρών της ΕΕ και των ΗΠΑ δεν είναι συμβατές με τη συμφωνία, θα πρέπει να υπερισχύει το πλαίσιο της ΕΕ. Η συμφωνία θεσπίζει τους όρους σχετικά με την έκδοση εγκληματιών μεταξύ της ΕΕ και των ΗΠΑ, με σκοπό τη βελτίωση της συνεργασίας στο πλαίσιο των υφιστάμενων σχέσεων σε θέματα έκδοσης. Με την απόφαση συνάπτεται εξ ονόματος της ΕΕ η συμφωνία με τις ΗΠΑ σχετικά με την έκδοση. Η συμφωνία συμπληρώνει τις διμερείς συνθήκες έκδοσης μεταξύ των χωρών της ΕΕ και των ΗΠΑ και ενισχύει τη συνεργασία στο πλαίσιο των υφιστάμενων σχέσεων σε θέματα έκδοσης.

Οι πράξεις για τις οποίες χωρεί έκδοση συνίστανται στις πράξεις οι οποίες τιμωρούνται από το δίκαιο τόσο της χώρας που ζητεί την έκδοση όσο και της χώρας από την οποία ζητείται η έκδοση με στερητική της ελευθερίας ποινή για μέγιστο χρονικό διάστημα (άνω του ενός έτους) ή με αυστηρότερη ποινή. Επίσης, το ίδιο ισχύει και για τη πράξη της απόπειρας διάπραξης ή συμμετοχής στη διάπραξη ενός τέτοιου αδικήματος. Εάν η χώρα από την οποία ζητείται η έκδοση επιτρέψει την έκδοση για μια πράξη για την οποία χωρεί έκδοση, πρέπει να επιτρέψει την έκδοση και για όλα τα άλλα αδικήματα που περιλαμβάνονται στην αίτηση, εφόσον το άλλο αδίκημα

τιμωρείται με στερητική της ελευθερίας ποινή ανωτάτου ορίου ενός έτους και πληρούνται όλες οι άλλες απαιτήσεις έκδοσης.

Επιπροσθέτως, οι χώρες της ΕΕ και οι ΗΠΑ μπορούν να επιτρέπουν τη διέλευση μέσω των εδαφών τους ενός ατόμου που παραδόθηκε από το ένα ή το άλλο μέρος σε μια τρίτη χώρα, ή το αντίστροφο. Οι αιτήσεις διέλευσης μπορούν να πραγματοποιούνται μέσω της διπλωματικής οδού, απευθείας μεταξύ του Υπουργείου Δικαιοσύνης των ΗΠΑ και του Υπουργείου Δικαιοσύνης της χώρας της ΕΕ ή μέσω της Interpol. Δεν απαιτείται άδεια για τις αεροπορικές μεταφορές, υπό την προϋπόθεση ότι δεν έχει προγραμματιστεί προσγείωση στο έδαφος της χώρας διέλευσης. Σε περίπτωση έκτακτης προσγείωσης, η εν λόγω χώρα μπορεί να ζητήσει αίτηση διέλευσης.

Αναφορικά με την αμοιβαία δικαστική συνδρομή

Όσον αφορά τις τραπεζικές πληροφορίες, κατόπιν αιτήσεως της αιτούσας χώρας, η χώρα στην οποία απευθύνεται η αίτηση πρέπει να **εντοπίζει και να γνωστοποιεί** ταχέως τα εξής: εάν ένα φυσικό ή νομικό πρόσωπο το οποίο είναι ύποπτο ή κατηγορούμενο για ποινικό αδίκημα έχει έναν ή περισσότερους τραπεζικούς λογαριασμούς, πληροφορίες σχετικά με άτομα ή νομικές οντότητες που έχουν καταδικασθεί για ποινικό αδίκημα ή ενέχονται σε ποινικό αδίκημα·, πληροφορίες που βρίσκονται στην κατοχή μη τραπεζικού χρηματοπιστωτικού ιδρύματος, πληροφορίες σχετικά με χρηματοοικονομικές συναλλαγές που δεν σχετίζονται με τραπεζικούς λογαριασμούς. Επίσης, οι αιτήσεις συνδρομής των χωρών της ΕΕ **διαβιβάζονται** από τις κεντρικές αρχές που είναι υπεύθυνες για την αμοιβαία δικαστική συνδρομή ή από τις εθνικές αρχές που είναι υπεύθυνες για τη διερεύνηση ή τη δίωξη εγκλημάτων. Οι ΗΠΑ διαβιβάζουν τις αιτήσεις

συνδρομής τους μέσω των εθνικών τους αρχών οι οποίες είναι υπεύθυνες για τη διερεύνηση ή τη δίωξη εγκλημάτων και οι οποίες ορίζονται ειδικά κατ' εφαρμογή του άρθρου15 παράγραφος 2 της συμφωνίας. Η αιτούσα χώρα μπορεί να χρησιμοποιήσει ένα άμεσο μέσο επικοινωνίας, συμπεριλαμβανομένης της τηλεομοιοτυπίας (φαξ) ή του ηλεκτρονικού ταχυδρομείου, για τη διαβίβαση της αίτησης συνδρομής και της σχετικής επικοινωνίας, συνοδευόμενων από τυπική επιβεβαίωση, εφόσον απαιτείται από τη χώρα στην οποία απευθύνεται η αίτηση. Η αιτούσα χώρα μπορεί να ζητήσει από τη χώρα στην οποία απευθύνεται η αίτηση να παραμείνουν εμπιστευτικά τόσο η αίτηση όσο και το περιεχόμενό της. Εάν η κεντρική αρχή της χώρας στην οποία απευθύνεται η αίτηση δεν μπορεί να ικανοποιήσει την αίτηση συνδρομής χωρίς παραβίαση της εμπιστευτικότητας, πρέπει να πληροφορήσει σχετικά την αιτούσα χώρα. Εν συνεχεία, η αιτούσα χώρα πρέπει να αποφασίσει εάν η αίτηση συνδρομής θα πρέπει να ικανοποιηθεί ή όχι. Η ΕΕ και οι ΗΠΑ οφείλουν να επιτρέπουν τη συγκρότηση και τη λειτουργία κοινών ερευνητικών ομάδων, για τη διευκόλυνση των ανακρίσεων ή των ποινικών διώξεων μεταξύ μίας ή περισσότερων χωρών της ΕΕ και των ΗΠΑ. Επιπλέον, η ΕΕ και οι ΗΠΑ οφείλουν να επιτρέπουν τις τηλεεικονοδιασκέψεις μεταξύ των χωρών της ΕΕ και των ΗΠΑ για τη λήψη καταθέσεων από μάρτυρες ή εμπειρογνώμονες στο πλαίσιο διαδικασιών.

Αναφορικά με τη συνδρομή που παρέχεται σε διοικητικές αρχές:

Αμοιβαία δικαστική συνδρομή πρέπει να παρέχεται επίσης στις εθνικές και σε άλλες διοικητικές αρχές, αλλά μόνο όταν για την ερευνώμενη συμπεριφορά προβλέπεται ποινική δίωξη ή παραπομπή στις ερευνητικές ή διωκτικές αρχές. Η συνδρομή δεν παρέχεται για θέματα για τα οποία η διοικητική αρχή προβλέπει ότι δεν θα υπάρξει, κατά περίπτωση, δίωξη ή παραπομπή. Οι αρχές που είναι υπεύθυνες για τη διαβίβαση των εν λόγω

αιτήσεων συνδρομής ορίζονται σύμφωνα με τις διμερείς συνθήκες περί αμοιβαίας δικαστικής συνδρομής μεταξύ των ενδιαφερόμενων χωρών. Εάν δεν υφίσταται τέτοια συνθήκη, οι αιτήσεις διαβιβάζονται μεταξύ του Υπουργείου Δικαιοσύνης των ΗΠΑ και του Υπουργείου Δικαιοσύνης ή άλλου αντίστοιχου Υπουργείου της χώρας της ΕΕ που είναι υπεύθυνη για τη διαβίβαση των αιτήσεων αμοιβαίας δικαστικής συνδρομής. Δεν μπορεί να αρνηθεί η συνδρομή για λόγους που αφορούν χορήγηση τραπεζικών στοιχείων που εμπίπτουν στο τραπεζικό απόρρητο.

Αναφορικά με την προστασία δεδομένων προσωπικού χαρακτήρα προβλέπονται τα εξής:

Η αιτούσα χώρα μπορεί να χρησιμοποιήσει μόνο τα αποδεικτικά στοιχεία ή τις πληροφορίες που διαβιβάζονται από τη χώρα στην οποία απευθύνεται η αίτηση: για ανακρίσεις και ποινικές διώξεις οι οποίες διεξάγονται σε αυτήν, για την προστασία της δημόσιας ασφάλειάς της από άμεση και σοβαρή απειλή, για μη ποινικές δικαστικές ή διοικητικές διαδικασίες οι οποίες έχουν κινηθεί σε αυτήν και οι οποίες συνδέονται άμεσα με ανακρίσεις ή ποινικές διώξεις, για άλλους σκοπούς, εφόσον οι πληροφορίες ή τα αποδεικτικά στοιχεία έχουν δημοσιοποιηθεί ή εφόσον η χώρα στην οποία απευθύνεται η αίτηση έχει δώσει προηγουμένως τη συγκατάθεσή της. Η χώρα στην οποία απευθύνεται η αίτηση μπορεί να επιβάλει επιπρόσθετους όρους που περιορίζουν τη χρήση των αποδεικτικών στοιχείων ή των πληροφοριών σε μια συγκεκριμένη περίπτωση εάν, λόγω της απουσίας αυτών των όρων, δεν ήταν σε θέση να ικανοποιήσει τη συγκεκριμένη αίτηση συνδρομής. Στην περίπτωση αυτή, η χώρα στην οποία απευθύνεται η αίτηση μπορεί να απαιτήσει από την αιτούσα χώρα να παράσχει πληροφορίες για τον τρόπο με τον οποίο χρησιμοποιεί τα αποδεικτικά στοιχεία ή τις πληροφορίες.

Επιπλέον των ανωτέρω περιορισμών στη χρήση, για την προστασία των δεδομένων προσωπικού χαρακτήρα και άλλων δεδομένων, η συμφωνία

μεταξύ των Ηνωμένων Πολιτειών της Αμερικής και της Ευρωπαϊκής Ένωσης σχετικά με την προστασία των πληροφοριών προσωπικού χαρακτήρα για την πρόληψη, τη διερεύνηση, την ανίχνευση και τη δίωξη ποινικών αδικημάτων (συμφωνία-πλαίσιο ΕΕ-ΗΠΑ) συμπληρώνει, όπου απαιτείται, τις εγγυήσεις της προστασίας των δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται στη συμφωνία.[62]

ΣΤ.1 Απόφαση Υπ'Αριθ.2000/520/ΕΚ

Γεγονός αποτελεί η δημιουργία προβλημάτων κατά τη διαβίβαση προσωπικών δεδομένων προς τρίτες χώρες που δεν διασφαλίζουν ένα ικανοποιητικό επίπεδο προστασίας, όπως είναι ιδίως, οι ΗΠΑ. Πιο συγκεκριμένα, ειδική περίπτωση συνιστά η συλλογή και διαβίβαση προσωπικών δεδομένων προς εταιρίες/φορείς που εδρεύουν στις ΗΠΑ. Αυτό συμβαίνει διότι σύμφωνα με το Αμερικανικό δίκαιο η επεξεργασία και η χρήση τους υπάγεται σε καθεστώς αυτορρύθμισης και αυτοπεριορισμού των εταιριών/φορέων-ιδιοκτητών ιστοσελίδων.[63] Κατά αυτό τον τρόπο η πολιτική διαχείρισης τους διαφοροποιείται και αυτό οδηγεί στη παροχή προστασίας κατώτερης των ευρωπαϊκών προτύπων. Σχετικά με τη διαβίβαση δεδομένων σε ιδιώτες, μέχρι πρόσφατα ήταν σε ισχύ οι αρχές «ασφαλούς λιμένα»(Safe Harbor),[64] μιας λίστας δηλαδή στην οποία μπορούν να καταχωρηθούν εθελοντικά οι αμερικανικές εταιρίες/φορείς υιοθετώντας ταυτόχρονα ένα συγκεκριμένο πλαίσιο προστασίας των προσωπικών δεδομένων των

[62] https://eur-lex.europa.eu/, Ιστοσελίδα Ευρωπαϊκής Ένωσης

[63] Βλ. Α Γραμματικάκη-Αλεξίου, Ηλεκτρονικό εμπόριο, ιδιωτικό διεθνές δίκαιο, διεθνές ομοιόμορφο δίκαιο και κοινοτικές ρυθμιστικές προσπάθειες- Μια συγκριτική επισκόπηση, ΕΕΕυρΔ 2001,σ.135

[64] Δηλαδή ειδικής συμφωνίας στην οποία προχώρησε η Ευρωπαϊκή Επιτροπή με το Υπουργείο Εμπορίου των ΗΠΑ. Το Δικαστήριο της ΕΕ (ΔΕΕ) είχε κηρύξει ανίσχυρη την απόφαση 2000/520 της Επιτροπής σύμφωνα με την οποία οι Ηνωμένες Πολιτείες εξασφάλιζαν ικανοποιητικό επίπεδο προστασίας (γνωστή και ως απόφαση "Safe Harbour - ασφαλούς λιμένα"), το ΔΕΕ, με την απόφαση Schrems II, προσφάτως κήρυξε ανίσχυρη και την απόφαση 2016/1250 σχετικά με την επάρκεια της προστασίας που παρέχεται από την ασπίδα προστασίας της ιδιωτικής ζωής Ευρωπαϊκής Ένωσης-Ηνωμένων Πολιτειών (γνωστή και ως απόφαση "EU-US Privacy Shield - ασπίδα προστασίας της ιδιωτικής ζωής"), η οποία είχε εκδοθεί σε αντικατάσταση της ακυρωθείσας απόφασης "ασφαλούς λιμένα".

