ΠΑΝΕΠΙΣΤΗΜΙΟ
ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ
ΕΦΑΡΜΟΣΜΕΝΗΣ
ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ
ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΕΡΕΥΝΑ ΚΑΙ ΚΑΤΑΣΧΕΣΗ ΑΠΟΘΗΚΕΥΜΕΝΩΝ ΔΕΔΟΜΕΝΩΝ ΥΠΟΛΟΓΙΣΤΗ

Διπλωματική Εργασία
της

Ειρήνης Πρ. Παντζαρτζή

Θεσσαλονίκη, 10.02.2024

ΕΡΕΥΝΑ ΚΑΙ ΚΑΤΑΣΧΕΣΗ ΑΠΟΘΗΚΕΥΜΕΝΩΝ ΔΕΔΟΜΕΝΩΝ ΥΠΟΛΟΓΙΣΤΗ

Ειρήνη Παντζαρτζή

Πτυχίο Νομικής Σχολής Δ.Π.Θ.

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ
ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής:
Κ. Θεοχάρης Ι. Δαλακούρας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή τη 01.03.2024

κος. Θεοχάρης Ι. Δαλακούρας	κος. Αποστολίδης Νικόλαος	Κος. Σαββίδης Νικόλαος
.....	.....	.....

Ειρήνη Πρ. Παντζαρτζή

Περίληψη

Σκοπός της παρούσας διπλωματικής εργασίας είναι η μελέτη, ανάλυση και η παρουσίαση της επίδρασης της ψηφιακής επανάστασης στον τομέα του ποινικού δικαίου και συγκεκριμένα στο δεύτερο και τρίτο κεφάλαιο του δεύτερου τμήματος του Κώδικα Ποινικής Δικονομίας, αφορώντων στις ανακριτικές πράξεις της έρευνας (αρ. 253 και 254 ΚΠΔ) και κατασχέσεως (αρ. 265 ΚΠΔ), με ιδιαίτερη έμφαση στη νέα διάταξη του άρθρου 265 ΚΠΔ, που τιτλοφορείται «Κατάσχεση Ψηφιακών Δεδομένων». Μέσω της παρούσας διπλωματικής εργασίας θα επιχειρηθεί η παρουσίαση του ιστορικού υποβάθρου του άρθρου 265 ΚΠΔ, οι ενωσιακές αξιώσεις και προτροπές που οδήγησαν στην ενσωμάτωση της διάταξης αυτής στην ελληνική έννομη τάξη, η πλήρης ανάλυση του ως άνω άρθρου όπως ισχύει σήμερα, τα δικονομικά κενά και η κάλυψη αυτών, το χρονικό όριο εφαρμογής της διάταξης και η εφαρμογή των διατάξεων του διαχρονικού δικαίου, καθώς και αρχές που πρέπει να τηρούνται και να προστατεύονται κατά την εφαρμογή της ως άνω διατάξεως, όπως και οι προκλήσεις και επιδιορθώσεις που ενδέχεται να χωρούν επ' αυτού στις μετέπειτα τροποποιήσεις του οικείου Κώδικα Ποινικής Δικονομίας, στον οποίο η διάταξη αυτή εμπεριέχεται και κατοχυρώνεται.

Λέξεις Κλειδιά: ψηφιακά δεδομένα, έρευνα, κατάσχεση, αποθήκευση, ανακριτικές αρχές, σύστημα υπολογιστή, δεδομένα υπολογιστή, απομακρυσμένο σύστημα υπολογιστή, πληροφοριακό σύστημα.

Abstract:
The main purpose of this thesis is to study, analyze and present the impact of the digital revolution in the field of criminal law, specifically in the second and third Chapters of the second Section of the Code of Criminal Procedure (Greece), relating to investigative acts of investigation (no. 253 and 254 CCP) and seizure of stored digital data (no. 265 CCP), with special emphasis on the new provision of article 265 CCP, entitled "Seizure of Stored Digital Data". Dia this thesis, emphasis will be given to the historical background of article 265 CCP, the EU claims and prompts that led to the incorporation of the provision of Article 265 CCP into the Greek legal order, the analysis of the article 265 CCP as it applies today, the procedural gaps and the their coverage, matters of temporal scope, the principles which must be observed and protected during the application of the above Article 265 CCP, as well as the challenges and amendments of the Code of Criminal Procedure that may be required.

Keywords: digital data, search, seizure, storage, investigative authorities, computer system, computer data, remote computer system, information system

Περιεχόμενα

Συμβολισμοί:

ΠΚ – Ποινικός Κώδικας
ΚΠΔ – Κώδικας Ποινικής Δικονομίας
Αρ. - Άρθρο
Παρ. - Παράγραφος
Στ. - Στοιχείο
Εδ. - Εδάφιο
ΑΠ – Άρειος Πάγος
Ν. / ν. – Νόμος
ΕΔΔΑ – Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου
ΔΕΕ – Δικαστήριο Ευρωπαϊκής Ένωσης

1.Εισαγωγή

1.1 Σημαντικότητα του θέματος

Διανύοντας την εποχή της ψηφιακής επανάστασης[1] σε κάθε πτυχή και έκφανση της ανθρώπινης δραστηριότητας, είναι αυτονόητο, πως τα αποτελέσματα μιας τέτοιας εξέλιξης και μεταβολής στον τρόπο διαβίωσης και δραστηριοποίησης του κοινωνικού συνόλου, δεν θα άφηναν ανεπηρέαστο τον τομέα της ποινικής δικαιοσύνης, και συγκεκριμένα τον τρόπο τέλεσης των διαφόρων εγκλημάτων, όπως αυτά τυποποιούνται στον οικείο Ποινικό Κώδικα, αλλά και την διαδικασία συλλογής των πειστηρίων του εγκλήματος, και όλων των εν γένει διαδικασιών από την προδικασία, την άσκηση της ποινικής διώξεως, μέχρι και της εκδόσεως αμετάκλητης αποφάσεως. Στο όχι και τόσο μακρινό μέλλον, κανείς δεν θα θυμάται ότι κάποτε ο ψηφιακός κόσμος αντιδιαστελλόταν προς τον «πραγματικό» κόσμο, όχι μόνο γιατί η ανθρώπινη εμπειρία μεταφέρεται σταδιακά στο ψηφιακό επίπεδο, όπου διάγεται μεγάλο μέρος της καθημερινότητας, αλλά και επειδή σχεδόν κάθε βήμα στον αναλογικό κόσμο αφήνει ανεξίτηλο ψηφιακό αποτύπωμα. Κάθε έκφανση του οικογενειακού, κοινωνικού και επαγγελματικού βίου είναι αναπόσπαστα δεμένη με τεχνολογικές εφαρμογές, με ολοένα αυξανόμενο βαθμό εξάρτησης.[2]

Η ψηφιοποίηση της της σύγχρονης εποχής, απαντάται στο σύνολο των δραστηριοτήτων της καθημερινότητας του ατόμου, το οποίο αφήνει το ψηφιακό του αποτύπωμα, μεταξύ άλλων, μέσω των ηλεκτρονικών συναλλαγών που εκτελεί, μέσω της χρήσης του παγκοσμίου συστήματος στιγματοθέτησης (GPS - Global Positioning System), μέσω των αναζητήσεων που πραγματοποιεί στον χώρο του διαδικτύου, και οι οποίες αναζητήσεις μπορούν να διαμορφώσουν το «προφίλ» του εκτελούντος αυτές αλλά και να φανερώσουν τις ανησυχίες και τα ενδιαφέροντα που το εκάστοτε άτομο παρουσιάζει ανά χρονικές στιγμές και περιόδους. Τα ως

[1] Με τον όρο **Ψηφιακή Επανάσταση** εννοούμε τη μετάβαση από την αναλογική-μηχανική ηλεκτρική τεχνολογία στην ψηφιακή τεχνολογία. Η ψηφιακή επανάσταση ξεκίνησε το 1980 και συνεχίζεται μέχρι και σήμερα. Εμμέσως, ο όρος αυτός αναφέρεται επίσης στις σαρωτικές αλλαγές τις οποίες επέφερε η πληροφορική και η τεχνολογία των επικοινωνιών κατά τη διάρκεια του δεύτερου μισού του 20ου αιώνα.

[2] Γιάννης Ναζίρης, Επίκουρος Καθηγητής ΑΠΘ, Δικηγόρος, ΠοινΔικ, [Νομική Βιβλιοθήκη], ISSN:1108-2755, τομ.24 τευχ.247 [2021] σελ.178-194

άνω μπορούν να επιτευχθούν, μέσω των επικοινωνιών που πραγματοποιεί το άτομο, είτε τηλεφωνικά δια της ομιλίας μέσω της χρήσεως του κινητού τηλεφώνου, είτε γραπτά, με την αποστολή μηνυμάτων (στα οποία συμπεριλαμβάνονται και τα ηχητικά μηνύματα), δια της χρήσεως των υπηρεσιών των μέσων κοινωνικής δικτύωσης, των γραπτών μηνυμάτων των υπηρεσιών κινητής τηλεφωνίας, ή της αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου (email).

Είναι λοιπόν προδήλως φανερό, πως η ως άνω σύγχρονη πραγματικότητα και η δημιουργία των προαναφερθέντων ψηφιακών αποτυπωμάτων, δεν θα άφηναν ανεπηρέαστο τον τομέα του ποινικού δικαίου, τόσο από πλευράς εμφάνισης νέων τρόπων τέλεσης των ήδη προβλεπομένων στον ισχύοντα ποινικό κώδικα εγκλημάτων ή και διάπραξη νέων εγκλημάτων που δεν προβλεπόταν πριν την ψηφιακή επανάσταση, λόγω της έλλειψης των τεχνικών μέσων, όσο και από πλευράς συλλογής αποδεικτικών μέσων και πειστηρίων για την κατάφαση ή μη της τέλεσης αδικημάτων, και όλα αυτά υπό το πρίσμα της αρχής της αναγκαιότητας σκοπού, της αρχής της αναλογικότητας, καθώς και της προστασίας των προσωπικών δεδομένων του υπόπτου ή του κατηγορουμένου και της αρχής της μη αυτοενοχοποίησης αυτού.

Ως «κυβερνοέγκλημα» ή «έγκλημα στον κυβερνοχώρο» νοούνται οι «αξιόποινες πράξεις που διαπράττονται με χρήση ηλεκτρονικών δικτύων επικοινωνιών και συστημάτων πληροφοριών ή οι αξιόποινες πράξεις εναντίον αυτών των δικτύων και συστημάτων»[3]. Στο πεδίο των κυβερνοεγκλημάτων, ιδίως των stricto sensu κυβερνοεγκλημάτων, ήτοι των αξιόποινων πράξεων που στρέφονται αμιγώς εναντίον ηλεκτρονικών δικτύων επικοινωνιών και πληροφοριακών συστημάτων, καθώς και των αξιόποινων πράξεων που διαπράττονται μέσω αυτών, η αναζήτηση και η ανάκτηση των ψηφιακών δεδομένων αποτελεί μείζον ζήτημα. Ο άυλός χαρακτήρας των ψηφιακών δεδομένων θέτει πλήθος ζητημάτων τόσο στον νομοθέτη όσο και στον εφαρμοστή του δικαίου για τη διερεύνηση των κυβερνοεγκλημάτων.[4] Η ιδιαιτερότητα των ως άνω δεδομένων, η οποία πηγάζει ευθέως από την άυλη φύση τους, καθιστά τη διαδικασία συλλογής αποδείξεων, στις περιπτώσεις τέλεσης κυβερνοεγκλημάτων, εξεζητημένη,

[3] Βλ. Επιτροπή των Ε.Κ., προς την κατεύθυνση γενικής πολιτικής σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο COM (2007) 267 τελικό, Βρυξέλλες 22.5.2007, σελ. 2

[4] Αλέξανδρος Ι Καργιόπουλος, Ηλεκτρονικό Έγκλημα, Θεοχάρης Ι Δαλακούρας, Εκδ. Νομική Βιβλιοθήκη, κεφ. 12- Ανακριτικές πράξεις επί ψηφιακών δεδομένων: Δικαιικοί άξονες και προβληματισμοί, σελ. 201

καθώς το σύνολο αυτών (των αποδείξεων) θα αναζητηθεί στον ψηφιακό και διαδικτυακό χώρο, από τον οποίο και θα πρέπει να ανακτηθούν.