πελατών τους εφάμιλλο του ευρωπαϊκού.[65]. Για να διασφαλιστεί η αξιοπιστία του εν λόγω εγχειρήματος, αναγκαίο και υποχρεωτικό είναι να τηρηθούν οι όροι προστασίας των προσωπικών δεδομένων ενώ η επανειλημμένη παραβίαση τους έχει ως απότοκο την αποβολή της εταιρίας/φορέα από την εν λόγω λίστα[66]. Συνεπώς, οι εταιρείες/φορείς που προχωρούν σ' αυτή, θεωρείται ότι πληρούν τις απαιτήσεις, που θέτει η ευρωπαϊκή –κοινοτική νομοθεσία και κατά συνέπεια η ροή δεδομένων προς αυτές είναι ελεύθερη. Συγκεκριμένα, σύμφωνα με την απόφαση υπ'αριθ. 2000/520 της Επιτροπής της ΕΕ, αναγνωριζόταν ότι όσοι οργανισμοί και εταιρείες στις ΗΠΑ προσχωρούσαν στις αρχές αυτές, μπορούσαν ελεύθερα να είναι αποδέκτες προσωπικών δεδομένων από την ΕΕ, υπό την προϋπόθεση ότι αυτοπιστοποιούνταν, με την κοινοποίηση εκ μέρους τους ορισμένων πληροφοριών προς το Υπουργείο Εμπορίου των ΗΠΑ. Η απόφαση αυτή, ωστόσο, κρίθηκε ως ανίσχυρη με την απόφαση της 6ης Οκτωβρίου 2015 του ΔΕΕ στην υπόθεση C-362/14 (Maximilian Shremms vs Data Protection Commissioner)[67]. Το Δικαστήριο προέβη, επίσης, στην ερμηνεία του άρθρου 25παρ.6 της Οδηγίας 95/46, για το οποίο δέχθηκε ότι έχει την έννοια ότι απόφαση που εκδίδεται βάσει της διατάξεως αυτής, όπως η απόφαση 200/520/ΕΚ της Επιτροπής, με την οποία η Ευρωπαϊκή Επιτροπή αποφαίνεται ότι η Τρίτη χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, δεν εμποδίζει την αρχή ελέγχου κράτους μέλους να εξετάσει αίτηση προσώπου σχετικά με την προστασία των δικαιωμάτων και των ελευθεριών του έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν,

[65]Βλ. Απόφαση 2000/520/ΕΚ της Ευρωπαϊκής Επιτροπής «σχετικά με επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ»,ΕΕL 115/14.

[66]Σύμφωνα με απόφαση της εποπτεύουσας Αρχής(Ομοσπονδιακή Επιτροπή Εμπορίου (FTC) και του Υπουργείου Μεταφορών των ΗΠΑ), https://eur-lτex.europa.eu/legal-content/el/TXT/?uri=CELEX:52002DC0045

[67]Βλ. Ιγγλεζάκη, Προστασία της ιδιωτικής ζωής. Η ακύρωση της απόφασης 200/520 της Επιτροπής της ΕΕ σχετικά με τις αρχές ασφαλούς λιμένα (Safe Harbour). Με αφορμή την απόφαση του ΔΕΕ στην υπόθεση C-362/14(Maximillian Schremms vs Data Protection Commissioner), Συνήγορος 111/2015, σελ.70

τα οποία έχουν διαβιβαστεί από κράτος μέλος προς την εν λόγω Τρίτη χώρα, όταν το πρόσωπο αυτό υποστηρίζει ότι η νομοθεσία και η πρακτική στην χώρα αυτή δεν εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας.[68]

Έπειτα, την 12η Ιουλίου 2016 υιοθετήθηκε η συμφωνία ΕΕ-ΗΠΑ με την ονομασία «ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα» (EU-U.S Privacy Shield)[69], η οποία άρχισε να ισχύει από 01.08.2016. Η νέα ρύθμιση συνεπάγεται πιο δεσμευτικές υποχρεώσεις για τις αμερικανικές εταιρείες και αυστηρότερη παρακολούθηση και επιβολή της νομοθεσίας, αλλά και αυστηρότερους κανόνες σχετικά με την πρόσβαση των δημόσιων αρχών των ΗΠΑ στα διαβιβαζόμενα δεδομένα.[70] Η "ασπίδα προστασίας" ακυρώθηκε τον Ιούλιο του 2020, καταφέροντας πλήγμα πολλές εταιρείες που είχαν βασιστεί στον μηχανισμό για τις ροές δεδομένων τους μεταξύ ΕΕ και ΗΠΑ.

ΣΤ.2 Συμφωνία Αμοιβαίας Δικαστικής Συνδρομής του 2003 μεταξύ ΕΕ και ΗΠΑ

Το έτος 2003 υπεγράφησαν μεταξύ της ΕΕ και των ΗΠΑ Συμφωνία αμοιβαίας δικαστικής συνδρομής και Συμφωνία έκδοσης[71,] οι οποίες τυγχάνουν συμπληρωματικής[72] εφαρμογής ως προς τις αντιστοίχου περιεχομένου συνθήκες, συμβάσεις ή συμφωνίες που τυχόν έχουν ήδη υπογράψει τα κράτη μέλη της ΕΕ με τις ΗΠΑ. Επομένως, στην περίπτωση της Ελλάδας οι ανωτέρω συμφωνίες εφαρμόζονται σε συνδυασμό με την κυρωθείσα με το Ν. 2804/2000, από 26-5-1999 διμερή μεταξύ Ελλάδας και ΗΠΑ

[68]Βλ. Ιωάννης Δημ. Ιγγλεζάκης, Δίκαιο Πληροφορικής, Γ΄έκδοση, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη

[69]https://www.privacyshield.gov, Privacy shield Framework

[70]Βλ. σχετικά Ι.Ιγγλεζάκη, Η ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα (EU-U.S Privacy Shield), Συνήγορος 113/2016, σελ.68 επ

[71]Δημοσιευθείσες αντιστοίχως στην ΕΕ L 181/34 της 19-7-2003 και ΕΕ L 181/27 της 19-7-2003.

[72]Βγόντζας Αντώνης, Δικαστική συνεργασία ΕΕ και ΗΠΑ – Μια νέα προοπτική στην καταπολέμηση του εγκλήματος ή μία ήττα του κράτους δικαίου;, ΠοινΔικ 2003, σελ. 743. Ως προς την ενδιαφέρουσα εν προκειμένω συμφωνία περί αμοιβαίας δικαστικής συνδρομής, σχετική πρόβλεψη υπάρχει στο άρθρο 3 παρ. 2 περ. α΄ αυτής

Σύμβαση αμοιβαίας δικαστικής συνδρομής σε ποινικές υποθέσεις και την κυρωθείσα με το Ν. 5554/1932, από 6-5-1931 διμερή μεταξύ Ελλάδας και ΗΠΑ Συνθήκη περί αμοιβαίας έκδοσης εγκληματιών και πλέον προβλέπεται κ η Ευρωπαϊκή Εντολή Έρευνας[73]. Και οι δύο ανωτέρω Συμφωνίες αντιμετώπισαν αρνητική δημοσιότητα στην ημεδαπή[74].

Η Σύμβαση Αμοιβαίας Δικαστικής Συνδρομής του 2003 μεταξύ ΕΕ και ΗΠΑ 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 ωριμάσε μετά τα τρομακτικά 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 τρομακρατίας. 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 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).

Από τις ανωτέρω Συμφωνίες, ενδιαφέρον εν προκειμένω παρουσιάζει αυτή περί αμοιβαίας δικαστικής συνδρομής και συγκεκριμένα το άρθρο 9 αυτής με τίτλο «*Περιορισμοί στη χρησιμοποίηση, για την προστασία των δεδομένων προσωπικού χαρακτήρα και άλλων*» και το τιτλοφορούμενο

[73]Δημοσιευθέντες αντιστοίχως στα Φ.Ε.Κ. Α΄ 49/3-3-2000 και Α΄ 218/7-7-1932.
[74]Χρυσικός Δημοσθένης, Η Συμφωνία Εκδόσεως μεταξύ Ευρωπαϊκής Ένωσης και ΗΠΑ – Σκέψεις και προβληματισμοί για ένα ζήτημα που δεν συζητήθηκε όσο θα έπρεπε, ΠοινΔικ 2003, σελ. 757

«Ταχεία διαβίβαση αιτήσεων» άρθρο 7 αυτής, σύμφωνα με το οποίο *«Οι αιτήσεις αμοιβαίας δικαστικής συνδρομής και οι σχετικές με αυτές γνωστοποιήσεις μπορούν να διαβιβάζονται με ταχέα μέσα επικοινωνίας, συμπεριλαμβανομένης της τηλεομοιοτυπίας (φαξ) ή του ηλεκτρονικού ταχυδρομείου, και ακολουθεί τυπική επιβεβαίωση, όταν απαιτείται, από το προς αίτηση κράτος. Το προς η αίτηση κράτος μπορεί να απαντά στην αίτηση με οιοδήποτε παρόμοιο ταχύ μέσο επικοινωνίας.»* Όπως προκύπτει από τη σύγκριση των διατάξεων του ως άνω άρθρου 9 της Συμφωνίας αμοιβαίας δικαστικής συνδρομής μεταξύ ΕΕ και ΗΠΑ και του άρθρου 7 της διμερούς Σύμβασης περί αμοιβαίας δικαστικής συνδρομής σε ποινικές υποθέσεις μεταξύ Ελλάδας και ΗΠΑ, καθίσταται προφανές ότι το επίπεδο προστασίας των υποβαλλομένων σε επεξεργασία ευαίσθητων προσωπικών δεδομένων έχει αυξηθεί στο πλαίσιο της Συμφωνίας μεταξύ ΕΕ και ΗΠΑ.

Το άρθρο 17 της Συμφωνίας προέβλεπε επανεξέταση της Συμφωνίας το αργότερο 5 έτη μετά την έναρξη της εφαρμογής της. Οι συζητήσεις για την επανεξέταση επέφεραν μια σειρά ζητημάτων όπως η αυξανόμενη ταχύτητα και ο αριθμός των αιτημάτων των Αρχών της Ε.Ε, που εκτελέστηκαν, ειδικά σε περιπτώσεις που περιελάμβαναν ηλεκτρονικά αποδεικτικά μέσα και η βελτίωση της απευθείας πρόσβασης των Ευρωπαϊκών Αρχών που διατηρούν οι Αμερικανοί Πάροχοι Υπηρεσιών. Τέλος, 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 αποτελούν βασικές προτεραιότητες προς βελτίωση της Συμφωνίας.

ΣΤ.3 Απευθείας επικοινωνία με Παρόχους Υπηρεσιών

Αυτή η περίπτωση αφορά την απευθείας συνεργασία των δικαστικών αρχών με τους αλλοδαπούς Παρόχους Υπηρεσιών. Πρακτικά, οι Δημόσιες Αρχές των Κρατών Μελών επικοινωνούν με τους Παρόχους 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 Ε.Ε.

Ο τρόπος αυτός αποτελεί τον κανόνα όσον αφορά την πρόσβαση των Ευρωπαϊκών δικαστικών αρχών σε ηλεκτρονικά μέσα που διατηρούν οι Πάροχοι Υπηρεσιών στις ΗΠΑ. Ομολογουμένως, οι αιτήσεις προς τους Παρόχους Υπηρεσιών αυξάνονται χρόνο με το χρόνο όπως επίσης και οι ανταπόκριση τους απέναντι στα αιτήματα που λαμβάνουν για πρόσβαση στα δεδομένα. Συγκεκριμένα λοιπόν, μεταξύ 2013-2016 σημειώθηκε αύξηση κατά 70% των αιτημάτων που προέρχονταν από Άρχές Κρατών Μελών της Ε.Ε προς τους Παρόχους Υπηρεσιών, υψηλό ποσοστό αιτημάτων επίσης παρατηρείται και σήμερα.

Το σημαντικό μειονέκτημα αυτής της συνεργασίας είναι ότι καλύπτει μόνο δεδομένα, που δεν αφορούν το περιεχόμενο, ενώ η πρόσβαση σε δεδομένα περιεχομένου απαγορεύεται από τη νομοθεσία των ΗΠΑ.

Η. Η ΔΙΑΣΥΝΟΡΙΑΚΗ ΡΟΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΓΙΑ ΣΚΟΠΟΥΣ ΕΘΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Η Ομάδα του άρθρου 29[75], η οποία τόνισε πως αφενός η νομοθεσία περί προσωπικών δεδομένων δεν εφαρμόζεται σε δραστηριότητες που αφορούν

[75]Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes (=Γνώμη 04/2014 σχετικά με την παρακολούθηση των ηλεκτρονικών επικοινωνιών για λόγους συλλογής πληροφοριών και εθνικής ασφάλειας) (819/14/EN WP 215).

την εθνική ασφάλεια, αφετέρου όμως εφαρμόζονται οι αρχές που προκύπτουν από τη Σύμβαση για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών [άλλως Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ)] και τη Σύμβαση 108, ήτοι οι αρχές της σύννομης και θεμιτής επεξεργασίας, του περιορισμού του σκοπού της επεξεργασίας, της αναγκαιότητας, της αναλογικότητας, της ακρίβειας και της διαφάνειας της επεξεργασίας, του σεβασμού των δικαιωμάτων των προσώπων και της επαρκούς ασφάλειας των δεδομένων.[76]

Επιπλέον, η Ομάδα του άρθρου 29 τόνισε πως τα παραπάνω αφορούν την εθνική ασφάλεια κρατών μελών της ΕΕ και όχι τρίτων κρατών. Επομένως, όταν η παρακολούθηση ευρωπαίων πολιτών διεξάγεται από τρίτα κράτη, τότε θα ισχύουν οι προϋποθέσεις του κεφαλαίου IV της Οδηγίας 95/46/ΕΚ περί διαβίβασης δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες. Όταν οι λόγοι εθνικής ασφάλειας ενός κράτους μέλους συμπίπτουν με εκείνους της τρίτης χώρας, θα πρέπει να δύνανται να αποδείξουν γιατί και πώς συμπίπτουν τα συμφέροντά τους, ώστε να παραμερισθούν οι διατάξεις του ευρωπαϊκού δικαίου περί προστασίας δεδομένων προσωπικού χαρακτήρα. Επίσης, υπογραμμίζει και ότι εταιρείες, οι οποίες επιτρέπουν την πρόσβαση υπηρεσιών ασφάλειας τρίτων χωρών στα αποθηκευμένα στους εξυπηρετητές τους προσωπικά δεδομένα ευρωπαίων πολιτών ή που συμμορφώνονται με διατάξεις περί παράδοσης σε τέτοιες υπηρεσίες μεγάλου όγκου προσωπικών δεδομένων ευρωπαίων πολιτών είναι πιθανόν να ενεργούν κατά παράβαση του ευρωπαϊκού δικαίου.

Στο σημείο αυτό χρήσιμη είναι η κατάδειξη της αρμοδιότητας της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.) για την αντιμετώπιση των ηλεκτρονικών επιθέσεων κατά υπολογιστικών συστημάτων. Συγκεκριμένα, η

[76]Αφορμή για την παραπάνω διαπίστωση ήταν η αποκάλυψη από τον Έντουαρντ Σνόουντεν (Edward Snowden) πρακτικών μαζικής παρακολούθησης των ηλεκτρονικών επικοινωνιών ακόμη και απλών πολιτών από μυστικές υπηρεσίες συγκεκριμένων κρατών.

Ε.Υ.Π.: *«Ορίζεται*[77] *ως η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων, η οποία μεριμνά για την πρόληψη και τη στατική και ενεργητική αντιμετώπιση ηλεκτρονικών επιθέσεων κατά δικτύων επικοινωνιών, εγκαταστάσεων αποθήκευσης πληροφοριών και συστημάτων πληροφορικής, σύμφωνα με τις διατάξεις της παρ. 3 του άρθρου 2 του π.δ. 325/2003.».* Ακόμη, αυτή ορίζεται ως Εθνικός Οργανισμός Ασφάλειας[78] σύμφωνα με το μέρος Ι παρ. 5 της Απόφασης 2001/264/ΕΚ116, δηλαδή, μεταξύ άλλων, και για «τη συγκέντρωση και καταγραφή στοιχείων για περιπτώσεις κατασκοπείας, δολιοφθορών, τρομοκρατίας και άλλες ανατρεπτικές δραστηριότητες».