Τα ως άνω κατέδειξαν στον νομοθέτη και στον εφαρμοστή του δικαίου την επιτακτικότητα της ανάγκης για αναθεώρηση και «εκσυγχρονισμό» των ήδη προβλεπόμενων και υφιστάμενων ανακριτικών πράξεων, μεταξύ των οποίων και της ανακριτικής πράξεως της κατάσχεσης στην περίπτωση συνδρομής άυλων πειστηρίων εγκλήματος, ακολουθώντας μια νεωτεριστική οπτική και προοπτική.

Σκοπός της παρούσας διπλωματικής εργασίας είναι η μελέτη, ανάλυση και η παρουσίαση της επίδρασης της ψηφιακής επανάστασης στον τομέα του ποινικού δικαίου και συγκεκριμένα στο δεύτερο και τρίτο κεφάλαιο του δεύτερου τμήματος του Κώδικα Ποινικής Δικονομίας, αφορώντων στις ανακριτικές πράξεις της έρευνας (αρ. 253 και 254 ΚΠΔ) και κατασχέσεως (αρ. 265 ΚΠΔ), με ιδιαίτερη έμφαση στη νέα διάταξη του άρθρου 265 ΚΠΔ, που τιτλοφορείται «Κατάσχεση Ψηφιακών Δεδομένων». Μέσω της παρούσας διπλωματικής εργασίας θα επιχειρηθεί η παρουσίαση του ιστορικού υποβάθρου του άρθρου 265 ΚΠΔ, οι ενωσιακές αξιώσεις και προτροπές που οδήγησαν στην ενσωμάτωση της διάταξης αυτής στην ελληνική έννομη τάξη, η πλήρης ανάλυση του ως άνω άρθρου όπως ισχύει σήμερα, τα δικονομικά κενά και η κάλυψη αυτών, το χρονικό όριο εφαρμογής της διάταξης και η εφαρμογή των διατάξεων του διαχρονικού δικαίου, καθώς και αρχές που πρέπει να τηρούνται και να προστατεύονται κατά την εφαρμογή της ως άνω διατάξεως, όπως και οι προκλήσεις και επιδιορθώσεις που ενδέχεται να χωρούν επ’ αυτού στις μετέπειτα τροποποιήσεις του οικείου Κώδικα Ποινικής Δικονομίας, στον οποίο η διάταξη αυτή εμπεριέχεται και κατοχυρώνεται.

1.2 Ιστορικό υπόβαθρο της διατάξεως του άρθρου 265 ΚΠΔ

Η ως άνω συλλογιστική, ήτοι η διαπίστωση πως, η ραγδαία τεχνολογική πρόοδος και εξέλιξη της σύγχρονης εποχής, οδήγησε προοδευτικά στον εντοπισμό της ύπαρξης νομοθετικού κενού, μεταξύ άλλων, και στον τομέα των προβλεπόμενων ανακριτικών πράξεων. Τούτο αποτέλεσε σημείο αναφοράς κατά την τροποποίηση του Κώδικα Ποινικής Δικονομίας που επήλθε με τον Ν. 4620/2019, ΦΕΚ Α’ 96/11-6-2019, που

τέθηκε σε ισχύ τη 01-07-2019, και ο οποίος εισήγαγε για πρώτη φορά στην ελληνική έννομη τάξη τη διάταξη του άρθρου 265 ΚΠΔ, όπως ισχύει μέχρι σήμερα, αφορώσα στην «Κατάσχεση Ψηφιακών Δεδομένων».

Δέον να σημειωθεί πως μέχρι του χρονικού αυτού σημείου θέσης σε εφαρμογή του ως άνω νόμου, ουδεμία ρητή και ειδική πρόβλεψη ανάμεσα στις ανακριτικές πράξεις υπήρχε, για την έρευνα και κατάσχεση ψηφιακών δεδομένων, παρά οι Αρχές κατέφευγαν σε αναλογική εφαρμογή των διατάξεων για την έρευνα και κατάσχεση υλικών αντικειμένων και εγγράφων, των άρθρων του δεύτερου και τρίτου Κεφαλαίου του δεύτερου τμήματος του Κώδικα Ποινικής Δικονομίας, ήτοι των άρθρων 253 επόμενα του ως άνω κώδικα.

Ρητά στην αιτιολογική έκθεση του ως άνω Νόμου 4620/2019, ΦΕΚ Α' 96/11-6-2019, αναφέρθηκε πως η ενσωμάτωση της προκειμένης ρύθμισης στο τρίτο κεφάλαιο του δεύτερου τμήματος του Κώδικα Ποινικής Δικονομίας, ήτοι στο κεφάλαιο αφορών στις διατάξεις της ανακριτικής πράξεως της Κατασχέσεως, καταγράφεται ως επιβεβλημένη νομοθετική κίνηση για την κάλυψη συγκεκριμένου κενού, συνάμα όμως και ως νεωτεριστική αποτύπωση επενέργειας της σύγχρονης τεχνολογικής εξέλιξης στην ποινική δίκη.[5]

Μάλιστα, η θέσπιση του ως άνω κανονιστικού πλαισίου και η ενσωμάτωσή του στην ελληνική έννομη τάξη, αποτέλεσε μεταξύ άλλων υλοποίηση της προτροπής για νομοθετική ρύθμιση, απορρέουσα τόσο από την Οδηγία 2016/680/ΕΕ, αναφορικά με 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, όσο και από τη Σύμβαση του Συμβουλίου της Ευρώπης, γνωστή και ως Σύμβαση της Βουδαπέστης, αναφορικά με το κυβερνοέγγλημα η οποία υπογράφηκε στη Βουδαπέστη στις 23.11.2001 και κυρώθηκε στην ελληνική έννομη τάξη με το Ν. 4411/2016, αλλά και από τη σύγχρονη νομολογία του ΕΔΔΑ. Ως σκοπός της ως άνω Συμβάσεως δε αναφέρεται η προστασία της κοινωνίας από το έγκλημα στον Κυβερνοχώρο με την θέσπιση της κατάλληλης νομοθεσίας που είναι απαραίτητη για την έρευνα,

[5] Αιτιολογική έκθεση, Σχέδιο Νόμου με τίτλο «Κύρωση του Κώδικα Ποινικής Δικονομίας», Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων, Αθήνα, 03-05-2019, σελ. 82-83

τη δίωξη και την εκδίκαση των εγκλημάτων του κυβερνοχώρου καθώς και των εγκλημάτων που διαπράττονται με τη χρήση συστημάτων ηλεκτρονικών υπολογιστών.[6]

Ειδικότερα με το άρθρο πρώτο του Ν. 4411/2016 (ΦΕΚ Α' 142/3-8-2016) κυρώθηκε, έχοντας αυξημένη τυπική ισχύ, κατά το άρθρο 28 παρ. 1 του Συντάγματος, και ενσωματώθηκε στην ελληνική έννομη τάξη , η υπ' αριθμόν 185/23-11-2001 Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο.[7] Συγκεκριμένα από τη διάταξη της πρώτης παραγράφου του άρθρου 19 της ως άνω Συμβάσεως, αφορώσα στην «Έρευνα και Κατάσχεση αποθηκευμένων δεδομένων υπολογιστή», ρητά ορίστηκε πως, «*1. Κάθε Συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να δοθεί η δυνατότητα στις αρμόδιες αρχές του να ερευνούν ή ομοίως να έχουν πρόσβαση: α. σε ένα σύστημα υπολογιστή ή σε μέρος αυτού και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτόν, και β. σε ένα μέσο αποθήκευσης δεδομένων υπολογιστή στο οποίο υπάρχουν αποθηκευμένα δεδομένα υπολογιστή μέσα στην επικράτειά του*». Την ως άνω μάλιστα διάταξη νόμου ο Έλληνας νομοθέτης ενσωμάτωσε δια του Ν. 4416/2016, χωρίς να διατηρήσει ως είχε δικαίωμα από το άρθρο 42 της Συμβάσεως της Βουδαπέστης, οποιαδήποτε επιφύλαξη υπέρ του εκδοθησόμενου νόμου.[8]

Στην αιτιολογική έκθεση κύρωσης της ως άνω Συμβάσεως στην ελληνική έννομη τάξη, ρητά παρουσιάζεται η αιτιολογική βάση που κατέδειξε την ανάγκη αναθεωρήσεως, μεταξύ άλλων και των υφιστάμενων διατάξεων του Κώδικα Ποινικής Δικονομίας που αφορούν στις ανακριτικές πράξεις. Συγκεκριμένα όπως εκτέθηκε, η ραγδαία ανάπτυξη της χρήσης του Διαδικτύου (Internet), η ψηφιοποίηση, η σύγκλιση κι η εκτεταμένη διασύνδεση των συστημάτων πληροφοριών, παρέχουν σημαντική διευκόλυνση στη διάπραξη ποινικών αδικημάτων

[6] Θεοχάρης Ι Δαλακούρας, Καθηγητής Νομικής Σχολής ΔΠΘ, Δικηγόρος, «Ουσιαστικές και δικονομικές διατάξεις της σύμβασης του συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν. 4411/2016)», Ηλεκτρονικό έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Νομική Βιβλιοθήκη, εκδ. 2023, επιμέλεια Θεοχάρης Ι Δαλακούρας, σελ. 3.

[7] Μαριάννα Κουδελή, Στρατιωτικός Δικαστής, Ζητήματα που άπτονται της κατάσχεσης ψηφιακών δεδομένων του άρθρου 265 του ΚΠΔ, Ηλεκτρονικό έγκλημα, επιμέλεια Θεοχάρης Ι Δαλακούρας, εκδ. Νομική Βιβλιοθήκη σελ. 525.

[8] Μαριάννα Κουδελή, Στρατιωτικός Δικαστής, Ζητήματα που άπτονται της κατάσχεσης ψηφιακών δεδομένων του άρθρου 265 του ΚΠΔ, Ηλεκτρονικό έγκλημα, επιμέλεια Θεοχάρης Ι Δαλακούρας, εκδ. Νομική Βιβλιοθήκη, σελ. 526.

διασυνοριακού χαρακτήρα.[9] Για τον λόγο αυτό, η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, η οποία ενσωματώθηκε στην ελληνική έννομη τάξη, αποτέλεσε ένα πρωτοποριακό κείμενο με το οποίο επιδιώχθηκε η θέσπιση κανόνων δικαίου, με σκοπό την αντιμετώπιση της εγκληματικότητας στο διαδίκτυο (Internet), αποβλέποντας μεταξύ άλλων στη συμπλήρωση των δικονομικών διατάξεων, που ισχύουν στα συμβαλλόμενα μέρη, μεταξύ των οποίων και της ελληνικής έννομης τάξης, προκειμένου να βελτιωθεί η δυνατότητα των Δικαστικών και Αστυνομικών Αρχών να διεξάγουν τις έρευνές τους «σε πραγματικό χρόνο» ("in real time"), ώστε να συλλέγουν τα απαραίτητα αποδεικτικά στοιχεία, στα γεωγραφικά όρια της εκάστοτε εθνικής επικράτειας, πριν τα στοιχεία αυτά χαθούν.[10] Καταδειχθήκε λοιπόν η ανάγκη εκσυγχρονισμού των υφιστάμενων ανακριτικών πράξεων, προκειμένου με τις νέες δικονομικές προβλέψεις να καταστεί δυνατή η αποτελεσματική και ασφαλής συλλογή στοιχείων του εγκλήματος, πριν αυτά αλλοιωθούν ή διαγραφούν, πρακτικές οι οποίες έχουν στην πράξη διευκολυνθεί με την ραγδαία πρόοδο της τεχνολογικής ανάπτυξης.

Συνεπώς δια του δεύτερου τμήματος του δεύτερου κεφαλαίου της Σύμβασης, επιδιώχθηκε η ενίσχυση των δικονομικών δυνατοτήτων των συμβαλλομένων μερών, με τη θέσπιση διαδικασιών που είναι περισσότερο προσαρμοσμένες στις ιδιαιτερότητες που χαρακτηρίζουν τις ανακριτικές πράξεις που διενεργούνται σε περιπτώσεις των εγκλημάτων τα οποία τελούνται μέσω συστήματος υπολογιστών. Με βάση τον πλήρη σεβασμό των θεμελιωδών δικαιωμάτων του ανθρώπου, επιδιώχθηκε, με τις διατάξεις των άρθρων 14 έως και 21 της Σύμβασης, η βελτίωση των δυνατοτήτων των συμβαλλομένων μερών να διεξάγουν στα δίκτυα

[9] Αιτιολογική Έκθεση στο σχέδιο Νόμου, «Κύρωση της σύμβασης του συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο και του πρόσθετου πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω συστημάτων υπολογιστών – μεταφορά στο ελληνικό δίκαιο της οδηγίας 2013 / 40 / ΕΕ του ευρωπαϊκού κοινοβουλίου και του συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005 / 222 / ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις», Κεφάλαιο Α', Α. Εισαγωγή, σελ. 1.