ΣΥΜΠΕΡΑΣΜΑΤΑ

Από τα προπαρατεθέντα προκύπτει ότι η ανάγκη αντιμετώπισης της τρομοκρατίας και των νέων μορφών εγκληματικότητας, που ανακύπτουν στον σύγχρονο παγκοσμιοποιημένο κόσμο, ο οποίος χαρακτηρίζεται από τις αθρόες μετακινήσεις προσώπων και την καλπάζουσα τεχνολογική πρόοδο, αλλά και η ανάγκη προσαρμογής των προληπτικών και κατασταλτικών μεθόδων στο περιβάλλον της ΕΕ, όπου η μετακίνηση των προσώπων έχει διευκολυνθεί πολύ, συνεπεία του δικαιώματος ελεύθερης κυκλοφορίας των πολιτών της και των μελών της οικογένειάς τους εντός αυτής, επέβαλαν την ανάγκη θέσπισης των ανωτέρω συμφωνιών και συμβάσεων και την ίδρυση διεθνών οργανισμών, κοινό γνώρισμα των οποίων είναι ότι προβλέπουν την ηλεκτρονική διαβίβαση τεράστιων όγκων προσωπικών δεδομένων στο πλαίσιο λειτουργίας τους.

Σύμφωνα με το άρθρο 1 παρ. 3 της Οδηγίας 2002/58/ΕΚ, αυτή δεν εφαρμόζεται στις δραστηριότητες α) της κοινής εξωτερικής πολιτικής και της πολιτικής ασφάλειας (τίτλοςV της Συνθήκης για τη Ευρωπαϊκή Ένωση119),

[77]Σύμφωνα με το άρθρο 4 παρ. 8 Ν. 3649/2008114
[78]Σύμφωνα με το άρθρο 2 παρ. 3 του Π.Δ. 325/2003115

της β) αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις (τίτλος VI της Συνθήκης για τη Ευρωπαϊκή Ένωση) και γ) «σε κάθε περίπτωση στις δραστηριότητες που αφορούν τη δημόσια ασφάλεια, την εθνική άμυνα, την ασφάλεια του κράτους (συμπεριλαμβανομένης της οικονομικής ευημερίας του κράτους εφόσον οι δραστηριότητες συνδέονται με θέματα ασφάλειας του κράτους) και στις δραστηριότητες του κράτους σε τομείς του ποινικού δικαίου.». Αν και πολλές από τις προπαρατεθείσες συμβάσεις στο πλαίσιο της ΕΕ συνήφθησαν ακριβώς στο πλαίσιο των ανωτέρω δραστηριοτήτων, αυτό δεν επηρεάζει κατά κανένα τρόπο το ενδεχόμενο τόσο προσωπικά δεδομένα διαβιβαζόμενα στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις μεταξύ των κρατών μελών της ΕΕ όσο και προσωπικά δεδομένα διαβιβαζόμενα στο πλαίσιο των υπολοίπων προαναφερθεισών διακρατικών διαβιβάσεων να υποκλαπούν και χρησιμοποιηθούν για αθέμιτους σκοπούς. Εν όψει των ανωτέρω, αποκτά ξεχωριστή σημασία η ερμηνεία της ανωτέρω Οδηγίας για την ορθή οριοθέτηση τόσο της έννοιας των δεδομένων προσωπικού χαρακτήρα όσο και της ποινικής προστασίας τους στον τομέα των ηλεκτρονικών επικοινωνιών κατ' εφαρμογή του ενσωματώσαντος την Οδηγία αυτή στην ημεδαπή έννομη τάξη, σύμφωνα με τον Ν. 3471/2006.

ΔΕΥΤΕΡΟ ΜΕΡΟΣ: ΣΧΕΔΙΟ ΚΑΝΟΝΙΣΜΟΥ E-EVIDENCE

ΕΙΣΑΓΩΓΙΚΑ

ι)Βασικά εισαγωγικά στοιχεία

Οι νέοι κανόνες για την καλύτερη πρόσβαση στα ηλεκτρονικά αποδεικτικά στοιχεία που προτείνει η Επιτροπή στοχεύουν στην επιτάχυνση της πρόσβασης σε αυτά ανεξάρτητα από το πού βρίσκονται τα δεδομένα.

Επιπλέον, θα επιτρέπουν στις δικαστικές αρχές μιας χώρας της ΕΕ να ζητούν απευθείας πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία από κάθε πάροχο υπηρεσιών διαδικτύου που προσφέρει υπηρεσίες στην Ευρωπαϊκή Ένωση και είναι εγκατεστημένος ή εκπροσωπείται σε άλλο κράτος μέλος. Συνέπεια αυτών θα είναι η επιτάχυνση της διεκπεραίωσης της αίτησης πρόσβασης, διότι δεν θα υπάρχει ανάγκη μεσολάβησης των αρχών άλλου κράτους-μέλους.

Με τους νέους κανόνες θα επιτρέπεται στις αρχές επιβολής του νόμου να δίνουν τη δυνατότητα στα κράτη-μέλη της ΕΕ να διευρύνουν αποτελεσματικότερα ενδείξεις εγκληματικών πράξεων ηλεκτρονικά και διασυνοριακά, παρέχοντας συγχρόνως επαρκείς εγγυήσεις στα δικαιώματα και τις ελευθερίες όλων των εμπλεκομένων. Είναι γνωστό, πως όλοι οι εγκληματίες και τρομοκράτες χρησιμοποιούν μηνύματα κειμένου, μηνύματα ηλεκτρονικού ταχυδρομείου και εφαρμογές προκειμένου να επικοινωνούν.

Σύμφωνα με τα όσα δήλωσε σχετικά ο αντιπρόεδρος, κ. Φρανς Τίμερνανς: «*Τα ηλεκτρονικά αποδεικτικά στοιχεία αποκτούν ολοένα και μεγαλύτερη σημασία στις ποινικές διαδικασίες. Δεν μπορούμε να επιτρέψουμε στους εγκληματίες και τους τρομοκράτες να εκμεταλλεύονται σύγχρονες και ηλεκτρονικές τεχνολογίες επικοινωνίας για να κρύβουν τις εγκληματικές τους ενέργειες και να ξεφεύγουν από τη δικαιοσύνη. Οι εγκληματίες και οι τρομοκράτες δεν πρέπει να έχουν μέρος να κρυφτούν στη Ευρώπη, ούτε εντός ούτε εκτός του διαδικτύου. Οι σημερινές προτάσεις θα δημιουργήσουν για πρώτη φορά εργαλεία που θα επιτρέπουν στις αρμόδιες αρχές όχι μόνο να συλλέγουν ηλεκτρονικά αποδεικτικά στοιχεία διασυνοριακά, γρήγορα και αποτελεσματικά, αλλά και να παρέχουν συγχρόνως ισχυρές εγγυήσεις για τα δικαιώματα και τις ελευθερίες όλων των εμπλεκομένων*». Προς την ίδια κατεύθυνση κύλησε και ο λόγος της κ. Βέρας Γιούροβα, επίτροπο Δικαιοσύνης, Καταναλωτών και Ισότητας των Φύλων, η οποία δήλωσε σχετικά: «*Ενώ οι αρχές επιβολής του νόμου εξακολουθούν να εργάζονται με*

δύσκαμπτες μεθόδους, οι εγκληματίες χρησιμοποιούν ταχύτατες τεχνολογίες αιχμής για τη δράση τους. Πρέπει να εξοπλίσουμε τις αρχές επιβολής του νόμου με μεθόδους του 21ου αιώνα για την αντιμετώπιση της εγκληματικότητας ακριβώς όπως και οι εγκληματίες χρησιμοποιούν μεθόδους του 21ου αιώνα για να διαπράξουν τα εγκλήματα τους».

Σήμερα, οι περισσότερες ποινικές έρευνες περιλαμβάνουν διασυνοριακά αιτήματα για λήψη ηλεκτρονικών αποδεικτικών στοιχείων που τηρούνται από παρόχους υπηρεσιών οι οποίοι εδρεύουν σε άλλο κράτος μέλος ή εκτός ΕΕ. Σε αυτό το σημείο και προκειμένου να ληφθούν τα στοιχεία αυτά χρειάζεται δικαστική συνεργασία και αμοιβαία δικαστική συνδρομή, όμως η σχετική διαδικασία είναι αναντίρρητα αργή. Πλέον τα περισσότερα εγκλήματα για τα οποία υπάρχουν ηλεκτρονικά αποδεικτικά στοιχεία σε άλλη χώρα δεν μπορούν να διερευνηθούν ή να διωχθούν και αυτό συμβαίνει κατά κύριο λόγω διότι απαιτείται πολύς χρόνος για τη συγκέντρωση αυτών των στοιχείων και διότι το νομικό πλαίσιο είναι κατακερματισμένο.

Οι προτεινόμενοι κανόνες περιέχονται τόσο σε έναν κανονισμό σχετικά με τις ευρωπαϊκές εντολές υποβολής και διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις όσο και σε μια οδηγία σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον ορισμό νόμιμων εκπροσώπων με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών.

ιι)Αναφορά στο Cloud Act

Ο Νόμος "περί Νόμιμης Χρήσης Δεδομένων στο εξωτερικό" (Clarifying Lawful Overseas Use of Data Act or CLOUD Act - HR 4943)[79]είναι ένας ομοσπονδιακός νόμος των Ηνωμένων Πολιτειών, που θεσπίστηκε το Μάρτιο του 2018. Με τον σχετικό νόμο, τροποποιήθηκε η ισχύουσα από το 1986

[79]Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018) https://www.congress.gov/bill/115th-congress/house-bill/4943/text

Νομοθεσία (Stored Communications Act - SCA) προκειμένου να επιτραπεί στις ομοσπονδιακές αρχές επιβολής του νόμου των ΗΠΑ να υποχρεώσουν τις εταιρείες τεχνολογίας που εδρεύουν στις ΗΠΑ , μέσω εντάλματος ή κλήτευσης να παρέχουν ζητούμενα δεδομένα, που είναι αποθηκευμένα σε διακομιστές ακόμα και εάν τα δεδομένα δεν είναι αποθηκευμένα στις ΗΠΑ αλλά σε ξένο κράτος. Με άλλα λόγια μέσω της σχετικής διάταξης εξουσιοδοτούνται τα αρμόδια ανακριτικά όργανα των ΗΠΑ να αιτηθούν και να λάβουν πρόσβαση σε δεδομένα, αποθηκευμένα σε τρίτη χώρα.[80]Αξίζει να σημειωθεί ότι η παραπάνω νομοθετική διάταξη ψηφίστηκε ενόσω εκκρεμούσε στο Ανώτατο Δικαστήριο των ΗΠΑ η υπόθεση "United States vs Microsoft". Στην υπόθεση αυτή, το κύριο ζήτημα που τέθηκε ενώπιον του Ανωτάτου Δικαστηρίου ήταν εάν οι αρχές επιβολής του νόμου των ΗΠΑ δύνανται με ένταλμα να εξαναγκάσουν μια αμερικανική εταιρεία να αποκαλύψει το περιεχόμενο email που είναι αποθηκευμένο στο τρίτη χώρα. Το Υπουργείο Δικαιοσύνης (DOJ) είχε προσφύγει στο ομοσπονδιακό δικαστήριο ζητώντας έκδοση εντάλματος, προκειμένου να υποχρεωθεί η Microsoft να αποκαλύψει στις αρχές τόσο το περιεχόμενο όσο και εξωτερικά στοιχεία επικοινωνίας. Στην συγκεκριμένη περίπτωση, κάποια εξωτερικά στοιχεία επικοινωνίας ήταν αποθηκευμένα εγχώρια, ενώ το περιεχόμενο της επικοινωνίας δηλαδή των email, ήταν αποθηκευμένο σε ένα διακομιστή στο Δουβλίνο, στην Ιρλανδία. Η Microsoft παρείχε πληροφορίες για τα εξωτερικά στοιχεία επικοινωνίας, αλλά αρνήθηκε να εκπληρώσει το ένταλμα ως προς το περιεχόμενο της επικοινωνίας, υποστηρίζοντας ότι η σχετική αποκάλυψη θα συνιστούσε ανεπίτρεπτη εφαρμογή εθνικής νομοθεσίας σε υπερεθνικό έδαφος. Από την άλλη η κυβέρνηση των ΗΠΑ υποστήριξε ότι ο νόμος υποχρέωνε τους παρόχους να αποκαλύπτουν τυχόν αρχεία υπό τον έλεγχό τους. Μετά από πολλές προσφυγές και αποκλίνουσες αποφάσεις από τα δικαστήρια, η υπόθεση έφτασε στο Ανώτατο Δικαστήριο. Εν αναμονή λοιπόν της απόφασης στην υπόθεση της Microsoft, η "CLOUD Act" συμπεριλήφθηκε

[80]Jennifer Daskal, "Unpacking the CLOUD Act", 2018

σε μια τροπολογία σε ένα γενικό νομοσχέδιο δαπανών και πέρασε απότομα. Ο νόμος υπογράφηκε στις 23 Μαρτίου 2018. Η υπόθεση Ηνωμένες Πολιτείες κατά της Microsoft απορρίφθηκε. Ο νόμος "CLOUD Act", όπως σχεδόν κάθε νομοθετικό εγχείρημα, αποτέλεσε προϊόν συμβιβασμού κατόπιν διαπραγμάτευσης, με αποτέλεσμα, εγγενώς να είναι ατελής. Μεταξύ άλλων ελαττωμάτων και ελλείψεων, δεν ρυθμίζει το ενδεχόμενο πολυμερών συμφωνιών, αφήνοντας αναπάντητα βασικά ερωτήματα σχετικά με τη δυνατότητα και τα περιγράμματα μιας πιθανής συμφωνίας ΗΠΑ και Ευρωπαϊκής Ένωσης[81] και παραμελεί να παρέχει ρητή προστασία σε εταιρείες που ανταποκρίνονται σε αιτήματα ξένων κυβερνήσεων για χορήγηση δεδομένων.[82]

Στον αντίποδα, θα έλεγε κανείς ωστόσο ότι αντικατοπτρίζει επίσης μια προσπάθεια να ανταπόκρισης στις μεταβαλλόμενες ανάγκες της επιβολής του νόμου, δημιουργώντας νέους μηχανισμούς για την αντιμετώπιση των αναγκών αυτών.