[10] Αιτιολογική Έκθεση στο σχέδιο Νόμου, «Κύρωση της σύμβασης του συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο και του πρόσθετου πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω συστημάτων υπολογιστών – μεταφορά στο ελληνικό δίκαιο της οδηγίας 2013 / 40 / ΕΕ του ευρωπαϊκού κοινοβουλίου και του συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005 / 222 / ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις», Κεφάλαιο Α', Β. Η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, σελ. 3.

έρευνες σε πραγματικό χρόνο (“in real time”, “en temps reel”) ανεξαρτήτως του είδους των διαπραττομένων εγκλημάτων και να συλλέγουν τις αναγκαίες για την στοιχειοθέτησή τους ηλεκτρονικές αποδείξεις πριν αυτές χαθούν οριστικά.[11] Δίνεται δηλαδή πλέον η δικονομική δυνατότητα στις ανακριτικές αρχές να έχουν πρόσβαση στα ψηφιακά δεδομένα του υπόπτου ή του κατηγορουμένου προκειμένου να προβούν σε έρευνα, κατάσχεση και επεξεργασία αυτών, με απώτερο σκοπό να κάνουν χρήση των συγκεκριμένων ψηφιακών αποτυπωμάτων, ώστε να αποφανθούν επί της συνδρομής ή μη της ενοχής του υπόπτου ή του κατηγορουμένου.

Στη δε Οδηγία 2016/680/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και συγκεκριμένα στην παράγραφο υπ’ αριθμόν 26 αυτής, ορίζεται ότι αξιώνεται από τα κράτη μέλη, πως «*κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σύννομη, θεμιτή και διαφανής σε σχέση με τα φυσικά πρόσωπα τα οποία αφορά και να πραγματοποιείται μόνο για συγκεκριμένους σκοπούς που προβλέπονται από το νόμο*». Ενώ στις παραγράφους υπ’ αριθμόν 27 και 28 της ίδιας ως άνω Οδηγίας, ορίζεται πως, «*Για την πρόληψη, διερεύνηση και τη δίωξη ποινικών αδικημάτων, οι αρμόδιες αρχές πρέπει να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα που συλλέγονται στο πλαίσιο της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης συγκεκριμένων ποινικών αδικημάτων και πέραν του πλαισίου αυτού, ώστε να κατανοούν καλυτέρα τις εγκληματικές δραστηριότητες και να προβαίνουν σε συσχετισμούς μεταξύ διαφορετικών διαπιστωθέντων ποινικών αδικημάτων*». (αρ. 27 Οδηγίας 2016/680/ΕΕ). Επιπλέον, «*Για να τηρείται η ασφάλεια σε σχέση με την επεξεργασία και να αποτρέπεται η επεξεργασία κατά παραβίαση της παρούσας Οδηγίας, τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο ώστε να εξασφαλίζεται το ενδεδειγμένο επίπεδο ασφάλειας και εμπιστευτικότητας, μεταξύ άλλων, με την αποτροπή της μη εξουσιοδοτημένης πρόσβασης σε*

[11] Αιτιολογική Έκθεση στο σχέδιο Νόμου, «Κύρωση της σύμβασης του συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο και του πρόσθετου πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω συστημάτων υπολογιστών – μεταφορά στο ελληνικό δίκαιο της οδηγίας 2013 / 40 / ΕΕ του ευρωπαϊκού κοινοβουλίου και του συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005 / 222 / ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις», Κεφάλαιο Α’, Β. Η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, σελ. 6.

δεδομένα προσωπικού χαρακτήρα ή΄ τη χρήση τους και στον εξοπλισμό που χρησιμοποιείται για την επεξεργασία, λαμβανομένων υπόψη του επιπέδου της διαθέσιμης τεχνολογίας, του κόστους εφαρμογής σε σχέση με τους κινδύνους και τη φύση των δεδομένων προσωπικού χαρακτήρα που πρέπει να προστατευτούν». (αρ. 28 Οδηγίας 2016/680/ΕΕ).

Ο Έλληνας λοιπόν νομοθέτης, λαμβάνοντας υπόψιν τις προαναφερθείσες αξιώσεις, απορρέουσες, τόσο από την Οδηγία 2016/680/ΕΕ, όσο και από τη Σύμβαση του Συμβουλίου της Ευρώπης, αναφορικά με το κυβερνοέγγλημα, αλλά και από τη σύγχρονη νομολογία του ΕΔΔΑ, και κυρίως λαμβάνοντας υπόψιν την επιτακτική ανάγκη για εκσυγχρονισμό των προβλεπομένων ανακριτικών πράξεων, στοχεύοντας στην ορθότερη και ταχύτερη απονομή δικαιοσύνης, που ακολουθεί τους σύγχρονους ρυθμούς, οδηγήθηκε δια του Ν. 4620/2019, ΦΕΚ Α' 96/11-6-2019, ο οποίος τέθηκε σε ισχύ τη 01-07-2019, στην τροποποίηση του μέχρι τότε ισχύοντος Κώδικα Ποινικής Δικονομίας, και στην εισαγωγή για πρώτη φορά στην ελληνική έννομη τάξη τη διάταξη του άρθρου 265 ΚΠΔ, αφορώσα στην ανακριτική πράξη της «Κατάσχεση Ψηφιακών Δεδομένων».

2. Έρευνα επί ψηφιακών δεδομένων – «Ψηφιακή» Έρευνα

Κατόπιν των ανωτέρω, δέον να σημειωθεί πως αναφορικά με την ανακριτική πράξη της έρευνας επί αποδεικτικών μέσων που φέρουν ψηφιακή μορφή, δεν τέθηκε δυνάμει του ως άνω υπ' αριθμόν 4620/2019 νόμου και της συνακόλουθης τροποποίησης του Ποινικού Κώδικα ειδική διάταξη νόμου που να προβλέπει τα όσα πρέπει να τηρούνται σχετικά.

Συνεπώς, στις περιπτώσεις όπου ανακύπτει η ανάγκη διενέργειας έρευνας επί αποδεικτικών μέσων που φέρουν ψηφιακή μορφή, τεκμαίρεται πως θα προβούμε στην αναλογική εφαρμογή των διατάξεων που αφορούν στις προϋποθέσεις για τη διενέργεια έρευνας επί υλικών - ενσώματων αντικειμένων, ήτοι των διατάξεων των άρθρων 253 και 254 παρ.1 στ. δ' ΚΠΔ. Από τον συνδυασμό των ως άνω διατάξεων συνάγεται ότι, για τη διενέργεια έρευνας προς αναζήτηση ψηφιακών δεδομένων ή απλής ακόμα πρόσβασης στο σύνολο ή σε μέρος ενός πληροφοριακού συστήματος και στα ψηφιακά δεδομένα που είναι αποθηκευμένα σε αυτό, καθώς και σε ένα

μεμονωμένο μέσο αποθήκευσης ψηφιακών δεδομένων, απαιτείται: α) να διεξάγεται ανακριτική διαδικασία για κακούργημα ή πλημμέλημα (άρθρο 253 ΚΠΔ), β) το υπό έρευνα αρχικό πληροφοριακό σύστημα ή το πληροφοριακό σύστημα στο οποίο επεκτείνεται η έρευνα ή το μεμονωμένο μέσο αποθήκευσης να βρίσκεται στο έδαφος της ελληνικής επικράτειας, γ) να μπορεί βάσιμα να υποτεθεί η βεβαίωση του εγκλήματος, η αποκάλυψη ή η σύλληψη των δραστών ή τέλος η βεβαίωση ή αποκατάσταση της ζημίας που προκλήθηκε είναι δυνατόν να πραγματοποιηθεί ή να διευκολυνθεί μόνο με αυτήν (άρθρο 253 ΚΠΔ) και δ) να τηρηθούν οι εγγυήσεις και διαδικασίες των άρθρων 4 και 5 του Ν. 2225/1994 σε συνδυασμό με τις όμοιες του άρθρου 254 παρ. 2 έως 5 (άρθρο 254 παρ. 1 στ. δ, 2 ΚΠΔ)[12].

Με την ως άνω ερμηνευτική προσέγγιση, και με την εγγύηση της πλήρωσης όλων των ορισθέντων ως άνω προϋποθέσεων, δύναται να επιχειρείται, στα πλαίσια ανακριτικών πράξεων, νομότυπα η έρευνα επί δεδομένων που φέρουν ψηφιακό χαρακτήρα, και έτσι να καλύπτονται εμμέσως, από την ελληνική έννομη τάξη οι αξιώσεις που τίθενται δια μέσου του άρθρου 19 παρ. 1 και 2 της Σύμβασης της Βουδαπέστης αναφορικά με την πρόσβαση και έρευνα επί ψηφιακών δεδομένων και των άρθρων 14 και 15 αυτής (της Σύμβασης της Βουδαπέστης) αναφορικά με τους όρους και τις εγγυήσεις υπό τις οποίες αυτές δέον να λαμβάνουν χώρα. Στην περίπτωση δε που διαξαχθεί έρευνα χωρίς την τήρηση των ως άνω προϋποθέσεων και η κτήση ψηφιακών δεδομένων ως αποδεικτικό υλικό, τεκμαίρεται πως η χρήση του υλικού αυτού στα πλαίσια ποινικής διαδικασίας, συνιστά παρανόμως κτηθέν αποδεικτικό υλικό κατά παράβαση της αρχής της ηθικής απόδειξης του άρθρου 177 παρ. 2 ΚΠΔ που οδηγεί σε απόλυτη ακυρότητα της διαδικασίας.

Στη συνέχεια αναφορικά με τις ειδικές ανακριτικές πράξεις της συγκαλυμμένης έρευνας και της ανακριτικής διείσδυσης, όταν αφορά σε έρευνα επί ψηφιακών δεδομένων στην πράξη ακολουθείται η αναλογική εφαρμογή της διάταξης του άρθρου 254 ΚΠΔ. Η δράση των αρμοδίων διωκτικών Αρχών έχει ήδη αναπτύξει μεθόδους εξιχνίασης, σε επίπεδο πληροφοριών, που στηρίζονται σε συγκαλυμμένη έρευνα, δηλαδή στην

[12] Δημήτριος Γκύζης, Αντιεισαγγελέας Εφετών, κεφ. 17 «Ψηφιακή ανακριτική πράξη», Ηλεκτρονικό έγκλημα, επιμέλεια Θεοχάρης Ι Δαλακούρας, εκδ. Νομική Βιβλιοθήκη, σελ. 374.

περιήγηση αστυνομικών σε ανοιχτές πήγες διαδικτύου, με ψευδή στοιχεία αποκρύπτοντας την ιδιότητά τους. [13] Επί της πράξεως, οι αστυνομικές Αρχές προβαίνοντας στη δημιουργία ψεύτικων διαδικτυακών προφίλ στα οποία παραθέτουν στοιχεία που σε καμία περίπτωση δεν μαρτυρούν την ιδιότητά τους, προβαίνουν σε διενέργεια ερευνών σε μέσα κοινωνικής δικτύωσης, ιστοτόπους, ιστοσελίδες αλλά και σε εφαρμογές ηλεκτρονικής αλληλογραφίας, προκειμένου να διερευνήσουν τα ψηφιακά ίχνη δραστών αναφορικά με τις αξιόποινες πράξεις που ρητά και περιοριστικά τυποποιούνται στη διάταξη του άρθρου 254 παρ. 1 ΚΠΔ, ήτοι όταν προκύπτουν σοβαρές και βάσιμες υποψίες για την τέλεση, μέσω ψηφιακών μέσων των εγκλημάτων των αξιόποινων πράξεων «*των παρ. 1 και 2 του άρθρου 187, του άρθρου 187Α, των παρ. 1 και 2 του άρθρου 207, του πρώτου εδαφίου της παρ. 1 του άρθρου 208, του άρθρου 208Α εκτός από τις ιδιαίτερα ελαφρές περιπτώσεις, της παρ. 1 του άρθρου 209, των άρθρων 323Α, 336 σε βάρος ανηλίκου, 338 σε βάρος ανηλίκου, των παρ. 1 και 3 του άρθρου 339, της παρ. 1 του άρθρου 342, των άρθρων 348Α, 348Β, 348Γ και 351Α του Ποινικού Κώδικα»,* υπό την προϋπόθεση πως η ως άνω πρακτική (ψηφιακή έρευνα) κρίνεται ως απαραίτητη για την διευκόλυνση της διαλεύκανσης του εγκλήματος. Η συγκαλυμμένη αυτή η ψηφιακή έρευνα παρουσιάζει τα χαρακτηριστικά ειδικής ανακριτικής πράξης, ήτοι δεν έχει κατασταλτικό μόνο χαρακτήρα, αλλά υπό προϋποθέσεις και προληπτικό, διενεργείται με μυστικότητα, μπορεί να διενεργηθεί επί ρητά προβλεπόμενων μόνο εγκλημάτων και συνιστά επέμβαση που θίγει θεμελιώδη δικαιώματα και ελευθερίες[14]. Λαμβάνοντας λοιπόν υπόψιν την ιδιαίτερη φύση των ψηφιακών δεδομένων επί των οποίων συντελείται η έρευνα, καθώς και το γεγονός πως πλέον στην πλειονότητα των τελεσθέντων εγκλημάτων συναντάται ψηφιακό αποτύπωμα, δέον στις μετέπειτα τροποποιήσεις του Κώδικα Ποινικής Δικονομίας να συμπεριληφθεί ειδικώς προβλεπόμενη διάταξη νόμου, η οποία θα ορίσει όλες εκείνες τις ειδικές δικονομικές προϋποθέσεις τα εχέγγυα για τη διενέργεια σύννομων ψηφιακών ερευνών στα πλαίσια των προβλεπόμενων ανακριτικών πράξεων.

[13] Δημήτριος Γκύζης, Αντιεισαγγελέας Εφετών, κεφ. 17 «Ψηφιακή ανακριτική πράξη», Ηλεκτρονικό έγκλημα, επιμέλεια Θεοχάρης Ι Δαλακούρας, εκδ. Νομική Βιβλιοθήκη, σελ. 380.

[14] Δημήτριος Γκύζης, Αντιεισαγγελέας Εφετών, κεφ. 17 «Ψηφιακή ανακριτική πράξη», Ηλεκτρονικό έγκλημα, επιμέλεια Θεοχάρης Ι Δαλακούρας, εκδ. Νομική Βιβλιοθήκη, σελ. 382.

Τέλος, από τον συνδυασμό των διατάξεων των άρθρων 258 και 265 παρ. 3 ΚΠΔ, συνάγεται η υποχρέωση των ανακριτικών Αρχών που προβαίνουν σε έρευνα ψηφιακών δεδομένων να συντάσσουν μετά το πέρας αυτής, ειδική και λεπτομερή έκθεση αναφορικά με τα ευρήματα και τα αποτελέσματα της έρευνας που διεξήγαγαν, καθώς και τις μεθόδους και τα μέσα που χρησιμοποιήθηκαν από μέρους τους προς τον ως άνω σκοπό. Η σύνταξη της ως άνω εκθέσεως κρίνεται δε ως απαραίτητη, καθώς η ιδιαίτερη φύση των ψηφιακών δεδομένων επί των οποίων επιχειρείται η έρευνα, είναι εύκολο να δημιουργήσει αμφιβολίες αναφορικά με την ορθότητα της διαδικασίας συλλογής αυτών και την τήρηση των επιταγών της αρχής της ηθικής απόδειξης, καθώς και την προστασία όλων των δικαιωμάτων του υπόπτου – κατηγορουμένου που ανάγονται στην σφαίρα προστασίας των προσωπικών του δεδομένων αυτού.

3. Από το προϊσχύσαν καθεστώς στο άρθρο 265 του νέου Κώδικα Ποινικής Δικονομίας

3.1. Οι ελλείψεις στο κανονιστικό πλαίσιο του προηγούμενου Κώδικα Ποινικής Δικονομίας

Ο προϊσχύσας Κώδικας Ποινικής Δικονομίας, δεν συμπεριλάμβανε ειδικές διατάξεις για την έρευνα και την κατάσχεση ψηφιακών δεδομένων, παρά στις περιπτώσεις εγκλημάτων που είτε διαπράττονταν μέσω ηλεκτρονικού υπολογιστή στον κυβερνοχώρο, είτε στις περιπτώσεις όπου τα πειστήρια και στοιχεία του εγκλήματος είχαν την μορφή ψηφιακών δεδομένων, ο εφαρμοστής του νόμου προέβαινε σε αναλογική εφαρμογή των διατάξεων για την έρευνα και κατάσχεση των υλικών αντικειμένων και των εγγράφων, των άρθρων 253 επ. ΚΠΔ, ήτοι εφαρμόζονταν οι γενικές διατάξεις σχετικά με το διαδικαστικό στάδιο κατά το οποίο χωρεί έρευνα και κατάσχεση, τα αρμόδια όργανα για τη διενέργεια της, την ακολουθητέα διαδικασία, την ένδικη προστασία του καθ' ού η κατάσχεση κ.ο.κ.[15]. Διαπιστώνουμε λοιπόν, δυνάμει των ανωτέρω πως τα ψηφιακά δεδομένα, που παρουσίαζαν ποινικό ενδιαφέρον ως στοιχεία ή πειστήρια εγκλήματος, εξισώνονταν δικονομικά και αντιμετωπίζονταν ως υλικά

[15] Γιάννης Ναζίρης, Επίκουρος Καθηγητής ΑΠΘ, Δικηγόρος, ΠοινΔικ, [Νομική Βιβλιοθήκη], ISSN:1108-2755, τομ.24 τευχ.247 [2021] σελ.178-194.

αντικείμενα, ήτοι ταυτίζονταν με τον υλικό τους φορέα, στις περιπτώσεις όπου υπήρχε τέτοιος. Συνεπώς, οι ιδιαιτερότητες που συνδέονται με την ανάκτηση και την διατήρηση ψηφιακών δεδομένων για ανακριτικούς σκοπούς αντιμετωπίζονταν όχι ως νομικά ζητήματα που έχριζαν δικονομικής ρύθμισης, αλλά σε ένα αμιγώς επιχειρησιακό πλαίσιο. Έτσι η ανάκτηση και ανάλυση ψηφιακών πειστηρίων ανατέθηκε σε ειδικά τμήματα στο πλαίσιο της ελληνικής αστυνομίας, όπως το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων της Διεύθυνσης εγκληματολογικών ερευνών και ιδίως στη Διεύθυνση Δίωξης ηλεκτρονικού εγκλήματος. [16]

Η αναλογική εφαρμογή όμως των ως άνω γενικών διατάξεων, δεν κατέστη εφικτό να αντιμετωπίσει τα ανακύπτοντα δικονομικά ζητήματα που απέρρεαν από την ιδιαιτερότητα της φύσεως των ψηφιακών δεδομένων, καθώς ο άυλος χαρακτήρας που αυτά φέρουν, τα διαφοροποιεί πλήρως από τα υλικά ενσώματα αντικείμενα. Συνεπώς, η κατάσχεση του υλικού φορέα των ψηφιακών δεδομένων, θα πρέπει να αντιμετωπίζεται διακριτά από την κατάσχεση των ψηφιακών δεδομένων που αυτός (ο υλικός φορέας) εμπεριέχει. Η πρακτική ταύτισης ή και εξομοίωσης του υλικού φορέα των ψηφιακών δεδομένων και των ψηφιακών δεδομένων καθαυτών, τόσο σε δικονομικό αλλά και σε πρακτικό επίπεδο, που ακολουθούνταν από τον προϊσχύοντα Κώδικα Ποινικής Δικονομίας, πέραν του γεγονότος πως περιόριζε την ταχύτητα και την ποιότητα της ανακριτικής πράξεως της κατάσχεσης, ελλόχευε πλείονες κινδύνους. Πριν την ενσωμάτωση στον Κώδικα Ποινικής Δικονομίας του νέου άρθρου 265, δε νοείτο κατάσχεση ψηφιακών δεδομένων επί τόπου, χωρίς παράλληλη κατάσχεση και του υλικού φορέα στον οποίο ενσωματώνονταν, γεγονός που δημιουργούσε δικονομικά κενά και ανασφάλεια δικαίου, αναφορικά με την απομακρυσμένη κατάσχεση ψηφιακών δεδομένων και την κατάσχεση ψηφιακών δεδομένων που δεν ενσωματώνονται σε κάποιον υλικό φορέα.

Επιπλέον, η πρόσβαση στα ψηφιακά δεδομένα του ατόμου και η επερχόμενη κατάσχεση του υλικού φορέα όπου αυτά ενσωματώνονται, προκειμένου να γίνει ανάκτηση ή περαιτέρω ανάλυση και αξιοποίησή τους, χωρίς την ύπαρξη ρητών διατάξεων νόμου που θα διασφαλίζουν την προστασία του υποκειμένου των ψηφιακών δεδομένων, μέσα από την

[16] Γιάννης Ναζίρης, Επίκουρος Καθηγητής ΑΠΘ, Δικηγόρος, ΠοινΔικ, [Νομική Βιβλιοθήκη], ISSN:1108-2755, τομ.24 τευχ.247 [2021] σελ.178-194.

πρόβλεψη των ειδικών και εξειδικευμένων διαδικασιών αλλά και μέσων που θα χρησιμοποιηθούν προς τους ανωτέρω σκοπούς της κατασχέσεως και ανάλυσης των δεδομένων, αλλά και η τύχη των δεδομένων αυτών αναφορικά με την διατήρησή και φύλαξή τους, έως ότου περατωθεί η ποινική διαδικασία, όπως και το μέτρο και η έκταση των δεδομένων που μέλλουν να αξιοποιηθούν, ως αφορώντα την επίδικη υπόθεση, από τα συνολικώς ανακτηθέντα ψηφιακά δεδομένα, συνιστούν κρίσιμα και ευαίσθητα ζητήματα, τα οποία δεν θα μπορούσαν να συνεχίζουν να αντιμετωπίζονται μέσω της αναλογικής εφαρμογής διατάξεων νόμων. Αντιθέτως δε, κρίθηκε ως επιβεβλημένη η ειδική και εμπεριστατωμένη πρόβλεψη και ρύθμισή τους δια της τροποποίησης των διατάξεων του Κώδικα Ποινικής Δικονομίας και της προσθήκης του νέου άρθρου 265 ΚΠΔ.

Ο ιδιαίτερος χαρακτήρας που φέρουν τα ψηφιακά δεδομένα έναντι των υλικών ενσώματων αντικειμένων άλλωστε, δεν θα μπορούσε να παραβλεφθεί επί μακρόν και να συνεχίσουν να τυγχάνουν αναλογικής εφαρμογής οι διατάξεις των δεύτερων επί περιπτώσεων των πρώτων. Υπάρχουν κατηγορίες ψηφιακών δεδομένων, που δύνανται να αποτελέσουν αντικείμενο ποινικής δίκης κατόπιν της κατασχέσεώς τους, που από την φύση τους αποτυπώνονται και εμφανίζονται με την μορφή του δυαδικού συστήματος ή με την μορφή μιας γλώσσας προγραμματισμού. Είναι λοιπόν προδήλως φανερό πως για την ανάκτηση, την δικαστηριακή αξιοποίηση, αλλά και την ασφαλή και αναλλοίωτη αποθήκευση τέτοιων δεδομένων, δεν θα επαρκούσαν οι προβλέψεις των διατάξεων για την κατάσχεση υλικών αντικειμένων ή εγγράφων, παρά επιβάλλεται η ρητή πρόβλεψη από διάταξη νόμου των διαδικασιών και των διατυπώσεων που πρέπει να τηρηθούν προκειμένου να επιτευχθεί η ασφαλής απόκτηση και αξιοποίηση των ως άνω δεδομένων, αλλά και η εξασφάλιση πως οι ως άνω διαδικασίες θα διενεργηθούν από καταλλήλως εκπαιδευμένα υποκείμενα, που θα φέρουν ειδικές και εξειδικευμένες γνώσεις επί του αντικειμένου. Επιπλέον η διασφάλιση του αναλλοίωτου χαρακτήρα των ως άνω δεδομένων, τόσο κατά τη διενέργεια των διαδικασιών ανάκτησης και κατάσχεσης, όσο και κατά τη φύλαξη και αποθήκευση αυτών, ήταν επιβεβλημένο να προβλέπεται ρητά και να επιβάλλεται ρητά από διάταξη νόμου, έτσι ώστε να εξασφαλίζονται όλα τα απαραίτητα προς τον ως άνω σκοπό μέσα και να υπάρχει ασφάλεια δικαίου, ορθή απονομή δικαιοσύνης

και εξασφάλισης ακεραίου του δικαιώματος υπεράσπισης του κατηγορουμένου.