iii)Αναγκαιότητα ψήφισης του σχεδίου Κανονισμού E-Evidence

Το πεδίο εφαρμογής του κανονισμού E-evidence αναφέρεται κυρίως στα εξής: οι εντολές για την υποβολή δεδομένων συνδρομητή και πρόσβασης μπορούν να εκδίδονται για οποιοδήποτε ποινικό αδίκημα, ενώ η πρόσβαση σε δεδομένα συναλλαγών και περιεχομένου θα πρέπει να υπόκειται σε αυστηρότερες απαιτήσεις, αυτό δείχνει συνάμα πόσο περισσότερο ευαίσθητη είναι η φύση των εν λόγω δεδομένων. Το όριο πρόσβασης στα δεδομένα αυτά εφαρμόζεται με βάση την αρχή της αναλογικότητας σε κάθε περίπτωση και σε συνδυασμό με συγκεκριμένες προϋποθέσεις. Στόχος είναι να εξασφαλίζεται ο σεβασμός τόσο της αναλογικότητας όσο και των δικαιωμάτων των επηρεαζόμενων προσώπων ενώ ταυτόχρονα το όριο που

[81]J. Daskal and P. Swire, "A Possible EU-US Agreement on Law Enforcement Access to Data?", Lawfare, 2018
[82]Jennifer Daskal, "Unpacking the CLOUD Act", 2018

εφαρμόζεται δεν θα πρέπει να περιορίζει την αποτελεσματικότητα της νομικής πράξης και χρήσης από τους επαγγελματίες του κλάδου. Επιπλέον, υπάρχουν συγκεκριμένα ποινικά αδικήματα για τα οποία τα αποδεικτικά στοιχεία είναι διαθέσιμα κυρίως σε ηλεκτρονική μορφή που σημαίνει πως αυτά έχουν παροδική διαθεσιμότητα. ανάμεσα σε αυτά είναι κυρίως εγκλήματα που συνδέονται με τον κυβερνοχώρο ή εγκλήματα που θα μπορούσαν να προκαλέσουν εκτενείς ή σοβαρές ζημιές. Στις περιπτώσεις μάλιστα που τα αδικήματα έχουν διαπραχθεί μέσω συστημάτων πληροφορικής η εφαρμογή του ίδιου ορίου όπως και για άλλα είδη αδικημάτων θα οδηγούσε κατά κύριο λόγο σε ατιμωρησία. Συνεπώς, η εφαρμογή του κανονισμού δικαιολογείται και για αδικήματα που το όριο της ποινής είναι μικρότερο από τρία έτη φυλάκιση. Ακόμη, σε περιπτώσεις στις οποίες τα ζητούμενα δεδομένα είναι αποθηκευμένα ή υποβάλλονται σε επεξεργασία στο πλαίσιο υποδομής που παρέχεται από πάροχο υπηρεσιών σε εταιρεία ή άλλη οντότητα που δεν είναι φυσικό πρόσωπο, συνήθως στην περίπτωση των υπηρεσιών φιλοξενίας, η ευρωπαϊκή εντολή υποβολής στοιχείων θα πρέπει να χρησιμοποιείται μόνο όταν δεν είναι πρόσφορη η λήψη άλλων ερευνητικών μέτρων που να απευθύνονται στην εταιρεία ή την οντότητα, ιδίως επειδή αυτό θα δημιουργούσε κίνδυνο υπονόμευσης της έρευνας. Το παρόν είναι σημαντικό για τις μεγαλύτερες οντότητες, όπως εταιρείες ή κρατικοί φορείς, που χρησιμοποιούν τις υπηρεσίες παρόχων υπηρεσιών για την παροχή των εταιρικών υποδομών ή υπηρεσιών ΤΠ τους ή και των δύο. Η εταιρεία ή άλλη οντότητα που αποτελεί τον πρώτο αποδέκτη ενδεχομένως να μην είναι πάροχος υπηρεσιών που υπάγεται στο πεδίο εφαρμογής του παρόντος κανονισμού.

Είναι σημαντικό να τονιστεί πως 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. Το εύρος και οι επιπτώσεις τους διαφέρουν ανάλογα με την εφαρμοστέα εθνική νομοθεσία που θα πρέπει να λαμβάνεται υπόψη κατά το χρόνο έκδοσης της εντολής, καθώς η αρχή έκδοσης μπορεί να εκδώσει την εντολή μόνο αν είναι διαθέσιμη παρόμοια εντολή για το ίδιο ποινικό αδίκημα σε συγκρίσιμη εγχώρια κατάσταση. Επιπροσθέτως αυτής της βασικής αρχής, ασυλίες και προνόμια που προστατεύουν τα δεδομένα πρόσβασης, συναλλαγών ή περιεχομένου στο κράτος μέλος του παρόχου υπηρεσιών θα πρέπει να λαμβάνονται υπόψη σε όσο το δυνατόν μεγαλύτερο βαθμό στο κράτος έκδοσης. Η διάταξη διασφαλίζει επίσης σεβασμό για τις υποθέσεις όπου η γνωστοποίηση των δεδομένων μπορεί να έχει επιπτώσεις για τα θεμελιώδη συμφέροντα του οικείου κράτους μέλους, όπως η εθνική ασφάλεια και άμυνα.

Τα ζητούμενα δεδομένα θα πρέπει να διαβιβάζονται στις αρμόδιες αρχές το αργότερο εντός 10 ημερών από την παραλαβή του πιστοποιητικού ΕΕΥ. Ο πάροχος θα πρέπει να συμμορφώνεται με συντομότερες προθεσμίες σε περιπτώσεις έκτακτης ανάγκης και όταν η αρχή έκδοσης αναφέρει άλλους λόγους παρέκκλισης από την δεκαήμερη προθεσμία. Εκτός από τον επικείμενο κίνδυνο διαγραφής των ζητούμενων δεδομένων, οι λόγοι αυτοί θα μπορούσαν να περιλαμβάνουν περιστάσεις που συνδέονται με υπό εξέλιξη έρευνα, για παράδειγμα όταν τα ζητούμενα δεδομένα σχετίζονται με άλλα επείγοντα ερευνητικά μέτρα που δεν μπορούν να υλοποιηθούν χωρίς τα δεδομένα που λείπουν ή που εξαρτώνται άλλως από αυτά.

Είναι σημαντική επιπλέον η πρόβλεψη μιας διαδικασίας για την επικοινωνία μεταξύ παρόχων υπηρεσιών και της δικαστικής αρχής έκδοσης σε περιπτώσεις όπου το πιστοποιητικό ευρωπαϊκής εντολής υποβολής στοιχείων (ΕΕΥ) ενδέχεται να είναι ελλιπές έτσι ώστε να δοθεί δυνατότητα στους παρόχους υπηρεσιών να αντιμετωπίζουν τυπικά προβλήματα.

Αν ο πάροχος υπηρεσιών δεν παράσχει τις πληροφορίες με εξαντλητικό τρόπο ή εγκαίρως για οποιονδήποτε άλλο λόγο, για παράδειγμα επειδή

θεωρεί ότι υπάρχει σύγκρουση με υποχρέωση που απορρέει από το δίκαιο τρίτης χώρας ή επειδή θεωρεί ότι η ευρωπαϊκή εντολή υποβολής στοιχείων δεν εκδόθηκε σύμφωνα με τους όρους του παρόντος κανονισμού, θα πρέπει να απευθύνεται στις αρχές έκδοσης και να τους παρέχει την προσήκουσα αιτιολόγηση. Ως εκ τούτου, η διαδικασία επικοινωνίας θα πρέπει να επιτρέπει γενικά τη διόρθωση ή την επανεξέταση του πιστοποιητικού ΕΕΥ από την αρχή έκδοσης σε πρώιμο στάδιο. Για να διασφαλίζεται η διαθεσιμότητα των δεδομένων, αν ο πάροχος υπηρεσιών μπορεί να εντοπίσει τα ζητούμενα δεδομένα, θα πρέπει να τα διατηρεί.[83]

Στο σημείο αυτό είναι απαραίτητο να τονιστεί πως οι πάροχοι υπηρεσιών και οι νόμιμοι εκπρόσωποί τους θα πρέπει να διασφαλίζουν το απόρρητο και, όταν αυτό ζητείται από την αρχή έκδοσης, να μην ενημερώνουν το πρόσωπο του οποίου τα δεδομένα ζητούνται, με σκοπό την προστασία της έρευνας ποινικών αδικημάτων, σε συμμόρφωση με το άρθρο 23 του κανονισμού (ΕΕ) 2016/679[84]. Ωστόσο, η ενημέρωση του χρήστη αποτελεί ουσιώδες στοιχείο που επιτρέπει τον έλεγχο και την προσφυγή στη δικαιοσύνη και, αν ζητήθηκε από τον πάροχο υπηρεσιών να μην ενημερώσει τον χρήστη, θα πρέπει να την παρέχει η αρχή σε περίπτωση που δεν υπάρχει κίνδυνος υπονόμευσης υπό εξέλιξη έρευνας, σύμφωνα με το εθνικό μέτρο με το οποίο έχει μεταφερθεί στο εθνικό δίκαιο το άρθρο 13 της οδηγίας (ΕΕ) 2016/68085.

[83]Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις.

[84]Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου2016, 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 οδηγίας95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

[85]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 (ΕΕL 119 της 4.5.2016, σ. 89).EL 41 EL

Σε περίπτωση μη συμμόρφωσης του αποδέκτη, η αρχή έκδοσης μπορεί να διαβιβάσει την πλήρη εντολή, συμπεριλαμβανομένου του σκεπτικού περί αναγκαιότητας και αναλογικότητας, μαζί με το πιστοποιητικό, στην αρμόδια αρχή του κράτους μέλους στο οποίο κατοικεί ή είναι εγκατεστημένος ο αποδέκτης του πιστοποιητικού. Το κράτος μέλος θα πρέπει να το εκτελεί σύμφωνα με την εθνική νομοθεσία του. Τα κράτη μέλη θα πρέπει να προβλέπουν την επιβολή αποτελεσματικών, αναλογικών και αποτρεπτικών χρηματικών κυρώσεων σε περίπτωση παραβιάσεων των υποχρεώσεων που προβλέπει ο παρών κανονισμός.

Όλα τα παραπάνω τα οποία σημειωτέον αποτελούν σκέψεις και αιτιολογία που οδήγησαν στην ψήφιση του Κανονισμού E-evidence θα αναλυθούν εκτενώς στο επόμενο μέρος της παρούσας εργασίας.

υι)Σύγκριση Cloud Act και E-Evidence

Αναντίρρητα, η νομοθετική πρωτοβουλία των ΗΠΑ "CLOUD ACT" αντιπροσωπεύει σε διεθνές επίπεδο την έναρξη ενός εποικοδομητικού διαλόγου για θέσπιση ουσιαστικών και διαδικαστικών κανόνων, που διέπουν την πρόσβαση των αρχών επιβολής του νόμου στα ψηφιακά αποδεικτικά στοιχεία και τη μεταβαλλόμενη σχέση μεταξύ των εδαφικών ορίων και της ανάγκης ψηφιακών αποδεικτικών στοιχείων. Από την άλλη, οι προτάσεις οδηγίας και κανονισμού "E- EVIDENCE" της Ευρωπαϊκής Ένωσης, αντιπροσωπεύουν τη συμβολή της Ευρώπης σε αυτή τη συζήτηση και έχουν αξιοσημείωτες ομοιότητες με τον νόμο CLOUD ACT. Ενώ ο νόμος "CLOUD ACT" έχει πλέον θεσπιστεί στη νομοθεσία των ΗΠΑ, η πρόταση της Ευρωπαϊκής Επιτροπής είναι ακόμη υπό εξέταση, κατά συνέπεια υπάρχει η ευκαιρία να τροποποιηθεί το κείμενο έτσι ώστε να ενισχυθούν οι εγγυήσεις για τα ατομικά δικαιώματα και να ελαχιστοποιηθούν οι κίνδυνοι. Οι δύο προτάσεις αν και έχουν σημαντικές διαφορές, παρουσιάζουν επίσης βασικές ομοιότητες. Και οι δύο προβλέπουν πρόσβαση σε δεδομένα και διατήρηση

αυτών ανεξάρτητα από το που αποθηκεύονται. Έτσι, πολλές από τις κριτικές που αφορούν το "CLOUD Act" να ισχύουν εξίσου και για την "E-Evidence". Ειδικότερα, όπως και στο "CLOUD ACT", έτσι και στο σχέδιο κανονισμού "E-EVIDENCE" προβλέπεται ένας μηχανισμός έκδοσης εντάλματος απευθείας προς ιδιωτική εταιρεία που κατέχει αποδεικτικά στοιχεία ενδιαφέροντος, ακόμη και αν αυτή η ιδιωτική εταιρεία βρίσκεται εκτός της εδαφικής δικαιοδοσίας της χώρας που διεξάγει την έρευνα, με στόχο την παράκαμψη της διαδικασίας αμοιβαίας νομικής συνδρομής.

Α. ΕΠΙΚΕΝΤΡΟ ΤΩΝ ΚΑΝΟΝΩΝ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ E-EVIDENCE

i) Η θέσπιση ευρωπαϊκής εντολής υποβολής στοιχείων:

Αυτό το μέτρο θα δίνει τη δυνατότητα σε δικαστική αρχή κράτους μέλους να ζητά ηλεκτρονικά αποδεικτικά στοιχεία (όπως μηνύματα ηλεκτρονικού ταχυδρομείου, κείμενα ή μηνύματα σε εφαρμογές) απευθείας από πάροχο υπηρεσιών που παρέχει υπηρεσίες στην Ένωση και είναι εγκατεστημένος ή εκπροσωπείται σε άλλο κράτος μέλος, ανεξάρτητα από τον τόπο στον οποίο βρίσκονται τα στοιχεία, και ο οποίος θα είναι υποχρεωμένος να απαντήσει μέσα σε 10 μέρες, και μέσα σε 6 ώρες σε περιπτώσεις έκτακτης ανάγκης (σε σύγκριση με τις 120 ημέρες που προβλέπονται για την υπάρχουσα ευρωπαϊκή εντολή έρευνας ή τους 10 μήνες που προβλέπονται για τη διαδικασία αμοιβαίας δικαστικής συνδρομής)·

ii) Η Αποτροπή της διαγραφής στοιχείων μέσω της πρόβλεψης μιας ευρωπαϊκής εντολής διατήρησης στοιχείων:

Αυτό το μέτρο θα δίνει τη δυνατότητα σε δικαστική αρχή κράτους μέλους να υποχρεώσει έναν πάροχο υπηρεσιών που παρέχει υπηρεσίες στην Ένωση και είναι εγκατεστημένος ή εκπροσωπείται σε άλλο κράτος μέλος να διατηρήσει συγκεκριμένα στοιχεία, ώστε να μπορέσει η αρχή να ζητήσει αυτά τα στοιχεία αργότερα μέσω αμοιβαίας δικαστικής συνδρομής, ευρωπαϊκής εντολής έρευνας ή ευρωπαϊκής εντολής υποβολής στοιχείων. Η ψηφιοποίηση της δικαιοσύνης[86]σκοπό έχει να διευκολύνει την πρόσβαση στη δικαιοσύνη, να βελτιώσει την εν γένει αποτελεσματικότητα και να διασφαλίσει την ανθεκτικότητα των δικαστικών συστημάτων σε περιόδους κρίσεων, όπως η πανδημία COVID-19. Το σύστημα e-CODEX[87] (επικοινωνία μέσω επιγραμμικής ανταλλαγής δεδομένων στον τομέα της ηλεκτρονικής δικαιοσύνης) αποτελεί βασικό τεχνολογικό και ψηφιακό καταλύτη για τον εκσυγχρονισμό των επικοινωνιών στο πλαίσιο της διασυνοριακής δικαστικής επικοινωνίας. Το e-CODEX καθιστά δυνατή τη διαλειτουργικότητα των συστημάτων ΤΠ που χρησιμοποιούν οι δικαστικές αρχές. Επιτρέπει σε διαφορετικά εθνικά συστήματα ηλεκτρονικής δικαιοσύνης να διασυνδέονται για να ανταλλάσσουν δεδομένα που αφορούν αστικές και ποινικές υποθέσεις.