Συνεπώς, δυνάμει των ανωτέρω, η ραγδαία ανάπτυξη της τεχνολογίας και το φυσικό επακόλουθο της δημιουργίας ψηφιακών αποτυπωμάτων και δεδομένων σε κάθε πτυχή της δραστηριότητας του ατόμου, επέβαλαν ως αναγκαία τη θεσμοθέτηση ειδικής διάταξης νόμου, για τη δικονομική μεταχείριση των ψηφιακών δεδομένων και εισήγαγαν στην ελληνική έννομη τάξη τη διάταξη του νέου άρθρου 265 ΚΠΔ, αναφορικά με την Κατάσχεση Ψηφιακών Δεδομένων.

3.2. Η Κατάσχεση ως ανακριτική πράξη του νέου Κώδικα Ποινικής Δικονομίας.

Η κατάσχεση ως ανακριτική πράξη του τρίτου κεφαλαίου του δεύτερου τμήματος του Κώδικα Ποινικής Δικονομίας, και συγκεκριμένα των άρθρων 260 επ. ΚΠΔ συνιστά δικονομική πράξη με την οποία προβλέπεται η αφαίρεση από την σφαίρα κατοχής του υπόπτου ή του κατηγορουμένου, ή και τρίτου προσώπου διακριτού από τις ως άνω έννοιες, υλικού αντικειμένου, κινητού ή ακινήτου, ή ακόμη και εγγράφων, αλλά και τίτλων αξιών σε τραπεζικά ιδρύματα δημόσια ή ιδιωτικά, και τραπεζικών λογαριασμών ή τραπεζικών θυρίδων και εν γένει όλων των αντικειμένων που συνιστούν προϊόντα που προέρχονται άμεσα ή έμμεσα από τη διερευνώμενη αξιόποινη πράξη ή σχετίζονται με το έγκλημα. Κατά συνέπεια, η ενεργοποίηση ή μη της δυνατότητας κατάσχεσης ενός ενσώματου αντικειμένου συνεπάγεται νόμιμη κατοχή είτε του είτε των ανακριτικών αρχών είτε του καθ' ου αντίστοιχα, αλλά ποτέ και των δύο ταυτόχρονα.[17] Ρητά δε ορίζεται από τη διάταξη του άρθρου 261 ΚΠΔ, πως μπορεί να διαταχθεί δέσμευση των περιουσιακών στοιχείων του κατηγορουμένου, εφόσον από μετά από τη διερεύνηση της περιουσιακής κατάστασης αυτού κατά το άρθρο 248 ΚΠΔ, προκύψουν σοβαρές ενδείξεις πως τα περιουσιακά αυτά στοιχεία προέρχονται άμεσα ή έμμεσα από τη διερευνώμενη αξιόποινη πράξη. Μάλιστα η ως άνω δέσμευση σε περιουσιακά στοιχεία δύναται να επιβληθεί ακόμη και αν ο

[17] Γιάννης Ναζίρης, Επίκουρος Καθηγητής ΑΠΘ, Δικηγόρος, ΠοινΔικ, [Νομική Βιβλιοθήκη], ISSN:1108-2755, τομ.24 τευχ.247 [2021] σελ.178-194.

κατηγορούμενος προέβη σε μεταβίβαση αυτής σε τρίτο πρόσωπο, αν από την έρευνα συνάγονται σοβαρές ενδείξεις πως τα υπό κρίση περιουσιακά αυτά στοιχεία προέρχονται άμεσα ή έμμεσα από τη διερευνώμενη αξιόποινη πράξη, πολλώ δε μάλλον αν η μεταβίβαση στο τρίτο αυτό πρόσωπο έγινε από πλευράς του κατηγορουμένου με διόλου εύλογο τίμημα. Κατάσχεση μπορεί να διαταχθεί σε οποιοδήποτε στάδιο της ποινικής διαδικασίας, ακόμη και πριν την κίνηση της ποινικής διώξεως, ακόμη και κατά τη διάρκεια της προκαταρκτικής εξέτασης (αρ. 243 παρ. 1 εδ. β ΚΠΔ), αλλά ακόμη και μετά το πέρας της ανάκρισης (αρ. 266 παρ. 1 ΚΠΔ), ενώ για την τύχη των κατασχεθέντων εγγράφων αποφαίνεται ειδικά, σύμφωνα με τα οριζόμενα στη διάταξη του άρθρου 372 ΚΠΔ το δικαστήριο. Τέλος σύμφωνα με τη διάταξη του άρθρου 259 ΚΠΔ, αναφορικά με τη μεσεγγύηση, ρητά από τη διάταξη του νόμου ορίζεται πως *«όποιος ενεργεί την ανάκριση μπορεί να προβαίνει οποτεδήποτε σε μεσεγγύηση πραγμάτων ή εγγράφων που σχετίζονται με το έγκλημα, ακόμη και όταν δεν κατασχέθηκαν, αλλά απλώς παραδόθηκαν σε αυτόν».*

3.3. Το νέο άρθρο 265 ΚΠΔ – «Κατάσχεση Ψηφιακών Δεδομένων»

Κατόπιν εκθέσεως των γενικότερων διατάξεων αφορώντων στην ανακριτική πράξη της κατασχέσεως ενσώματων αντικειμένων, οι οποίες, πριν τη θέση σε εφαρμογή του ν. 4620/1019, τύγχαναν αναλογικής εφαρμογής και για τις περιπτώσεις κατάσχεσης των άυλων ψηφιακών δεδομένων, δέον να ακολουθήσει η παράθεση και ανάλυση του νέου άρθρου 265 ΚΠΔ, το οποίο τέθηκε σε ισχύ τη 01-07-2019, και ισχύει από της θεσπίσεώς του αναλλοίωτο μέχρι και σήμερα, φέροντας τον τίτλο «Κατάσχεση Ψηφιακών Δεδομένων». Σύμφωνα με τα προβλεπόμενα στην ως άνω διάταξη νόμου λοιπόν, ορίζονται τα εξής:

*«**1.** Η κατάσχεση ψηφιακών δεδομένων μπορεί να επιβληθεί:*

α) Σε ένα σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτόν, στα οποία έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση,

β) σε ένα μέσο αποθήκευσης δεδομένων υπολογιστή στο οποίο υπάρχουν αποθηκευμένα δεδομένα υπολογιστή και έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση,

γ) σε ένα απομακρυσμένο σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτόν ή σε ένα απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτό, τα οποία είναι διασυνδεδεμένα στο σύστημα υπολογιστή στο οποίο έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση. Στην τελευταία περίπτωση, τα ψηφιακά δεδομένα που είναι αποθηκευμένα και προσβάσιμα μέσω συστήματος και υπηρεσιών νεφοϋπολογιστικής (cloud services) δεν θεωρούνται αποθηκευμένα σε απομακρυσμένο σύστημα υπολογιστή ή σε απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή τα οποία είναι διασυνδεδεμένα στο σύστημα υπολογιστή στο οποίο έχουν φυσική πρόσβαση οι αρχές.

2. *Η κατά τα ανωτέρω κατάσχεση πραγματοποιείται αποκλειστικά με τη χρήση κατάλληλου εξοπλισμού που επιτρέπει σε εκείνον που τη διεξάγει:*

α) Την αφαίρεση και την κατάσχεση του υλικού φορέα των υπό στοιχείων α-γ της παρ. 1, στο οποίο βρίσκονται αποθηκευμένα τα δεδομένα και/ή

β) την αντιγραφή και την αφαίρεση των αποθηκευμένων ψηφιακών δεδομένων των υπό στοιχείων α-γ της παρ. 1 σε μέσο αποθήκευσης δεδομένων και

γ) την αναπαραγωγή και την επαλήθευση της αυθεντικότητας και της ακεραιότητας των κατασχεθέντων δεδομένων.

3. *Η κατάσχεση που διενεργείται κατά τις παρ. 1 και 2, βεβαιώνεται με ειδική έκθεση, η οποία αναφέρει ειδικώς τις ενέργειες της παρ. 2 που πραγματοποιεί εκείνος που διεξάγει την ανάκριση.*

4. *Τα ψηφιακά δεδομένα που κατάσχονται διατηρούνται αποθηκευμένα καθ' όλη τη διάρκεια της ποινικής διαδικασίας σε ένα και μόνο υλικό μέσο αποθήκευσης που περιέχεται στη δικογραφία. Ασφαλές αντίγραφο αυτού ώστε να διασφαλίζεται η δυνατότητα ανάκτησης των δεδομένων που έχουν κατασχεθεί, σε περίπτωση απώλειας ή καταστροφής, σχηματίζεται κατά την κατάσχεσή τους και διατηρείται στο γραφείο πειστηρίων του πρωτοδικείου στο οποίο υποβάλλεται η δικογραφία και το οποίο παρέχει τις κατάλληλες εγγυήσεις φυσικής ασφάλειας και πρόσβασης σε εκείνους μόνο που ασκούν καθήκοντα στην υπόθεση. Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία.*

5. *Η πρόσβαση και η δυνατότητα αναπαραγωγής των ψηφιακών δεδομένων που κατάσχονται επιτρέπεται μόνο σε όσους ασκούν δικαστικά, εισαγγελικά και ανακριτικά καθήκοντα στην υπόθεση ή τους γραμματείς. Προς το σκοπό*

αυτό χρησιμοποιούνται τα κατάλληλα τεχνικά μέσα. Τέτοια μέσα είναι η κρυπτογράφηση και η χρήση κωδικών ασφαλείας για την πρόσβαση και αναπαραγωγή των κατασχεμένων ψηφιακών δεδομένων από το υλικό μέσο αποθήκευσης στο οποίο βρίσκονται αποθηκευμένα. Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία.

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

3.3.1. Η έννοια των ψηφιακών δεδομένων - Ορισμοί

Στο σημείο αυτό, πριν προβούμε στην ανάλυση των όσων νομικών ζητημάτων ορίζονται στο ως άνω άρθρο 265 ΚΠΔ, δέον να καταφύγουμε στην ανάλυση και κατανόηση των τεχνολογικών και τεχνικών όρων που εμφανίζονται σε αυτό.

Η έννοια των ψηφιακών δεδομένων κατά το ελληνικό ποινικό δίκαιο, τίθεται στη διάταξη του άρθρου 13 παρ. 1 περ. ζ' ΠΚ, όπου ρητά ορίζεται πως, *«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 μία λειτουργία»,* ενώ πληροφοριακό σύστημα, από την ίδια ως άνω διάταξη του άρθρου 13 παρ. 1 περ. στ' ΠΚ, ορίζεται πως *«είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών».* Ο ορισμός αυτός τέθηκε αρχικά στον προϊσχύσαντα Ποινικό Κώδικα, δυνάμει της πρώτης παραγράφου του δεύτερου άρθρου του Ν. 4411/2016, με τον οποίο κυρώθηκε στην ελληνική έννομη τάξη η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, και διατηρήθηκε

απαράλλακτός (ο ορισμός) μετά τις τροποποιήσεις που επέφερε ο Ν. 4620/2019 και η θέση σε ισχύ του νέου Ποινικού Κώδικα.