---

[86]Η αποτελεσματική πρόσβαση στη δικαιοσύνη στην ΕΕ παρεμποδίζεται από την ανάγκη για ανταλλαγές εγγράφων σε χαρτί και για φυσική παρουσία. Οι ψηφιακές τεχνολογίες έχουν τη δυνατότητα να διευκολύνουν την πρόσβαση στα συστήματα δικαιοσύνης και να βελτιώσουν την απόδοση αυτών των συστημάτων. Η πρωτοβουλία αυτή θα καθορίσει μια δέσμη μέτρων για την ενίσχυση της ψηφιοποίησης στα συστήματα δικαιοσύνης σε ολόκληρη την ΕΕ, συμπεριλαμβανομένων πιθανών μέτρων για τη νομοθεσία, τη χρηματοδότηση και την πληροφορική, https://ec.europa.eu/info/law/betterregulation/haveyoursay/initiatives/12547%CE%A8%CE%B7%CF%86%CE%B9%CE%BF%CF%80%CE%BF%CE%B9%CE%B7%CF%83%CE%B7%CF%84%CE%B7%CF%82%CE%B4%CE%B9%CE%BA%CE%B1%CE%B9%CE%BF%CF%83%CF%85%CE%D%CE%B7%CF%82-%CF%83%CF%84%CE%B7%CE%BD-%CE%95%CE%95_el

[87]https://en.wikipedia.org/wiki/Fore-CODEX, Ερμηνεία Fore CODEX

Το σύστημα αυτό αναπτύσσεται επί σειρά ετών και επί του παρόντος τελεί υπό τη διαχείριση κοινοπραξίας κρατών μελών και άλλων οργανισμών. Στόχος του συμβιβαστικού κειμένου είναι να παράσχει ένα βιώσιμο, μακροπρόθεσμο νομικό πλαίσιο για το σύστημα, μεταβιβάζοντας τη διαχείρισή του στον eu-LISA.

Ο οργανισμός αναμένεται να αναλάβει την ευθύνη του συστήματος e-CODEX το νωρίτερο την 1η Ιουλίου 2023 και το αργότερο στις 31 Δεκεμβρίου 2023. Το προσωρινό κείμενο εισάγει διατάξεις για την προστασία της ανεξαρτησίας της δικαστικής εξουσίας, στοιχεία σχετικά με τη δομή διακυβέρνησης και διαχείρισης εντός του eu-LISA και δυνατότητες για τα κράτη μέλη να συμβάλουν στην περαιτέρω ανάπτυξη του συστήματος e-CODEX.

Αναφορικά με το γενικότερο πλαίσιο, εντός του οποίου θα τύχει εφαρμογής το συγκεκριμένο σύστημα, πρέπει να αναφερθούν ορισμένα στοιχεία. Το σύστημα e-CODEX αποτελείται από δέσμη στοιχείων λογισμικού που καθιστά δυνατή τη συνδεσιμότητα μεταξύ εθνικών συστημάτων. Παρέχει στους χρήστες του (αρμόδιες δικαστικές αρχές, επαγγελματίες του νομικού κλάδου και πολίτες) τη δυνατότητα ηλεκτρονικής αποστολής ή λήψης εγγράφων, νομικών εντύπων, αποδεικτικών στοιχείων ή άλλων πληροφοριών με ταχύτητα και ασφάλεια. Με τον τρόπο αυτό το e-CODEX καθιστά δυνατή τη συγκρότηση διαλειτουργικών και ασφαλών αποκεντρωμένων δικτύων για την επικοινωνία μεταξύ των εθνικών συστημάτων ΤΠ που αναλαμβάνουν την υποστήριξη της διασυνοριακής συνεργασίας σε αστικές και ποινικές υποθέσεις. Για παράδειγμα, το e-CODEX παρέχει ήδη στήριξη στο σύστημα ηλεκτρονικής ανταλλαγής ψηφιακών πειστηρίων και υποστηρίζει τις ανταλλαγές σε περιπτώσεις ευρωπαϊκών εντολών έρευνας και αμοιβαίας δικαστικής συνδρομής στον τομέα της δικαστικής συνεργασίας σε ποινικές υποθέσεις.

iii)Ύπαρξη ισχυρών εγγυήσεων και μέσα έννομης προστασίας:

Και οι δύο εντολές μπορούν να εκδοθούν μόνο στο πλαίσιο ποινικών διαδικασιών και θα ισχύουν όλες οι δικονομικές εγγυήσεις του ποινικού δικαίου. Οι νέοι κανόνες εγγυώνται ισχυρή προστασία των θεμελιωδών δικαιωμάτων, όπως συμμετοχή των δικαστικών αρχών και πρόσθετες απαιτήσεις για τη λήψη ορισμένων κατηγοριών στοιχείων. Περιλαμβάνουν επίσης, εγγυήσεις για το δικαίωμα προστασίας των προσωπικών δεδομένων. Οι πάροχοι υπηρεσιών και τα πρόσωπα απ' τα οποία ζητούνται δεδομένα θα καλύπτονται από διάφορες εγγυήσεις, όπως η δυνατότητα του παρόχου υπηρεσιών να ζητήσει επανεξέταση αν, για παράδειγμα, η εντολή παραβιάζει προδήλως τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.

v) Υποχρέωση των παρόχων υπηρεσιών να ορίζουν νόμιμο εκπρόσωπο στην Ένωση:

Η Ευρωπαϊκή Επιτροπή προτείνει νέους κανόνες προκειμένου να δώσει τη δυνατότητα στις αστυνομικές και τις δικαστικές αρχές να λαμβάνουν ευκολότερα και ταχύτερα τα ηλεκτρονικά αποδεικτικά στοιχεία που χρειάζονται, π.χ. ηλεκτρονικά μηνύματα ή έγγραφα που βρίσκονται στο υπολογιστικό νέφος, για τη διερεύνηση, τη δίωξη και την καταδίκη εγκληματιών και τρομοκρατών. Οι νέοι κανόνες θα επιτρέψουν στις αρχές επιβολής του νόμου στα κράτη μέλη της ΕΕ να διερευνούν αποτελεσματικότερα ενδείξεις εγκληματικών πράξεων ηλεκτρονικά και διασυνοριακά, παρέχοντας συγχρόνως επαρκείς εγγυήσεις για τα δικαιώματα και τις ελευθερίες όλων των εμπλεκομένων. Όλοι οι εγκληματίες και οι τρομοκράτες χρησιμοποιούν μηνύματα κειμένου, μηνύματα ηλεκτρονικού ταχυδρομείου και εφαρμογές για να επικοινωνούν.

Σε διασυνοριακές υποθέσεις που αφορούν στη 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 Δικαστικής Συνεργασίας. Η δεύτερη αυτή οδός αφορά την απευθείας συνεργασία των δικαστικών αρχών με τους αλλοδαπούς παρόχους Υπηρεσιών. Για να διασφαλιστεί ότι όλοι οι πάροχοι υπηρεσιών που παρέχουν υπηρεσίες στην Ευρωπαϊκή Ένωση υπόκειται στις ίδιες υποχρεώσεις, ακόμη και αν η έδρα τους βρίσκεται σε τρίτη χώρα, υποχρεούται να ορίσουν νόμιμο εκπρόσωπο στην Ένωση για την παραλαβή, τη συμμόρφωση και την εκτέλεση των αποφάσεων και των εντολών που εκδίδονται από τις αρμόδιες αρχές των κρατών μελών για τη συγκέντρωση αποδεικτικών στοιχείων σε ποινικές διαδικασίες.

vi) Παροχή ασφαλείας δικαίου στις επιχειρήσεις και τους παρόχους υπηρεσιών:

Ενώ σήμερα οι αρχές επιβολής του νόμου εξαρτώνται συχνά από την καλή θέληση των παρόχων υπηρεσιών να τους παράσχουν τα αποδεικτικά στοιχεία που χρειάζονται, στον μέλλον η εφαρμογή των ίδιων κανόνων για την εντολή παροχής ηλεκτρονικών αποδεικτικών στοιχείων θα βελτιώσει την ασφάλεια δικαίου για τις αρχές και τους παρόχους υπηρεσιών.

Β. ΛΗΨΗ ΑΠΟΔΕΙΞΕΩΝ-ΝΕΟΣ ΚΑΝΟΝΙΣΜΟΣ ΕΕ 2020/1783

Βάση του άρθρου 7 του Κανονισμού ΕΕ 2020/1783 με τη λήψη των αποδείξεων που προβλέπεται προκύπτει η βελτίωση του συστήματος διαβιβάσεως παραγγελιών και αντίστροφης διαβίβασης διεξαχθεισών αποδείξεων, μέσω της ψηφιοποίησης αυτού. Αυτό επιτυγχάνεται, όπως και στον Κανονισμό για τις επιδόσεις, με την υποχρεωτική δημιουργία ενός αποκεντρωμένου συστήματος Τεχνολογιών Πληροφορικής(ΤΠ) που θα περιλαμβάνει εθνικά συστήματα ΤΠ μέσω μιας υποδομής επικοινωνιών και

θα επιτρέπει την ασφαλή και αξιόπιστη διασυνοριακή ανταλλαγή πληροφοριών σε πραγματικό χρόνο μεταξύ των εθνικών συστημάτων.

Επιπλέον, με την απευθείας διεξαγωγή αποδείξεων μέσω εικονοτηλεδιάσκεψης. αναμένεται να εξορθολογιστεί η διαβίβαση παραγγελιών και να καταστεί ευκολότερη η ακρόαση/εξέταση προσώπων χωρίς να απαιτείται να ταξιδέψουν σε άλλη χώρα.

Η ακρόαση μέσω βιντεοδιάσκεψης μπορεί να είναι σε ορισμένες περιπτώσεις ιδιαίτερα σημαντική για τη λυσιτελή εφαρμογή διατάξεων άλλων Κανονισμών και αξιόλογα τέτοια παραδείγματα προσφέρει ο αναθεωρημένος Κανονισμός 1111/2019(Βρυξέλες ΙΙ (β ή ter) αναφορικά ιδίως με την ακρόαση των γονέων και του παιδιού.

Γ. ΠΡΟΤΑΣΗ ΚΑΝΟΝΙΣΜΟΥ ΓΙΑ ΤΟ ΣΥΣΤΗΜΑ ΕΠΙΚΟΙΝΩΝΙΑΣ E-CODEX

Η ψηφιοποίηση της δικαστικής συνεργασίας που αδρομερώς περιγράφηκε ανωτέρω πρέπει να βασίζεται σε αρχές όπως διαλειτουργικότητα (εθνικών συστημάτων), φορητότητα, ασφάλεια και ακεραιότητα δεδομένων. Οι αρχές αυτές υπηρετούνται από το συστήματα του e-CODEX. Στις 2 Δεκεμβρίου 2020 η Επιτροπή υπέβαλε πρόταση Κανονισμού (έγγραφο 13709/20) σχετικά με ένα μηχανοργανωμένο σύστημα επικοινωνίας σε διασυνοριακές αστικές και ποινικές διαδικασίες(σύστημα e-CODEX)

Ανάθεση e-CODEX στον οργανισμό eu-LISA

Το σύστημα e-CODEX (επικοινωνία μέσω επιγραμμικής ανταλλαγής δεδομένων στον τομέα της ηλεκτρονικής δικαιοσύνης εγκαινιάστηκε στο

πλαίσιο του πολυετούς σχεδίου για την ηλεκτρονική δικαιοσύνη 2009-2013, με στόχο κυρίως την προώθηση της ψηφιοποίησης των διασυνοριακών δικαστικών διαδικασιών και τη διευκόλυνση της επικοινωνίας μεταξύ των δικαστικών αρχών των κρατών μελών. Αναπτύχθηκε από 21 κράτη μέλη (Μεταξύ των οποίων η Ελλάδα) τη συμμετοχή και άλλων τρίτων χωρών/εδαφών και οργανισμών μεταξύ 2010 και 2016 και τελεί υπό την διαχείριση κοινοπραξίας κρατών μελών και άλλων οργανισμών, που χρηματοδοτείται από επιχορήγηση της ΕΕ.

Η Επιτροπή, στην ανακοίνωση της με τίτλο- «Η ψηφιοποίηση της δικαιοσύνης στην Ευρωπαϊκή Ένωση-Μια εργαλειοθήκη ευκαιριών», την οποία δημοσίευσε την ίδια μέρα μαζί με την ανωτέρω πρόταση Κανονισμού, θεωρεί ότι το e-CODEX αποτελεί το κύριο εργαλείο και το σημείο αναφοράς για την δημιουργία ενός διαλειτουργικού, ασφαλούς και αποκεντρωμένου δικτύου επικοινωνίας μεταξύ εθνικών συστημάτων ΤΠ σε διασυνοριακές αστικές και ποινικές διαδικασίες.

Η εκτίμηση επιπτώσεων που συνοδεύει την πρόταση κατέδειξε ότι η καλύτερη λύση για τη διασφάλιση σταθερού μέλλοντος για το e- CODEX είναι η μεταφορά του στον «Ευρωπαϊκό Οργανισμό για τη λειτουργική διαχείριση συστημάτων ΤΠ μεγάλης κλίμακας στον χώρο ελευθερίας, ασφάλειας και δικαιοσύνης», γνωστό και ως «eu-LISA», και η εξουσιοδότηση του εν λόγω Οργανισμού να μεριμνά για τη λειτουργική διαχείριση συστήματος.