Μολονότι ο εν λόγω ορισμός τέθηκε στις διατάξεις του Ποινικού Κώδικα, είναι σαφές ότι μπορεί να αξιοποιηθεί για την εφαρμογή όχι μόνο των διατάξεων του ουσιαστικού ποινικού αλλά και του δικονομικού ποινικού δικαίου[18]. Εξάλλου, οι δύο ως άνω θεμελιώδεις νόμοι – κώδικες συνυπάρχουν αυτονόητα στην ποινική διαδικασία, άρα ο ερμηνευτής τους δικαιούται να προσφεύγει σε αμφότερους για την πλήρη κατανόηση του φαινομένου που ονομάζεται «απονομή ποινικής δικαιοσύνης».[19] Η κατανόηση των δύο ως άνω ορισμών, οι οποίοι εμφανίζονται στη διάταξη του άρθρου 265 ΚΠΔ, είναι κομβικής σημασίας, ώστε να διαπιστώσουμε τι μπορεί να αποτελέσει αντικείμενο κατάσχεσης, στα πλαίσια της ως άνω διάταξης νόμου.

3.3.2. Κατηγορίες Ψηφιακών Δεδομένων

Αρχικά από τον ορισμό των ψηφιακών δεδομένων, όπως αυτός παρατίθεται στον Ποινικό Κώδικα, συνάγεται πως αυτά (τα ψηφιακά δεδομένα), στον βαθμό που απασχολούν το ποινικό δίκαιο, συνιστούν «παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα», συνιστούν δηλαδή μία παράθεση δεδομένων που αρχικώς, ήτοι αμέσως μετά την ανάκτησή τους, συνιστούν ένα σύνολο ψηφιακών δεδομένων που μέσω της κατάλληλης επεξεργασίας και ανάλυσής τους, δύνανται να αποδώσουν μία πληροφορία που θα αξιολογηθεί και θα αξιοποιηθεί στα πλαίσια των ανακριτικών πράξεων. Είναι μάλιστα σημαντικό να σημειωθεί πως, από την ως άνω διάταξη νόμου συνάγεται πως, τα ψηφιακά δεδομένα που κατάσχονται στα πλαίσια της ανακριτικής πράξεως του άρθρου 265 ΚΠΔ, δεν συνιστούν αποκλειστικά επεξεργασμένη μορφή δεδομένων, που είναι διαθέσιμα για άμεση αξιοποίηση από πλευράς των Αρχών, αλλά επεξεργάσιμη μορφή δεδομένων, ήτοι μπορεί να συνιστούν και πληροφορία που εξάγεται σε μορφή δυαδικού συστήματος ή σε μορφή γλώσσας προγραμματισμού,

[18] Γιάννης Ναζίρης, Επίκουρος Καθηγητής ΑΠΘ, Δικηγόρος, ΠοινΔικ, [Νομική Βιβλιοθήκη], ISSN:1108-2755, τομ.24 τευχ.247 [2021] σελ.178-194.

[19] Μαριάννα Κουδελή, Στρατιωτικός Δικαστής, Ζητήματα που άπτονται της κατάσχεσης ψηφιακών δεδομένων του άρθρου 265 του ΚΠΔ, Ηλεκτρονικό έγκλημα, επιμέλεια Θεοχάρης Ι Δαλακούρας, σελ. 528.

γεγονός που καθιστά απαραίτητη τη συνδρομή ατόμων με ιδιαίτερες γνώσεις και τεχνογνωσίες, με στόχο την αξιοποίηση των εξαχθέντων πληροφοριών.

Τόσο όμως ο Ποινικός Κώδικας, όσο και ο Κώδικας Ποινικής Δικονομίας αρκούνται στην απλή παράθεση του ορισμού των ψηφιακών δεδομένων, χωρίς να προβαίνουν σε περαιτέρω διάκριση και ανάλυση αυτών, όπως αυτή (η διάκριση) έχει παρατεθεί από τη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο, και συγκεκριμένα τα ψηφιακά δεδομένα διακρίνονται στις εξής κατηγορίες:

- **Δεδομένα συνδρομητή / χρήστη (subscriber data),** ήτοι όλα τα δεδομένα, οι πληροφορίες και άλλο περιεχόμενο που παρέχονται από ή για λογαριασμό του Συνδρομητή στην Υπηρεσία, συμπεριλαμβανομένου αυτού που οι Χρήστες Λογαριασμού εισάγουν ή ανεβάζουν στην Υπηρεσία.

- **Δεδομένα κίνησης (traffic data),** ήτοι τα δεδομένα υπολογιστών που σχετίζονται με μία επικοινωνία μέσω ενός συστήματος υπολογιστή, δημιουργούμενα από ένα σύστημα υπολογιστή που αποτελούσε τμήμα της αλυσίδας επικοινωνίας, τα οποία καταδεικνύουν την προέλευση, τον προορισμό, το δρομολόγιο, τον χρόνο, την ημερομηνία, το μέγεθος, τη διάρκεια ή τον τύπο της υφιστάμενης υπηρεσίας της επικοινωνίας. Είναι λοιπόν τα δεδομένα υπολογιστών που σχετίζονται με μία επικοινωνία μέσω ενός συστήματος υπολογιστή, δημιουργούμενα από ένα σύστημα υπολογιστή που αποτελούσε τμήμα της αλυσίδας επικοινωνίας, τα οποία καταδεικνύουν την προέλευση, τον προορισμό, το δρομολόγιο, το χρόνο, την ημερομηνία, το μέγεθος, τη διάρκεια ή τον τύπο της υφιστάμενης υπηρεσίας της επικοινωνίας. (άρθρο 1, παρ. 1 περ. δ', Κεφάλαιο Ι, Σύμβασης της Βουδαπέστης για το Κυβερνοέγγλημα)

- **Δεδομένα περιεχομένου (content data)**, έννοια η οποία δεν τυποποιείται ρητά στο σώμα της ως άνω Συμβάσεως, αλλά

αναφέρεται στο περιεχόμενο ορισμένης επικοινωνίας. Στην κατηγορία αυτή εμπίπτει το αρχείων κειμένου (όπως μηνύματα ηλεκτρονικής αλληλογραφίας), ήχου (όπως μουσική), εικόνας (όπως ταινίες) κ.α.[20]

Η μη διάκριση και κατηγοριοποίηση των ψηφιακών δεδομένων από μέρους της ελληνικής έννομης τάξης, συνεπάγεται την όμοια και ίση αντιμετώπιση των δεδομένων αυτών, όταν στα πλαίσια της διαδικασίας κατασχέσεώς τους δυνάμει του άρθρου 265 ΚΠΔ, επιχειρείται η κατάσχεση, ανάκτηση και ανάλυσή τους. Τίθεται λοιπόν ο προβληματισμός, αν στα πλαίσια των ανακριτικών πράξεων και συγκεκριμένα της έρευνας και την κατάσχεσης των ως άνω δεδομένων, θα έπρεπε να συντρέχουν διαφορετικές νομοθετικές προβλέψεις, ως προς την μεταχείρισή τους ή αν επαρκεί ο προστασία αυτών, υπό το πρίσμα του απορρήτου των επικοινωνιών και της αρχής της αναλογικότητας και αναγκαιότητας σκοπού που διέπει το σύνολο της ανακριτικής διαδικασίας.

Πέραν της ως άνω κατηγοριοποίησης των ψηφιακών δεδομένων, η οποία πηγάζει από το σώμα του κειμένου της Σύμβασης της Βουδαπέστης, περαιτέρω διάκριση των ψηφιακών δεδομένων που θα μπορούσε να παρουσιάζει ενδιαφέρον στα πλαίσια των ανακριτικών πράξεων του άρθρου 265 ΚΠΔ, εξαιτίας τόσο της ιδιαίτερης φύσης τους, της ιδιαιτερότητας στην επεξεργασία και ανάκτησή τους, αλλά κυρίως λόγω της προστασίας των δεδομένων που περικλείουν, είναι η ακόλουθη:

- **Δομημένα, Ημιδομημένα, Μη δομημένα δεδομένα:** Δομημένα είναι τα δεδομένα που αναπαριστώνται με αυστηρή μορφοποίηση, Ημιδομημένα είναι τα δεδομένα που συλλέγονται με έναν καθορισμένο τρόπο πριν γίνει γνωστό με ποια ακριβώς μορφή θα αποθηκευτούν, με αποτέλεσμα οι πληροφορίες που συλλέγονται να μην έχουν ταυτόσημη δομή αναμεταξύ τους, Μη δομημένα είναι τα δεδομένα τα οποία δεν διαθέτουν κάποια εγγενή σειρά, με αποτέλεσμα να καθίσταται δυσχερής η ταξινόμηση και η συσχέτιση τους.

[20] Γιάννης Ναζίρης, Επίκουρος Καθηγητής ΑΠΘ, Δικηγόρος, ΠοινΔικ, [Νομική Βιβλιοθήκη], ISSN:1108-2755, τομ.24 τευχ.247 [2021] σελ.178-194.

- **Μεταδεδομένα:** Είναι τα δεδομένα που χρησιμοποιούνται για την περιγραφή δομημένων, ημιδομημένων και μη δομημένων δεδομένων.
- **Χρονοσημασμένα η ακολουθιακά δεδομένα:** Είναι εκείνα τα δεδομένα που αναπαριστούν μία χρονική ακολουθία ανάκτησης η επεξεργασίας σε πραγματικό ή μη χρόνο.
- **Χωροχρονικά δεδομένα:** Είναι τα δεδομένα που αποτυπώνουν ταυτόχρονα τον χώρο και τον χρόνο ορισμένους συμβάντος και χρησιμοποιούνται κατά κανόνα για να αποτυπώσουν τις μεταβολές που επέρχονται σε ορισμένη γεωγραφικά περιοχή κατά χρόνου. Τέτοιου είδους είναι τα δεδομένα που αφορούν την κίνηση οχημάτων αλλά και τις ανωμαλίες σε ένα δίκτυο τηλεπικοινωνιών.
- **Δεδομένα μηχανών:** Είναι εκείνα τα δεδομένα που δημιουργούνται μέσα από την λειτουργία διαφόρων συσκευών. Επειδή συλλέγονται ανώνυμα και χρησιμοποιούνται για στατιστικούς σκοπούς ή για την αντιμετώπιση προβλημάτων που ανακύπτουν κατά την χρήση συσκευών και εφαρμογών δεν συγκαταλέγονται στα προσωπικά δεδομένα.
- **Ανοιχτά δεδομένα:** Είναι τα δεδομένα που είναι ελεύθερα προσβάσιμα στον καθένα. Η ελεύθερη πρόσβαση σε αυτά δεν συνεπάγεται αυτονόητα και την δυνατότητα ευχερούς αξιοποίησης τους, αφού σε αρκετές περιπτώσεις αποθηκεύονται σε μορφή μη κατανοητή από το μέσο χρήστη.
- **Σκοτεινά δεδομένα:** Είναι τα δεδομένα που παραμένουν αδρανή, χωρίς να αξιοποιούνται από κάποιο πληροφοριακό σύστημα ή εφαρμογή.
- **Δεδομένα σε πραγματικό χρόνο:** Είναι εκείνα τα δεδομένα που αποτελούν αντικείμενο επεξεργασίας σε πληροφοριακό σύστημα, το οποίο παρέχει απαιτούμενο επίπεδο υπηρεσίας ως συνάρτηση των διαθέσιμων πόρων, εντός ενός εγγυημένου χρόνου απόκρισης, ανεξάρτητα από το φόρτωμα του συστήματος όταν δεχθεί εξωτερικό ερέθισμα. Η δυνατότητα ανάκτησης δεδομένων σε πραγματικό χρόνο αποτελεί βασική προτεραιότητα των ανακριτικών αρχών σήμερα.
- **Γονιδιωματικά δεδομένα:** Είναι εκείνα τα δεδομένα συνίστανται στην ανάλυση του γονιδιώματος (DNA), και τα οποία ανήκουν στην κατηγορία των ευαίσθητων δεδομένων.

- **Δεδομένα υψηλών διαστάσεων:** Είναι σύνθετα δεδομένα (όπως π.χ. βιομετρικά δεδομένα που αφορούν την αναγνώριση προσώπου), η οπτικοποίηση και επεξεργασία των οποίων προϋποθέτει κατά κανόνα εφαρμογή τεχνικών μείωσης διάστασης.[21]

Όλες οι ως άνω δε εκτεθείσες κατηγορίες ψηφιακών δεδομένων, συνιστούν, μέρος της ευρύτερης κατηγορίας των «μεγάλων» δεδομένων (big data).