Δ. ΕΥΡΩΠΑΪΚΗ ΕΝΤΟΛΗ ΥΠΟΒΟΛΗΣ ΣΤΟΙΧΕΙΩΝ

i) Ορισμός

Είναι η δεσμευτική απόφαση Αρχής Έκδοσης Κράτους-Μέλους της ΕΕ, η οποία υποχρεώνει τον Πάροχο Υπηρεσιών, που παρέχει υπηρεσίες στην

Ένωση και είναι εγκατεστημένος ή εκπροσωπείται σε «άλλο Κράτος-Μέλος», να υποβάλλει ηλεκτρονικά αποδεικτικά στοιχεία[88]. Η παρούσα πρόταση κανονισμού εφαρμόζεται μόνο στις περιπτώσεις, στις οποίες ο πάροχος της υπηρεσίας είναι εγκατεστημένος ή εκπροσωπείται σε άλλο Κράτος-Μέλος και οι εντολές που προβλέπονται από τον Κανονισμό δεν μπορούν να χρησιμοποιηθούν για εγχώριες έρευνες. Ως «άλλο Κράτος-Μέλος» νοείται Κράτος-Μέλος διαφορετικό από αυτό, στο οποίο ανήκει η Αρχή Έκδοσης. 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 επικράτεια τους.[89]

ii) Προϋποθέσεις για την Έκδοση

Η Έκδοση ΕΕΥ στοιχείων, με τις οποίες ζητείται η υποβολή «δεδομένων συνδρομητή»[90] ή «δεδομένων πρόσβασης»[91] επιτρέπεται αρχικά για οποιοδήποτε αδίκημα, υπό την προϋπόθεση όμως ότι είναι αναγκαία και αναλογική και ότι διατίθεται παρόμοιο μέτρο για τον ίδιο ποινικό αδίκημα σε συγκρίσιμη εγχώρια κατάσταση στο Κράτος Έκδοσης[92]. 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*

[88]Σύμφωνα με τους ορισμούς της Πρότασης Κανονισμού που αναφέρονται στο άρθρο 2.
[89]Βλ. Αιτιολογική Σκέψη(15) της Πρότασης Κανονισμού Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών σε ποινικές υποθέσεις.
[90]Δεδομένα συνδρομητή: Πληροφορίες που αφορούν την ταυτότητα του συνδρομητή (ονοματεπώνυμο, ημερομηνία γέννησης, διεύθυνση, τηλέφωνο, κλπ.), καθώς και το είδος και τη διάρκεια της χρησιμοποιούμενης υπηρεσίας.
[91]Δεδομένα πρόσβασης: Πληροφορίες που αφορούν την έναρξη και λήξη της περιόδου πρόσβασης ενός χρήστη σε μια υπηρεσία (ημερομηνία και ώρα χρήσης, διεύθυνση IP, κλπ.)
[92]Βλ. Άρθρο 5 παρ.1,2,3 ό.π

άρθρου 3,4,5 της Απόφασης Πλαισίου 2001/413/ΔΕΥ[93]*, τα αδικήματα των άρθρων 3 έως 7 της Οδηγίας 2011/93ΕΕ*[94] *τα αδικήματα των άρθρων 3 έως 8 της Οδηγίας 2013/40/ΕΕ* [95]*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) 2017/541*[96]. Από τις τρεις αυτές προσπάθειες οι οποίες δεν πρέπει να συντρέχουν σωρευτικά η πρώτη σχετίζεται με 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 Κράτος 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 προστατευμένες σχέσεις (όπως το δικηγορικό απόρρητο), αναφέρονται και σε άλλες πράξεις αμοιβαίας αναγνώρισης, όπως η Ευρωπαϊκή Εντολή Έρευνας[97].

[93]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» (EEL 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.

[94]Οδηγία 2011/92/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και 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 17.2.2011

[95]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

[96]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 για την τροποποίηση της απόφασης 2005/671/ΔΕΥ του Συμβουλίου, ΕΕ L 88/6 της 31.3.2017

[97]Αιτιολογική Σκέψη 35 Πρότασης Κανονισμού

iii) Η αρμόδια αρχή Έκδοσης ΕΕΥ

Η ΕΕΥ στοιχείων για δεδομένα συναλλαγών[98] και δεδομένα περιεχομένου[99] μπορεί να εκδοθεί από δικαστή, δικαστήριο και ανακριτή με αρμοδιότητα στη συγκεκριμένη υπόθεση. Η 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 έκδοση της και να εγκριθεί αυτή από δικαστή, δικαστήριο ή ανακριτή του κράτους Έκδοσης. 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 συναλλαγών και δεδομένα περιεχομένου αλλά επιπρόσθετα οι τελευταίες δύναται να εκδίδονται ή να εγκρίνονται και από εισαγγελέα με αρμοδιότητα στη συγκεκριμένη υπόθεση. Καθώς τα δεδομένα συνδρομητή και τα δεδομένα πρόσβασης θεωρούνται λιγότερο ευαίσθητα, οι ΕΕΥ στοιχείων με τις οποίες ζητείται η γνωστοποίηση τους, 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.

[98]Δεδομένα συναλλαγών: Πληροφορίες που αφορούν την χρήση μιας υπηρεσίας από τον εκάστοτε συνδρομητή και επικεντρώνονται κυρίως στον εντοπισμό της πηγής και του προορισμού ενός μηνύματος, την ανίχνευση της τοποθεσίας της συσκευής, καθώς και τον ακριβή προσδιορισμό της ημερομηνίας, ώρας και διάρκειας μιας επικοινωνίας

[99]Δεδομένα περιεχομένου: Περιλαμβάνουν οποιαδήποτε πληροφορία μοιραζόμαστε στον ψηφιακό κόσμο και αποθηκεύεται σε ψηφιακή μορφή, όπως κείμενο, φωνή, βίντεο, εικόνες και ήχος.

v) Περιεχόμενο των ΕΕΥ

Η ΕΕΥ στοιχείων πρέπει να περιλαμβάνει τις ακόλουθες πληροφορίες[100]: 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 των λόγων για τους οποίους συνίσταται αυτά, σε περίπτωση που τα ζητούμενα δεδομένα αποθηκεύονται ή υποβάλλονται σε επεξεργασία ως μέρος υποδομής, που παρέχεται από τον Πάροχο Υπηρεσιών σε εταιρεία ή άλλη οντότητα που δεν είναι φυσικό πρόσωπο, επιβεβαίωση ότι η εντολή συμμορφώνεται με την οντότητα που δεν είναι φυσικό πρόσωπο, επιβεβαίωση ότι η εντολή συμμορφώνεται με την παράγραφο 6 του άρθρου 5 της πρότασης του 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 1 της πρότασης Κανονισμού[101].

Ε.ΠΡΟΒΛΗΜΑΤΙΣΜΟΙ ΣΧΕΤΙΚΑ ΜΕ ΤΟ ΣΧΕΔΙΟ ΚΑΝΟΝΙΣΜΟΥ

Η οδηγία 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου προβλέπει την απόκτηση, την πρόσβαση και την υποβολή αποδεικτικών

[100]Βλ. Άρθρο 5 παρ.5
[101]Βλ. άρθρο 8, Συνθήκη της Βουδαπέστης

στοιχείων σε ένα κράτος μέλος για ποινικές έρευνες και διαδικασίες σε άλλο κράτος μέλος. Οι διαδικασίες και τα χρονοδιαγράμματα που προβλέπονται στην ΕΕΕ μπορεί να μην ενδείκνυνται για τις ηλεκτρονικές πληροφορίες, οι οποίες είναι πιο ασταθείς και θα μπορούσαν να διαγραφούν ευκολότερα και ταχύτερα. Συνεπώς, ο παρών κανονισμός προβλέπει ειδικές διαδικασίες που αφορούν τη φύση των ηλεκτρονικών πληροφοριών. Ωστόσο, προκειμένου να αποφευχθεί μακροπρόθεσμα ο κατακερματισμός του πλαισίου της Ένωσης για τη δικαστική συνεργασία σε ποινικές υποθέσεις, η Επιτροπή θα πρέπει να διενεργήσει ενδιάμεση αξιολόγηση της λειτουργίας του κανονισμού σε σχέση με την οδηγία 2014/41/ΕΕ.

Ο παρών κανονισμός σέβεται τα θεμελιώδη δικαιώματα και τηρεί τις αρχές που αναγνωρίζονται από το άρθρο 6 της ΣΕΕ και από τον Χάρτη, από το διεθνές δίκαιο και τις διεθνείς συμφωνίες στις οποίες είναι συμβαλλόμενα μέρη η Ένωση ή όλα τα κράτη μέλη, συμπεριλαμβανομένης της Ευρωπαϊκής Σύμβασης για την Προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών, καθώς και από τα συντάγματα των κρατών μελών, στα αντίστοιχα πεδία εφαρμογής τους. Σε αυτά τα δικαιώματα και τις αρχές περιλαμβάνονται, ιδίως, ο σεβασμός της ιδιωτικής και οικογενειακής ζωής, η προστασία των δεδομένων προσωπικού χαρακτήρα, το δικαίωμα πραγματικής προσφυγής και αμερόληπτου δικαστηρίου, το τεκμήριο αθωότητας και τα δικαιώματα της υπεράσπισης, οι αρχές της νομιμότητας και της αναλογικότητας, καθώς και το δικαίωμα του προσώπου να μη δικάζεται ή να μην τιμωρείται ποινικά δύο φορές για την ίδια αξιόποινη πράξη.

Καμία διάταξη του παρόντος κανονισμού δεν θα μπορούσε να θεωρηθεί ότι απαγορεύει την άρνηση εκτέλεσης ευρωπαϊκή εντολής υποβολής στοιχείων, όταν υπάρχουν λόγοι, βάσει αντικειμενικών στοιχείων, οι οποίοι οδηγούν στο συμπέρασμα ότι η ευρωπαϊκή εντολή υποβολής στοιχείων εκδόθηκε με σκοπό τη δίωξη ή την τιμωρία προσώπου με βάση το φύλο, τη

φυλετική ή την εθνοτική καταγωγή, τη θρησκεία, τον σεξουαλικό προσανατολισμό ή την ταυτότητα φύλου, την ιθαγένεια, τη γλώσσα ή τις πολιτικές πεποιθήσεις του προσώπου αυτού, ή ότι το εν λόγω πρόσωπο ενδέχεται να περιέλθει σε δυσμενή θέση για οποιονδήποτε από τους λόγους αυτούς.

Ο μηχανισμός της ευρωπαϊκής εντολής υποβολής και της ευρωπαϊκής εντολής διατήρησης ηλεκτρονικών πληροφοριών σε ποινικές διαδικασίες λειτουργεί υπό την προϋπόθεση της αμοιβαίας εμπιστοσύνης μεταξύ των κρατών μελών και με βάση το τεκμήριο συμμόρφωσης των άλλων κρατών μελών με το δίκαιο της Ένωσης, το κράτος δικαίου και, ιδίως, με τα θεμελιώδη δικαιώματα, που αποτελούν ουσιώδη στοιχεία του χώρου ελευθερίας, ασφάλειας και δικαιοσύνης στην Ένωση. Ωστόσο, εάν η αρχή εκτέλεσης έχει βάσιμους λόγους να πιστεύει ότι η εκτέλεση ευρωπαϊκής εντολής υποβολής στοιχείων δεν θα ήταν συμβατή με τις υποχρεώσεις της όσον αφορά την προστασία των θεμελιωδών δικαιωμάτων που αναγνωρίζονται στο άρθρο 6 της ΣΕΕ και στον Χάρτη, η εκτέλεση της ευρωπαϊκής εντολής υποβολής στοιχείων θα πρέπει να απορρίπτεται. Προτού αποφασίσει να προβάλει έναν από τους λόγους μη αναγνώρισης ή μη εκτέλεσης που προβλέπονται στον παρόντα κανονισμό, η αρχή εκτέλεσης θα πρέπει να συμβουλεύεται την αρχή έκδοσης προκειμένου να λάβει οποιεσδήποτε αναγκαίες πρόσθετες πληροφορίες. Οι πληροφορίες σχετικά με αιτιολογημένη πρόταση της Επιτροπής προς το Συμβούλιο βάσει του άρθρου 7 παράγραφοι 1 και 2 της ΣΕΕ, η οποία υποδεικνύει συστημικές ή γενικευμένες ελλείψεις, θα πρέπει να έχουν ιδιαίτερη σημασία για τους σκοπούς της εν λόγω αξιολόγησης.

Αν υπάρχει απόφαση του Ευρωπαϊκού Συμβουλίου με την οποία διαπιστώνεται, υπό τις προϋποθέσεις του άρθρου 7 παράγραφος 2 της ΣΕΕ, ότι υπάρχει σοβαρή και διαρκής παραβίαση, στο κράτος μέλος έκδοσης, των αρχών που εξαγγέλλονται στο άρθρο 2 της ΣΕΕ, όπως αρχές που είναι

σύμφυτες με το κράτος δικαίου, η δικαστική αρχή εκτέλεσης μπορεί να αποφασίσει αυτεπάγγελτα να προβάλει έναν από τους λόγους μη αναγνώρισης ή μη εκτέλεσης που προβλέπονται στον παρόντα κανονισμό, χωρίς να χρειάζεται να προβεί σε ειδική αξιολόγηση.

Ο σεβασμός της ιδιωτικής και οικογενειακής ζωής και η προστασία των φυσικών προσώπων όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα αποτελούν θεμελιώδη δικαιώματα. Σύμφωνα με τα άρθρα 7 και 8 παράγραφος 1 του Χάρτη και το άρθρο 16 παράγραφος 1 της ΣΛΕΕ, κάθε πρόσωπο έχει δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής του ζωής, της κατοικίας και των επικοινωνιών του, και προστασίας των προσωπικών δεδομένων που το αφορούν. Κατά την εφαρμογή του παρόντος κανονισμού, τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα προστατεύονται και ότι η επεξεργασία τους πραγματοποιείται μόνο σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και την οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, καθώς και την οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται βάσει του παρόντος Κανονισμού θα πρέπει να υποβάλλονται σε επεξεργασία μόνο όταν αυτό είναι απαραίτητο και κατά τρόπο ανάλογο προς τους σκοπούς της πρόληψης, της διερεύνησης, της διαπίστωσης και της δίωξης εγκλημάτων ή της επιβολής ποινικών κυρώσεων και της άσκησης των δικαιωμάτων της υπεράσπισης. Ειδικότερα, τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι εφαρμόζονται κατάλληλες πολιτικές και μέτρα για την προστασία των δεδομένων ως προς τη διαβίβαση δεδομένων προσωπικού χαρακτήρα από τις αρμόδιες αρχές προς τους παρόχους υπηρεσιών για τους σκοπούς του παρόντος κανονισμού, συμπεριλαμβανομένων μέτρων για την ασφάλεια των δεδομένων. Οι πάροχοι υπηρεσιών θα πρέπει να διασφαλίζουν ότι οι ίδιες εγγυήσεις ισχύουν για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα

προς τις αρμόδιες αρχές. Μόνο εξουσιοδοτημένα πρόσωπα θα πρέπει να έχουν πρόσβαση σε πληροφορίες που περιέχουν δεδομένα προσωπικού χαρακτήρα.

Σύμφωνα με τη νομολογία του Ευρωπαϊκού Δικαστηρίου, η γενική και χωρίς διάκριση διατήρηση δεδομένων από τις εθνικές αρχές ασφαλείας της ΕΕ θίγει σοβαρά τους κανόνες περί προστασίας της ιδιωτικής ζωής που κατοχυρώνονται, ιδίως, στον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ. Ως εκ τούτου, η εφαρμογή του παρόντος κανονισμού δεν θα πρέπει να έχει ως αποτέλεσμα τη γενική και χωρίς διάκριση διατήρηση δεδομένων, ούτε θα πρέπει να θίγει τυχόν δικαιώματα ή υποχρεώσεις των παρόχων υπηρεσιών όσον αφορά την ασφάλεια των δεδομένων, συμπεριλαμβανομένου του δικαιώματος κρυπτογράφησης.

Σχετικά με τη νομική πλευρά

Ο βασικότερος προβληματισμός που προκύπτει είναι η ίδια η νομική βάση του Κανονισμού. Η βασικότερη νομική βάση που αφορά το σχέδιο Κανονισμού για τα ηλεκτρονικά αποδεικτικά στοιχεία, είναι το άρθρο 82 της ΣΛΕΕ, σχετικά με τη δικαστική συνεργασία σε ποινικά ζητήματα. Τα δικονομικά δικαιώματα στις ποινικές διαδικασίες, τα οποία προβλέπονται στις οδηγίες 2010/64/ΕΕ, 2012/13/ΕΕ, 2013/48/ΕΕ, 2016/343, 2016/800 και 2016/1919 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου θα πρέπει να εφαρμόζονται, εντός του πεδίου εφαρμογής των εν λόγω οδηγιών, στις ποινικές διαδικασίες που καλύπτονται από τον παρόντα κανονισμό όσον αφορά τα κράτη μέλη που δεσμεύονται από τις εν λόγω οδηγίες. Οι

δικονομικές εγγυήσεις που προβλέπονται στον Χάρτη θα πρέπει να εφαρμόζονται σε όλες τις διαδικασίες που καλύπτονται από τον παρόντα κανονισμό.

Σε περίπτωση που το κράτος μέλος έκδοσης έχει λόγους να πιστεύει ότι ενδέχεται να εκκρεμεί παράλληλη ποινική διαδικασία σε άλλο κράτος μέλος, θα πρέπει να συμβουλεύεται τις αρχές του εν λόγω κράτους μέλους σύμφωνα με την απόφαση-πλαίσιο 2009/948/ΔΕΥ του Συμβουλίου.

Η παρούσα νομική πράξη θεσπίζει τους κανόνες σύμφωνα με τους οποίους, στο πλαίσιο μιας ποινική διαδικασίας, αρμόδια δικαστική αρχή στην Ευρωπαϊκή Ένωση μπορεί να διατάξει έναν πάροχο υπηρεσιών που παρέχει υπηρεσίες στην Ένωση να υποβάλει ή να διατηρήσει ηλεκτρονικές πληροφορίες που μπορούν να χρησιμεύσουν ως αποδεικτικά στοιχεία μέσω ευρωπαϊκής εντολής υποβολής ή διατήρησης στοιχείων. Ο παρών κανονισμός εφαρμόζεται σε όλες τις διασυνοριακές περιπτώσεις στις οποίες ο πάροχος της υπηρεσίας έχει την κύρια εγκατάστασή του σε άλλο κράτος μέλος ή, εάν δεν είναι εγκατεστημένος στην Ένωση, εκπροσωπείται νομίμως σε άλλο κράτος μέλος. Οι αρχές των κρατών μελών δεν θα πρέπει να εκδίδουν εγχώριες εντολές με εξωεδαφικά αποτελέσματα για την υποβολή ή τη διατήρηση ηλεκτρονικών πληροφοριών που θα μπορούσαν να ζητηθούν βάσει του παρόντος κανονισμού.

Οι πάροχοι υπηρεσιών που παίζουν σημαντικότερο ρόλο στη συλλογή ηλεκτρονικών πληροφοριών στην ποινική διαδικασία είναι οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών και συγκεκριμένοι πάροχοι υπηρεσιών της κοινωνίας των πληροφοριών που διευκολύνουν την αλληλεπίδραση μεταξύ των χρηστών. Ως εκ τούτου, και οι δύο αυτές κατηγορίες παρόχων θα πρέπει να καλύπτονται από τον παρόντα κανονισμό. Οι υπηρεσίες ηλεκτρονικών επικοινωνιών ορίζονται στην οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Συμπεριλαμβάνουν υπηρεσίες διαπροσωπικών επικοινωνιών όπως υπηρεσίες φωνής μέσω IP, άμεσης ανταλλαγής μηνυμάτων και ηλεκτρονικού ταχυδρομείου. Οι κατηγορίες των υπηρεσιών της κοινωνίας των πληροφοριών που περιλαμβάνονται στον παρόντα κανονισμό είναι εκείνες στις οποίες η αποθήκευση των δεδομένων αποτελεί καθοριστικό στοιχείο της υπηρεσίας που παρέχεται στον χρήστη, και αφορούν ιδίως τα μέσα κοινωνικής δικτύωσης στον βαθμό που δεν χαρακτηρίζονται υπηρεσίες ηλεκτρονικών επικοινωνιών, τις επιγραμμικές αγορές που διευκολύνουν τις συναλλαγές μεταξύ των χρηστών τους (όπως καταναλωτές ή επιχειρήσεις) και άλλες υπηρεσίες φιλοξενίας, συμπεριλαμβανομένων υπηρεσιών που παρέχονται μέσω υπολογιστικού νέφους.

Οι πάροχοι υπηρεσιών υποδομής διαδικτύου (ISPs) που σχετίζονται με την εκχώρηση ονομάτων και αριθμών, όπως καταχωρητές και μητρώα ονομάτων χώρου και πάροχοι υπηρεσιών, διακομιστή μεσολάβησης, ή περιφερειακά μητρώα διαδικτύου για διευθύνσεις πρωτοκόλλου διαδικτύου («IP»), έχουν ιδιαίτερα σημαντικό ρόλο σε ό,τι αφορά την ταυτοποίηση των δραστών που βρίσκονται πίσω από κακόβουλους ή παραβιασμένους ιστότοπους. Τηρούν δεδομένα που θα μπορούσαν να επιτρέψουν την ταυτοποίηση του φυσικού προσώπου ή της οντότητας που βρίσκεται πίσω από ιστότοπο ο οποίος έχει χρησιμοποιηθεί σε εγκληματική δραστηριότητα, ή το θύμα εγκληματικής δραστηριότητας.

Οι εντολές που εκδίδονται στο πλαίσιο του παρόντος κανονισμού θα πρέπει να απευθύνονται στην κύρια εγκατάσταση των παρόχων υπηρεσιών ή, αν πρόκειται για παρόχους υπηρεσιών που δεν είναι εγκατεστημένοι σε ένα από τα κράτη μέλη που δεσμεύονται από τον παρόντα κανονισμό, στους νόμιμους εκπροσώπους που έχουν οριστεί γι' αυτόν τον σκοπό. Αν πρόκειται για πάροχο υπηρεσιών με εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, η κύρια εγκατάσταση θα πρέπει να είναι ο τόπος της κεντρικής του διοίκησης στην Ένωση, εκτός εάν οι αποφάσεις όσον αφορά τους σκοπούς και

τα μέσα της επεξεργασίας δεδομένων λαμβάνονται σε άλλη εγκατάσταση του παρόχου υπηρεσιών στην Ένωση και η εγκατάσταση αυτή έχει την εξουσία να εφαρμόζει τις εν λόγω αποφάσεις, οπότε ως κύρια εγκατάσταση θα πρέπει να θεωρείται η εγκατάσταση που έλαβε τις αποφάσεις αυτές·

Ο παρών κανονισμός ρυθμίζει μόνο τη συλλογή των δεδομένων που αποθηκεύει ο πάροχος υπηρεσιών κατά τον χρόνο έκδοσης της 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 έκδοσης της ευρωπαϊκής εντολής υποβολής ή διατήρησης στοιχείων.

Σχετικά με τη διάκριση των δεδομένων

Αυτό που παρατηρείται σε αυτή τη περίπτωση είναι πως αφενός δεν υπάρχει οριοθέτηση των τεσσάρων κατηγοριών δεδομένων και αφετέρου δεν παρουσιάζεται, ως προς την κατηγοριοποίηση των δεδομένων. Τα μεταδεδομένα περιλαμβάνονται τόσο στη κατηγορία «δεδομένων πρόσβασης», όσο και στην κατηγορία «δεδομένων συναλλαγών» με την προϋπόθεση ότι αυτά δεν αποτελούν «δεδομένα πρόσβασης».

Στη Σύμβαση της Βουδαπέστης για το Κυβερνοέγκλημα συναντάται ο όρος «πληροφορίες για συνδρομητές», στη Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες απαντώνται οι όροι «δεδομένα θέσης» και «δεδομένα κίνησης» στην Πρόταση Κανονισμού για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες εντοπίζονται οι όροι «περιεχόμενο ηλεκτρονικών επικοινωνιών» και «μεταδεδομένα ηλεκτρονικών επικοινωνιών». Είναι αξιοσημείωτο πως ο όρος «δεδομένα

συνδρομητή» δεν συναντάται σε καμία Οδηγία, ούτε στον Γενικό Κανονισμό Προστασίας Δεδομένων, ούτε στη Σύμβαση της Βουδαπέστης.

Επιχειρώντας να θέσει κανείς τα ψηφιακά δεδομένα σε ένα εννοιολογικό πλαίσιο, εντοπίζει **τέσσερα (4) επίπεδα**, καθένα από τα οποία θέτει διακριτά νομικά ζητήματα[102]:

α) Στο κατώτερο επίπεδο βρίσκονται **τα ίδια τα ψηφιακά δεδομένα**, τα οποία υπόκεινται σε κατάσχεση υπό την έννοια της αντιγραφής τους και θέσης του αντιγράφου στη διάθεση των αρχών, χωρίς ωστόσο να στερείται την πρόσβαση σε αυτά ο καθ' ου η κατάσχεση.

β) Σε ένα δεύτερο επίπεδο βρίσκεται ο **υλικός φορέας** στον οποίο αποθηκεύονται τα δεδομένα, ο οποίος υπόκειται σε κατάσχεση υπό την παραδοσιακή έννοια, και επομένως αφαιρείται από την κατοχή του καθ' ου.

γ) Αμέσως μετά βρίσκεται **ο χώρος** όπου φυλάσσεται ο υλικός φορέας, όπου ενδέχεται να τίθενται ειδικές προϋποθέσεις για τη διεξαγωγή έρευνας.

δ) Τέλος, η **εδαφική επικράτεια** όπου διακρατούνται τα δεδομένα, εφόσον δεν συμπίπτει με εκείνη του κράτους που διεξάγει την έρευνα, θέτει ζητήματα δικαστικής συνδρομής κατ' άρθρο 458 ΚΠΔ, είτε ζητήματα αποστολής Ευρωπαϊκής Εντολής Έρευνας (ΕΕΕ)[103].

Σχετικά με τη δικαστική προστασία

Ένα από τα πλέον καίρια σημεία κριτικής εντοπίζεται στο γεγονός πως η υποχρέωση συμμόρφωσης και εκτέλεσης μιας ΕΕΥ ή ΕΕΔ είναι πλέον

[102] Βλ. Ι. Ναζίρης στη Μελέτη του με θέμα «*Κατάσχεση ψηφιακών δεδομένων, κατ' άρθρο 265 του ΚΠΔ*», δημοσιευμένη στο ηλεκτρονικό τεύχος του νομικού περιοδικού «ΠΟΙΝΙΚΗ ΔΙΚΑΙΟΣΥΝΗ», Τεύχος 3ο, Μάρτιος 2021

[103] Βλ. Οδηγία 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 3ης Απριλίου 2014 περί της Ευρωπαϊκής Εντολής Έρευνας σε ποινικές υποθέσεις, η οποία ενσωμάτωσε ο Έλληνας Νομοθέτης στο εσωτερικό δικαϊκό μας σύστημα, με τον ν. 4489/2017

αρμοδιότητα του παρόχου των ηλεκτρονικών υπηρεσιών και όχι των κρατικών ή δικαστικών αρχών.

Ο πάροχος γίνεται πλέον υπεύθυνος για τον έλεγχο της προστασίας των θεμελιωδών δικαιωμάτων και καλείται να κρίνει εάν και κατά πόσο μια ΕΕΥ ή ΕΕΔ παραβιάζει τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.

Προκύπτει συνεπώς το ερώτημα κατά πόσο ο ιδιώτης πάροχος είναι κατάλληλος να αποφασίζει για την προστασία των θεμελιωδών δικαιωμάτων. Σε συνδυασμό μάλιστα με το γεγονός πως ο πάροχος υπόκειται σε κυρώσεις σε περίπτωση μη συμμόρφωσης με μία ΕΕΥ ή ΕΕΔ, είναι άξιο απορίας το εάν πράγματι θα πραγματοποιεί τον απαιτούμενο έλεγχο και θα μεριμνά για την προστασία των δικαιωμάτων ή υπό των φόβο της μη συμμόρφωσης θα προχωρά εν τέλει στην εκτέλεση κάθε ΕΕΥ.

Συνεπώς, το σημαντικότερο πρόβλημα που δημιουργείται με το νέο θεσμικό πλαίσιο είναι η μετατόπιση της υποχρέωσης ελέγχου της προστασίας των προσωπικών δεδομένων από το κράτος στον ιδιώτη πάροχο, ο οποίος επιφορτίζεται με την κρίσιμη απόφαση υποβολής ή μη των αποθηκευμένων δεδομένων, περιορίζοντας έτσι σημαντικά τον προστατευτικό ρόλο του κράτους.[104]

Η προβλεπόμενη προστασία που αφορά τους Αποδέκτες των εντολών, που επιτυγχάνεται μέσω των διαδικασιών ελέγχου των άρθρων 15 και 16 της Πρότασης Κανονισμού, αφορά μόνο της ΕΕΥ στοιχείων, με την αιτιολογία ότι η ΕΕΔ στοιχείων δεν έχουν ως αποτέλεσμα τη γνωστοποίηση δεδομένων και ότι ως εκ τούτου δε θα πρέπει να γεννιούνται ανησυχίες[105].

Ταυτόχρονα, η πράξη για την οποία ζητείται η υποβολή των προσωπικών δεδομένων δεν απαιτείται να ενέχει την ίδια απαξία στην έννομη τάξη του κράτους έκδοσης και του κράτους εκτέλεσης. Η κατάργηση του κριτηρίου

[104]Βλ. Άρθρο Κωνσταντίνου Ζουμπουλάκη «Η πρόσβαση των αρχών στα ηλεκτρονικά αποδεικτικά στοιχεία: Τι συμβαίνει με τα προσωπικά μας δεδομένα;», 19 Ιουνίου 2019 https://www.homodigitalis.gr/posts/3928

[105]Βλ. Αιτιολογική Έκθεση Πρότασης Κανονισμού

αυτού (dual criminality) μειώνει το επίπεδο προστασίας των προσωπικών δεδομένων και διευκολύνει την πρόσβαση ακόμη και σε περιπτώσεις που αφορούν ήσσονος σημασίας αδικήματα.

Το μοναδικό όριο που θέτει ο Κανονισμός αφορά την πρόσβαση σε δεδομένα συναλλαγών και περιεχομένου, όπου μια ΕΕΥ μπορεί να εκδοθεί μόνο για αδικήματα που επισύρουν στερητική της ελευθερίας ποινή με ανώτατο όριο τουλάχιστον τριών ετών στο κράτος έκδοσης.