Βασικό ερώτημα που προκύπτει σε σχέση με τα ψηφιακά δεδομένα, ως αποδεικτικά μέσα στο ισχύον σύστημα της Ποινικής Δικονομίας, είναι αν υπάρχει ανάγκη ένταξής τους, ως ιδιαίτερο αποδεικτικό μέσο, στο άρθρο 177 ΚΠΔ. Η απάντηση στο ερώτημα οφείλει να είναι καταφατική. Για λόγους σαφήνειας αλλά ιδίως για λόγους νομιμότητας των ανακριτικών πράξεων που σχετίζονται με τα ψηφιακά δεδομένα, ο νομοθέτης οφείλει να εντάξει τα ψηφιακά δεδομένα, ως ιδιαίτερο αποδεικτικό στοιχείο, στο άρθρο 177 ΚΠΔ[22], αναφορικά με την αρχή της ηθικής απόδειξης. Σύμφωνα με τα οριζόμενα στην ως άνω αρχή, «οι δικαστές δεν ακολουθούν νομικούς κανόνες αποδείξεων, πρέπει όμως να αποφασίζουν κατά την πεποίθησή τους, ακολουθώντας τη φωνή της συνείδησής τους και οδηγούμενοι από την απροσωπόληπτη κρίση που προκύπτει από τις συζητήσεις και που αφορά την αλήθεια των πραγματικών περιστατικών, την αξιοπιστία των μαρτύρων και την αξία των άλλων αποδείξεων, αιτιολογώντας πάντοτε ειδικά και εμπεριστατωμένα με ποια αποδεικτικά μέσα και με ποιους συλλογισμούς σχημάτισαν την δικανική τους κρίση». Η ιδιαιτερότητα της φύσης, του τρόπου έρευνας και κατάσχεσης και η ευαλωτότητα των ως άνω ψηφιακών δεομένων, καταδεικνύουν την ανάγκη εφαρμογής επί των περιπτώσεων αυτών του άρθρου 177 ΚΠΔ. Προς τούτο, πρέπει να ληφθούν υπόψιν δύο παράμετροι: Πρώτον τα ψηφιακά δεδομένα είναι διακριτά και αυτοτελή έναντι των υλικών μέσων αποθήκευσης τους, όσο και φυσικά των εγγράφων[23]. Δεύτερον τα ψηφιακά

[21] Γιάννης Ναζίρης, Επίκουρος Καθηγητής ΑΠΘ, Δικηγόρος, ΠοινΔικ, [Νομική Βιβλιοθήκη], ISSN:1108-2755, τομ.24 τευχ.247 [2021] σελ.178-194.

[22] Αλέξανδρος Ι Καργιόπουλος, Ηλεκτρονικό Έγκλημα, Θεοχάρης Ι Δαλακούρας, Εκδ. Νομική Βιβλιοθήκη, κεφ. 12- Ανακριτικές πράξεις επί ψηφιακών δεδομένων: Δικαιικοί άξονες και προβληματισμοί, σελ 203

δεδομένα όπως ειδικώς προσδιορίζονται στον Ποινικό Κώδικα, και συγκεκριμένα η διαδικασία που επιβάλλεται να τηρηθεί από πλευράς των Αρχών σε περίπτωση που απαιτείται η έρευνα και κατάσχεσή τους, ως αποδεικτικά μέσα ή πειστήρια εγκλήματος, τυποποιείται πλέον ρητά στον Κώδικα Ποινικής Δικονομίας, δια του άρθρου 265 ΚΠΔ. Τίθενται δηλαδή, πλέον δια του νόμου, όλες οι ειδικές και απαραίτητες διαδικασίες και διατυπώσεις που πρέπει να τηρηθούν, όταν επιβάλλεται η συλλογή και κατάσχεση, στα πλαίσια της ποινικής διαδικασίας, ψηφιακών δεδομένων. Και στην ιδιαίτερη όμως αυτή περίπτωση κτήσης αποδεικτικού μέσου, σκοπός του δικαστή είναι η αναζήτηση της ουσιαστικής αλήθειας, μέσω της ελεύθερης εκτίμησης των αποδείξεων, ακολουθώντας την φωνή της συνείδησής τους και οδηγούμενοι από την απροσωπόληπτη κρίση τους που προκύπτει από τις συζητήσεις και που αφορά την αλήθεια των πραγματικών γεγονότων, και την αξιοπιστία μεταξύ άλλων των κτηθέντων αποδείξεων. Συνεπώς, δυνάμει των ως άνω, κρίνεται ως επιβεβλημένη η εφαρμογή του προεκτεθέντος άρθρου 177 ΚΠΔ και στις περιπτώσεις κατάσχεσης ψηφιακών δεδομένων του άρθρου 265 ΚΠΔ.

3.3.3. Ανάλυση του άρθρου 265 ΚΠΔ

Στην πρώτη παράγραφο του άρθρου 265 ΚΠΔ, αναφορικά με την κατάσχεση ψηφιακών δεδομένων ορίζεται πως, *«Η κατάσχεση ψηφιακών δεδομένων μπορεί να επιβληθεί: α) Σε ένα σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτόν, στα οποία έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση, β) σε ένα μέσο αποθήκευσης δεδομένων υπολογιστή στο οποίο υπάρχουν αποθηκευμένα δεδομένα υπολογιστή και έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση, γ) σε ένα απομακρυσμένο σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτόν ή σε ένα απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτό, τα οποία είναι διασυνδεδεμένα στο σύστημα υπολογιστή στο οποίο έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση. Στην τελευταία περίπτωση, τα ψηφιακά δεδομένα που είναι*

[23] Αλέξανδρος Ι Καργιόπουλος, Ηλεκτρονικό Έγκλημα, Θεοχάρης Ι Δαλακούρας, Εκδ. Νομική Βιβλιοθήκη, κεφ. 12- Ανακριτικές πράξεις επί ψηφιακών δεδομένων: Δικαιικοί άξονες και προβληματισμοί, σελ. 203

αποθηκευμένα και προσβάσιμα μέσω συστήματος και υπηρεσιών νεφοϋπολογιστικής (cloud services) δεν θεωρούνται αποθηκευμένα σε απομακρυσμένο σύστημα υπολογιστή ή σε απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή τα οποία είναι διασυνδεδεμένα στο σύστημα υπολογιστή στο οποίο έχουν φυσική πρόσβαση οι αρχές».

Παρατηρούμε πως στην πρώτη αυτή παράγραφο του νέου άρθρου 265 ΚΠΔ, ο νομοθέτης επιχειρεί να παραθέσει και να οριοθετήσει τα μέσα - υλικά και άυλα-, επί των οποίων δύναται να επιχειρηθεί κατάσχεση από τις αρμόδιες ανακριτικές Αρχές, με ευρύτερο σκοπό την κατάσχεση των ψηφιακών δεδομένων που ενσωματώνονται σε αυτά. Διαπιστώνουμε συνεπώς, πως ενώ η διάταξη του άρθρου 265 ΚΠΔ πραγματεύεται την κατάσχεση ψηφιακών, άρα άυλων δεδομένων, η ίδια ως άνω ρύθμιση νόμου συμπεριλαμβάνει πρόβλεψη και για την κατάσχεση και του υλικού φορέα, στον οποίο ενσωματώνεται το ψηφιακό δεδομένο.

Από τα οριζόμενα στη διάταξη του άρθρου 265 παρ. 1 ΚΠΔ, συνάγεται πως κατάσχεση μπορεί να επιβληθεί, «σε ένα σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτόν, σε ένα μέσο αποθήκευσης δεδομένων υπολογιστή και σε ένα απομακρυσμένο σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτόν ή σε ένα απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτό». Παρατηρούμε λοιπόν, πως, ο νομοθέτης προβαίνει σε απαρίθμηση των μέσων επί των οποίων μπορεί να επιβληθεί κατάσχεση με σκοπό την ανάκτηση ψηφιακών δεδομένων, χωρίς όμως η ρύθμιση αυτή να είναι εξαντλητική όλων των περιπτώσεων υλικών φορέων που μπορούν να περικλείουν ψηφιακά δεδομένα, αλλά ούτε και να αφήνεται ρητά δυνατότητα διεύρυνσης των περιοριστικά αναφερόμενων περιπτώσεων επί των οποίων χωρεί κατάσχεση κατά τα οριζόμενα στην ως άνω διάταξη. Το γεγονός αυτό στην πράξη, δύναται να προκαλέσει ζητήματα, αρχικώς διαδικαστικά που στην πορεία θα καταλήξουν ουσιαστικά, καθώς στην ρύθμιση της ως άνω διάταξης νόμου, δεν περικλείονται οι περιπτώσεις των κινητών τηλεφώνων, των tablets, αλλά και των έξυπνων συσκευών, όπως είναι τα έξυπνα ρολόγια ή οι έξυπνες συσκευές. Στην περίπτωση λοιπόν που μια τέτοια συσκευή όπως οι προαναφερθείσες, περιέχει υλικό με την μορφή ψηφιακών δεδομένων

κρίσιμων για την πορεία της διερεύνησης τέλεσης της αξιόποινης πράξης, θα ανακύπτει το ζήτημα του αν μπορεί να εφαρμοστεί αναλογικά η διάταξη του άρθρου 265 ΚΠΔ, ώστε να δοθεί στις Αρχές η δυνατότητα να προβούν στην κατάσχεση και αξιοποίηση των ως άνω δεδομένων ή αν θα παρέχεται στις τελευταίες μόνο η δυνατότητα για κατάσχεση μόνον του υλικού φορέα των ψηφιακών δεδομένων κατ΄ άρθρον 260 επ.

Στο σημείο αυτό να επισημανθεί πως, η κατάσχεση του άρθρου 265 ΚΠΔ, όπως άλλωστε καταδεικνύει και ο τίτλος του άρθρου αυτού του Κώδικα Ποινικής Δικονομίας, αναφέρεται ουσιαστικά στην κατάσχεση των ψηφιακών δεδομένων καθαυτών και όχι στην κατάσχεση του υλικού φορέα στην οποία αυτά ενσωματώνονται, και η οποία (κατάσχεση του υλικού φορέα), αποτελεί αναγκαίο «μέσο», με το οποίο θα επιτευχθεί ο ουσιαστικός σκοπός της διατάξεως, ήτοι η κατάσχεση του ψηφιακού δεδομένου που το μέσο αυτό ενσωματώνει. Η «συγκατάσχεση» λοιπόν του ενσώματου αντικειμένου και των ψηφιακών δεδομένων που αυτό φέρει, ενώ προβλέπεται από τη διάταξη του άρθρου 265 ΚΠΔ, δέον να γίνεται στο μέτρο του αναγκαίου, ώστε με τον τρόπο αυτό να επιτυγχάνεται τόσο η ταχύτητα της ποινικής διαδικασίας, με την κατάσχεση και εξαγωγή μόνον των κομβικών για την υπό κρίση ποινική υπόθεση ψηφιακών δεδομένων, και όχι του συνόλου των δεδομένων που δύναται να φέρει ένας υλικός φορέας (π.χ. ένας ηλεκτρονικός υπολογιστής), αλλά ταυτοχρόνως να προστατεύεται και ο ύποπτος ή ο κατηγορούμενος από τη διαρροή προσωπικών του δεδομένων που δεν είναι κρίσιμα για την υπό κρίση υπόθεση, αλλά και να μην στερείται (ο ύποπτος ή ο κατηγορούμενος) το δικαίωμα ιδιοκτησίας του επί του υλικού αντικειμένου με την «συγκατάσχεσή» του από τις Αρχές.

Αντίθετη στην άποψη αυτή υπήρξε η γνωμοδότηση υπ’ αριθμόν 6/18.02.2021 ΑΠ, σύμφωνα με την οποία ο αντιεισαγγελέας του Αρείου Πάγου, κατόπιν σχετικού ερωτήματος που του απευθύνθηκε αποφάνθηκε πως, τα άυλα ψηφιακά δεδομένα που είναι αποθηκευμένα σε ένα σύστημα ή σε ένα μέσο αποθήκευσης δεδομένων ή σε ένα απομακρυσμένο σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού ή σε ένα απομακρυσμένο μέσο αποθήκευσης υπολογιστή, αποτελούν μέρος του υλικού φορέα στον οποίο εμπεριέχονται, είτε πρόκειται για σύστημα υπολογιστή είτε για μέσο αποθήκευσης, από τη φύση δε του πράγματος και κατά λογική ακολουθία, τα ψηφιακά δεδομένα κατάσχονται ταυτόχρονα με τον περιέκτη υλικό

φορέα, ανεξάρτητα από το είδος και την μορφή του, χωρίς να συντρέχει περίπτωση διακριτής κατάσχεσής τους.[24]

Στη συνέχεια, άξιο επισήμανσης στα πλαίσια της πρώτης παραγράφου του άρθρου 265 ΚΠΔ, συνιστά το γεγονός πως δίνεται στις αρχές η δυνατότητα, να προβούν σε κατάσχεση «ψηφιακών δεδομένων σε ένα απομακρυσμένο σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού, καθώς και σε ένα απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή και στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτό», δίνεται δηλαδή η δυνατότητα στις ανακριτικές Αρχές να προβαίνουν σε κατάσχεση ψηφιακών δεδομένων, χωρίς να έρχονται σε φυσική – άμεση επαφή με τον υλικό φορέα στον οποίο αυτά ενσωματώνονται.