Σε κάθε άλλη περίπτωση, ακόμη και αν οι νόμοι του κράτους εκτέλεσης προβλέπουν ένα αυξημένο πλαίσιο προστασίας των προσωπικών δεδομένων, αυτό είναι πλέον αδιάφορο. Παράλληλα, η υποβολή των δεδομένων συνδρομητή και πρόσβασης μπορεί να διαταχθεί για οποιοδήποτε αδίκημα.

Η σημασία των ηλεκτρονικών αποδεικτικών στοιχείων για την αποτελεσματική καταπολέμηση του εγκλήματος είναι αδιαμφισβήτητη. Στην εποχή των μέσων κοινωνικής δικτύωσης, ο όγκος και η ιδιαίτερη φύση των ψηφιακών δεδομένων καθιστούν πράγματι αναγκαία την θέσπιση νέων εργαλείων για την έγκαιρη και αποτελεσματική πρόσβαση των αρχών στα ψηφιακά δεδομένα.

Για να επιστρέψουμε ωστόσο και στο αρχικό μας ερώτημα, η παραδοχή αυτή δεν αρκεί για να άρει τους όποιους ενδοιασμούς εγείρει η νομοθετική πρόταση της Ευρωπαϊκής Ένωσης. Η ανάγκη για αποτελεσματικότητα πρέπει να συμβαδίζει με το κρίσιμο αίτημα της αποτελεσματικής προστασίας των προσωπικών δεδομένων και είναι συνεπώς καθήκον του Ευρωπαίου νομοθέτη να κινηθεί προς τον σκοπό αυτό.

Σχετικά με τις διαβιβάσεις δεδομένων σε τρίτες χώρες

Το ΔΕΕ έκρινε ότι οι τυποποιημένες συμβατικές ρήτρες 2010/87 (στο εξής ΤΣΡ) για τη διαβίβαση προσωπικών δεδομένων σε εκτελούντες την

επεξεργασία εγκατεστημένους εκτός ΕΕ (Απόφαση της Επιτροπής 2010/87) παραμένουν ισχυρές και για τη διαβίβαση προσωπικών δεδομένων στις ΗΠΑ, υπό συγκεκριμένες προϋποθέσεις. Ειδικότερα, πριν από οποιαδήποτε διαβίβαση με βάση τις ΤΣΡ, ο εξαγωγέας –με τη βοήθεια του εισαγωγέα των δεδομένων– πρέπει να εξετάζει εάν το επίπεδο προστασίας των δεδομένων το οποίο κατοχυρώνει ο ΓΚΠΔ, εξασφαλίζεται στην εκάστοτε τρίτη χώρα, λαμβάνοντας υπόψη τις συνθήκες της συγκεκριμένης διαβίβασης και πρόσθετα μέτρα που μπορεί αυτός να λάβει. Σε περίπτωση δε που καταλήξει στο συμπέρασμα ότι δεν παρέχεται επαρκές επίπεδο προστασίας, ο εξαγωγέας πρέπει να αναστείλει τη διαβίβαση ή/και να καταγγείλει τη σύμβαση με τον εισαγωγέα.

Πηγή: **http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm**, European Commision, Frequently Asked Questions: New EU rules to obtain electronic evidence

ΣΥΜΠΕΡΑΣΜΑΤΑ

Κλείνοντας με την παρούσα διπλωματική εργασία συμπεραίνεται ότι οι διασυνοριακές ροές ψηφιακών δεδομένων αυξάνονται, με τον ίδιο φρενήρη ρυθμό, με τον οποίο αυξάνεται μεταξύ άλλων και η χρήση των κοινωνικών δικτύων, των υπηρεσιών ηλεκτρονικού ταχυδρομείου, των υπηρεσιών διαδικτυακής επικοινωνίας, των υπηρεσιών αποθήκευσης δεδομένων. Όπως είναι προφανές αλλά και απολύτως λογικό και ευκταίο είναι η εξάλειψη του εγκλήματος στον χώρο του Διαδικτύου, στη λεγόμενη κοινωνία της Διακινδύνευσης.

Ο στόχος αυτός, εντούτοις δεν θα πρέπει να επιδιώκεται με κάθε κόστος αλλά θα πρέπει φυσικά να λαμβάνεται σοβαρά υπόψιν η προστασία της ιδιωτικής ζωής, των δικαιωμάτων του ανθρώπου καθώς και η προστασία των κάθε είδους, ευαίσθητων και μη, προσωπικών δεδομένων. Τα νομοθετικά μέτρα, επίσης, που θα ληφθούν στο μέλλον θα πρέπει να λαμβάνουν σοβαρά υπόψιν τους τις αρχές της νομιμότητας, της αναγκαιότητας, της αναλογικότητας, που αποτελούν και τον ακρογωνιαίο λίθο της Ευρωπαϊκής Νομοθεσίας.

Όπως είναι λογικό, όταν οι πολίτες των κρατών βλέπουν τους ηγέτες να λαμβάνουν μέτρα για την προστασία των συνταγματικά κατοχυρωμένων δικαιωμάτων τους, όπως εν προκειμένω η πρόταση Κανονισμού, ενώ παράλληλα προστρέχουν για την πάταξη κάθε είδους εγκληματικής ενέργειας στον Κυβερνοχώρο, ένα είναι σίγουρο, ότι εδραιώνεται μέσα τους το κοινό περί δικαίου αίσθημα καθώς και η εμπιστοσύνη τους στο κράτος δικαίου. Στόχος είναι η λήψη ενιαίων μέτρων σε παγκόσμια κλίμακα, που θα δημιουργήσει ομοιομορφία στα δίκαια των κρατών ανά τον κόσμο, κάτι που αναμένεται να δημιουργήσει ασφάλεια δικαίου και να ενισχύσει φυσικά την οικουμενική διασυνοριακή συνεργασία των κρατών.

Σε υπερεθνικό επίπεδο λοιπόν όλες αυτές οι πρωτοβουλίες που αναφέρθηκαν επιδιώκουν πράγματι να ανταποκριθούν στην αυξανόμενη ψηφιοποίηση των πληροφοριών, στον ρόλο τρίτων παρόχων στον έλεγχο αυτών των πληροφοριών και στο γεγονός ότι οι πάροχοι και τα δεδομένα ενδιαφέροντος διατηρούνται ολοένα και περισσότερο εκτός συνόρων. Αυτές οι αλλαγές παρέχουν τόσο ευκαιρίες όσο και προκλήσεις. Κατά την ανάκτηση δεδομένων και αποδεικτικών στοιχείων σε διεθνές, υπερεθνικό επίπεδο, σαφώς διακυβεύονται κυριαρχικά συμφέροντα επιβολής και ενυπάρχουν σημαντικές προκλήσεις. Τόσο η "CLOUD ACT" των ΗΠΑ όσο και η Ευρωπαϊκή πρόταση "E - Evidence", αποτελούν σημαντική συνεισφορά σε αυτές τις προσπάθειες – μια συνεισφορά που μπορεί και πρέπει να οικοδομηθεί μέσω της σύναψης ισχυρών διμερών συμφωνιών που προστατεύουν και προάγουν την ιδιωτική ζωή και τις πολιτικές ελευθερίες.

Στόχος τέτοιων συμφωνιών θα πρέπει να είναι η διευκόλυνση της νόμιμη και ταχείας διασυνοριακής πρόσβασης σε δεδομένα μέσω ρητά καθορισμένων διαδικασιών, που παράλληλα προστατεύουν τα υποκείμενα και προωθούν την ασφάλεια σε παγκόσμιο επίπεδο. Έτσι,

δεν πρέπει να λησμονείται ότι με όλες αυτές τις διασυνοριακές προτάσεις, που αποσκοπούν στην υποβοήθηση της διαδικασίας επιβολής του νόμου σε διεθνές επίπεδο, θα πρέπει να διασφαλίζονται πρωτίστως με καθιέρωση ειδικών δικλείδων ασφαλείας και τα δικαιώματα των υποκειμένων, που θα έλεγε κανείς ότι έως σήμερα αφήνονται "εκτεθειμένα" και αποτελούν το μεγαλύτερο "κενό" που διαπιστώνεται στις υφιστάμενες νομοθετικές προσπάθειες.

ΒΙΒΛΙΟΓΡΑΦΙΑ

i) Ελληνική βιβλιογραφία

Α Γραμματικάκη-Αλεξίου, Ηλεκτρονικό εμπόριο, ιδιωτικό διεθνές δίκαιο, διεθνές ομοιόμορφο δίκαιο και κοινοτικές ρυθμιστικές προσπάθειες- Μια συγκριτική επισκόπηση, ΕΕΕυρΔ 2001,σ.135

Αντώνης Βγόντζας, Δικαστική συνεργασία ΕΕ και ΗΠΑ – Μια νέα προοπτική στην καταπολέμηση του εγκλήματος ή μία ήττα του κράτους δικαίου, ΠοινΔικ 2003, σελ. 743.

Διονύσιος Δ. Σπινέλλης, Η δικαστική συνεργασία σε ποινικές υποθέσεις στην Ευρώπη και ειδικότερα η ευρωπαϊκή εντολή έρευνας, Ιανουάριος 2016

Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, έκδοση 2018, σελ.353

Ι.Ιγγλεζάκη, Η ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα (EU-U.S Privacy Shield), Συνήγορος 113/2016, σελ.68 επ

Ι.Ιγγλεζάκη, Προστασία της ιδιωτικής ζωής. Η ακύρωση της απόφασης 200/520 της Επιτροπής της ΕΕ σχετικά με τις αρχές ασφαλούς λιμένα (Safe Harbour). Με αφορμή την απόφαση του ΔΕΕ στην υπόθεση C-362/14(Maximillian Schremms vs Data Protection Commissioner), Συνήγορος 111/2015, σελ.70

Ιωάννης Δημ. Ιγγλεζάκης, Δίκαιο Πληροφορικής, Γ΄έκδοση, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη

Μ.Καϊάφα –Γκμπράντι και Ε.Συμεωνίδου Καστανίδου, σελ. 55- 56

Κ. Βλαχόπουλος, «Ηλεκτρονικό Έγκλημα», 2007, εκδ. Νομική Βιβλιοθήκη, σελ. 137

Κωνσταντίνος Ζουμπουλάκης «Η πρόσβαση των αρχών στα ηλεκτρονικά αποδεικτικά στοιχεία: Τι συμβαίνει με τα προσωπικά μας δεδομένα;», 19 Ιουνίου 2019 https://www.homodigitalis.gr/posts/3928

Παναγιώτης Δ. Αρμαμέντος και Βασίλης Α.Σωτηρόπουλος, «Προσωπικά δεδομένα, Ερμηνεία κατ' άρθρο, Οι τροποποιήσεις του Ν.2472/1997 απ' τους Ν.3471/2006 και 3625/2007», Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη

Στ. Δασκαλόπουλου, Η Ευρωπαϊκή Εντολή Έρευνας (Ε.Ε.Ε.): Ο νέος θεσμός Δικαστικής Συνεργασίας επί ποινικών υποθέσεων εντός της Ευρωπαϊκής Ένωσης, ΠοινΧρ 2018, σελ. 173.

Χρυσικός Δημοσθένης, Η Συμφωνία Εκδόσεως μεταξύ Ευρωπαϊκής Ένωσης και ΗΠΑ – Σκέψεις και προβληματισμοί για ένα ζήτημα που δεν συζητήθηκε όσο θα έπρεπε, ΠοινΔικ 2003, σελ. 757

ii) Ελληνικά Νομοθετικά Κείμενα

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» (ΕΕL 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.

Απόφαση 2000/520/ΕΚ της Ευρωπαϊκής Επιτροπής «σχετικά με επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ»,ΕΕL 115/14.

Άρθρο 4 παρ. 8 Ν. 3649/2008114

Άρθρο 2 παρ. 3 του Π.Δ. 325/2003115

Άρθρο 1 παρ.1 Ο περί της Ευρωπαϊκής Εντολής Έρευνας σε Ποινικές Υποθέσεις Νόμος του 2017 (181(Ι)/2017)

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

Κανονισμός του Ευρωπαϊκού κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή

διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις (SWD(2018) 118 final και SWD(2018) 119 final, https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52018PC0225 και αιτιολογικές σκέψεις (31-46)

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 Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης –πλαισίου 2005/22/ΔΕΥ του Συμβουλίου, ρυθμίσεις Σωφρονιστικής και εγκληματικής πολιτικής και άλλες διατάξεις.

Οδηγία 2011/92/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και 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 17.2.2011

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

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 της 4.5.2016, σ. 89)

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 για την τροποποίηση της απόφασης 2005/671/ΔΕΥ του Συμβουλίου, ΕΕ L 88/6 της 31.3.2017

iii) Ξενόγλωσση βιβλιογραφία

A proposed electronic evidence exchange across the European Union By Maria Angela Biasiotti

Bachmaier Winter L., Transnational Evidence, σελ. 51.

Cybertime 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)

Daskal Jennifer and P. Swire, "A Possible EU-US Agreement on Law Enforcement Access to Data?", Lawfare, 2018

Daskal Jennifer, "Unpacking the CLOUD Act", 2018

Mitrakas, A.,Zaitch, D., "Law, Cybercrime and digital forensics: Trailling Digital Suspects", Kanellis P., Kiountouzis, E., Kolokontronis N.Drakoulis, M.(Eds), Digital Crime and Forensic Science in Cyberspace, London 2006, pp. 267-290 και Maria Karyda, Lilian Mitrou, "Internet Forensics: Legal and

Technical issues", University of the Aegean, Deparntment of Information and Communication Systems Engineering, Karlovassi, Samos

Nykodym N., Taylor, R.,Vilela, J., "Criminal Profiling and Insider cyber crime", Digital Investigation, Vol. 2 issue 4, 2005, pp. 261-265 και Maria Karyda, Lilian Mitrou, "Internet Forensics: Legal and Technical issues", University of the Aegean, Department of Information and Communication Systems Engineering, Karlovassi, Samos

Philippe Jougleux, Lilian Mitrou, Tatiana-Eleni Synodinou , The Legal Regulation of Cyber Attacks, Edited by Ioannis Iglezakis

Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, 2017

iv) Ξενόγλωσση αρθρογραφία

Explanatory Report to the Convention on Cybertime, σελ. 50

v) Ηλεκτρονικές πηγές

http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm [Ημ/νια πρόσβασης 3/4/2022]

https://eur-ltex.europa.eu/legal-content/el/TXT/?uri=CELEX:52002DC0045 [Ημ/νια πρόσβασης 1/4/2022]

https://eur-lex.europa.eu/ [Ημ/νια πρόσβασης 3/5/2022]

https://ejustice.europa.eu/92/EL/european_investigation_order_mutual_legal_assistance_and_joint_investigation_teams [Ημ/νια πρόσβασης 5/5/2022]

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_el.pdf. [Ημ/νια πρόσβασης 1/3/2022]

https://ccdcoe.org/transborder-data-access-quo-vadis-council-europe.html [Ημ/νια πρόσβασης 2/2/2022]

Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018) https://www.congress.gov/bill/115th-congress/housebill/4943/text [Ημ/νια πρόσβασης 4/10/22]