Η δυνατότητα αυτή που δίνεται στις ανακριτικές Αρχές, να διεισδύουν σε ψηφιακά δεδομένα που βρίσκονται αποθηκευμένα σε ένα απομακρυσμένο υλικό μέσο αποθήκευσης ή ακόμη και σε ψηφιακά δεδομένα που δεν ενσωματώνονται σε κάποιον υλικό φορέα, μέσω κάποιου συστήματος VPN (Virtual Private Network), το οποίο συνιστά ένα δίκτυο που χρησιμοποιεί κατά κύριο λόγο δημόσια τηλεπικοινωνιακή υποδομή, όπως το Διαδίκτυο, και δίνει τη δυνατότητα σε απομακρυσμένα γραφεία ή σε χρήστες που ταξιδεύουν να έχουν πρόσβαση σε ένα κεντρικό οργανωτικό δίκτυο, ή κάποιας άλλης αντίστοιχης τεχνολογίας συνιστά αρχικά μία καινοτόμο διαδικασία διενέργειας των ανακριτικών πράξεων, κατά την εκτέλεση των οποίων δεν θα χρειάζεται να τηρούνται οι ιδιαίτερες διατυπώσεις των άρθρων 253 επ. ΚΠΔ που αφορούν προϋποθέσεις για τη διενέργεια ερευνών – ειδικών ανακριτικών πράξεων, αλλά ταυτόχρονα συνεπάγεται και την επάνδρωση των ανακριτικών αρχών με προσωπικό που φέρει ειδικές γνώσεις τεχνολογίας και με ειδικό εξοπλισμό για την ασφαλή εξαγωγή, επεξεργασία και αποθήκευση των ως άνω δεδομένων.

Αναφορικά δε με την ορθή αναγνώριση, διαλογή, συλλογή και διατήρηση ψηφιακών τεκμηρίων, έχουν διατυπωθεί κάποιες πρακτικές και κατευθυντήριες οδηγίες οι οποίες εν μέρει έχουν αποτυπωθεί στο διεθνές πρότυπο ISO/IEC 27037:2012 αναφορικά με την «Αναγνώριση, Διαλογή, Συλλογή και διατήρηση ψηφιακών τεκμηρίων», καθώς και στον οδηγό

[24] Γνωμοδότηση ΑΠ υπ' αριθμόν 6/18.02.2021

ορθής πρακτικής για τις ψηφιακές αποδείξεις που δημοσιεύτηκε στο Ηνωμένο Βασίλειο τον Μάρτιο του 2012 από το Association of Chief Police Officers. Τα πιο πάνω εγχειρίδια παρέχουν οδηγίες, κατευθυντήριες γραμμές και υποστήριξη σε άτομα και οργανισμούς για τον χειρισμό κάθε είδους ψηφιακού τεκμηρίου. Σύμφωνα με το διεθνές πρότυπο ISO/IEC 27037:2012, οι πιο κάτω βασικές αρχές πρέπει να διέπουν τον χειρισμό των ψηφιακών τεκμηρίων, ήτοι α) η Συνάφεια, δηλαδή πρέπει το υλικό που αποκτήθηκε να είναι σχετικό με την έρευνα που διεξάγεται, ήτοι να περιέχει πληροφορίες που ενισχύουν την διεξαγόμενη έρευνα, β) η Αξιοπιστία όπου όλες οι διαδικασίες που χρησιμοποιούνται στο χειρισμό τεκμηρίων πρέπει να είναι ελέγξιμες και επαναλαμβανόμενες, και γ) η Επάρκεια όπου πρέπει να συγκεντρωθεί αρκετό υλικό για να μπορεί να διεξαχθεί μία σωστή έρευνα[25].

Κατά το πρώτο διαδικαστικό στάδιο της αναγνώρισης των πειστηρίων, θα πρέπει αρχικά να διασφαλίζεται πως τηρούνται όλες οι προϋποθέσεις διεξαγωγής σύννομης έρευνας αυτών, όπως οι προϋποθέσεις αυτές διατυπώνονται στο άρθρο 253 ΚΠΔ, ενώ στη συνέχεια θα πρέπει να εντοπιστούν εκείνα τα ψηφιακά δεδομένα τα οποία πρόκειται να διαδραματίσουν κομβικό ρόλο στην πορεία της υπόθεσης για την οποία διενεργείται η έρευνα, να αξιολογείται δηλαδή η αποδεικτική ισχύς που δύνανται να παρουσιάζουν, ενώ προτεραιότητα θα πρέπει να δοθεί στην αναγνώριση και συλλογή των πιο ευάλωτων εξ αυτών, έτσι ώστε να ελαχιστοποιηθεί κατά το δυνατόν η αλλοίωσή τους. Στη συνέχεια, αναφορικά με τη συλλογή των επίμαχων πειστηρίων, δέον να σημειωθεί πως στην περίπτωση που από την έρευνα εντοπιστούν ηλεκτρονικές συσκευές που κρίνεται πως περιέχουν κρίσιμα ψηφιακά δεδομένα, ακολουθείται ανά περίπτωση είτε κατάσχεση του συνόλου του υλικού φορέα, είτε μόνο του ψηφιακού πειστηρίου που εμπεριέχεται σε αυτές, ενώ τέλος δια της διαδικασίας της ανακτήσεως δημιουργείται σύμφωνα με τις επιταγές του νόμου αντίγραφο εκ των κατασχεθέντων ψηφιακών δεδομένων που εμπεριέχονται στον υλικό φορέα, η αντιγραφή αυτή γίνεται

[25] Αναστάσιος Χ. Παπαθανασίου, Αστυνομικός Υποδιευθυντής, ΜΔΕ, ΜΔΕ Πληροφορικής (ΠΑΠΕΙ), ΜΔΕ Ποινικών Επιστημών και Εγκληματολογίας (ΕΚΠΑ), ΜΔΕ Κυβερνοασφάλειας (ΠΑΔΑ), Υπ. ΔΝ Πληροφορικής (ΠΑΠΕΙ), κεφ. «13. Κυβερνοέγκλημα, Ψηφιακή εγκληματικότητα και κατάσχεση ψηφιακών δεδομένων», Ηλεκτρονικό Έγκλημα, Θεοχάρης Ι Δαλακούρας, Εκδ. Νομική Βιβλιοθήκη, σελ. 272.

είτε επί τόπου, είτε κατόπιν μεταφοράς του υλικού φορέα στα εργαστήρια που διαθέτουν οι Αρχές. Τέλος η αποθήκευση και διατήρηση των κατασχεθέντων ψηφιακών πειστηρίων, θα πρέπει να γίνεται με απόλυτο γνώμονα την ασφαλή και αναλλοίωτη διατήρηση αυτών, σύμφωνα με τις επιταγές του νόμου.

Ρητά στη διάταξη της πρώτης παραγράφου του ως άνω άρθρου δε, ορίζεται πως, «*τα ψηφιακά δεδομένα που είναι αποθηκευμένα και προσβάσιμα μέσω συστήματος και υπηρεσιών νεφοϋπολογιστικής (cloud services) δεν θεωρούνται αποθηκευμένα σε απομακρυσμένο σύστημα υπολογιστή ή σε απομακρυσμένο μέσο αποθήκευσης δεδομένων υπολογιστή τα οποία είναι διασυνδεδεμένα στο σύστημα υπολογιστή στο οποίο έχουν φυσική πρόσβαση οι αρχές».* Δυνάμει των ως άνω συνάγεται πως, οποιοδήποτε ψηφιακό δεδομένο βρίσκεται ανεβασμένο και αποθηκευμένο σε οποιαδήποτε υπηρεσία cloud δεν θεωρείται ως φυσικά προσβάσιμο από τις Αρχές. Τίθεται λοιπόν το ερώτημα εάν αυτό το ψηφιακό υλικό, ως μη φυσικά προσβάσιμο από τις αρχές, υπόκειται η μη σε κατάσχεση. Η απάντηση είναι μάλλον καταφατική, διότι άλλως δεν θα υπήρχε ανάγκη να τοποθετηθεί ως υποπερίπτωση της παραγράφου, που αναφέρεται σε ποια ψηφιακά δεδομένα μπορεί να επιβληθεί κατάσχεση. Άρα και γραμματικά και λογικοσυστηματικά προκύπτει ότι η πρόθεση του νομοθέτη ήταν και τα δεδομένα αυτά να υπόκειται σε ψηφιακή κατάσχεση, απλώς τα αντιδιαστέλλει από τις προηγούμενες περιπτώσεις κατά τις οποίες οι αρχές πράγματι έχουν φυσική πρόσβαση στα δεδομένα η θεωρείται κατά πλάσμα δικαίου ότι έχουν φυσική πρόσβαση σε αυτά διότι θέλει να τους προσδώσει μεγαλύτερη προστασία. Η ανάγκη μεγαλύτερης προστασίας δικαιολογείται από την μεγαλύτερη ευαλωτότητά τους, καθώς τα δεδομένα αυτά κυκλοφορούν άυλα σε παγκόσμιο επίπεδο και με τον τρόπο αυτό είναι πολλαπλώς πιο ευάλωτα σε οποιαδήποτε απομακρυσμένη πρόσβαση ανά τον κόσμο άρα και αλλοίωση και καταστροφή. Έτσι αντιμετωπίζονται στην ελληνική έννομη τάξη νομικά ισάξια με τα λεγόμενα δεδομένα κίνηση σε πραγματικό χρόνο και τα δεδομένα επικοινωνίας, τα οποία προστατεύονται ως απόρρητα. Το ως άνω σημαίνει ότι προτού αυτά τύχουν αρχικά έρευνας και μετέπειτα ψηφιακής κατάσχεσης από τις αρχές

θα πρέπει να έχει προηγηθεί οπωσδήποτε η διαδικασία της άρσης του απορρήτου όπως αυτή προβλέπεται στα άρθρα 4 και 5 του ν. 2225 / 1994.[26]

Συνεπώς στην περίπτωση όπου από τις αρμόδιες ανακριτικές αρχές κριθεί απαραίτητο να προβούν σε κατάσχεση ψηφιακών δεδομένων που βρίσκονται αποθηκευμένα σε cloud services, θα πρέπει αυτές να προβαίνουν αρχικώς στη διαδικασία της άρσης απορρήτου και στη συνέχεια στην κατάσχεση και αξιοποίηση των ως άνω δεδομένων.

Ακολούθως, στη δεύτερη παράγραφο του υπό ανάλυση άρθρου 265 ΚΠΔ, αναφέρεται πως *«Η κατά τα ανωτέρω κατάσχεση πραγματοποιείται αποκλειστικά με τη χρήση κατάλληλου εξοπλισμού που επιτρέπει σε εκείνον που τη διεξάγει: α) Την αφαίρεση και την κατάσχεση του υλικού φορέα των υπό στοιχείων α-γ της παρ. 1, στο οποίο βρίσκονται αποθηκευμένα τα δεδομένα και/ή β) την αντιγραφή και την αφαίρεση των αποθηκευμένων ψηφιακών δεδομένων των υπό στοιχείων α-γ της παρ. 1 σε μέσο αποθήκευσης δεδομένων και γ) την αναπαραγωγή και την επαλήθευση της αυθεντικότητας και της ακεραιότητας των κατασχεθέντων δεδομένων.*

Από τη διατύπωση της δεύτερης αυτής παραγράφου του άρθρου 265 ΚΠΔ, καταδεικνύεται η ιδιαίτερη μέριμνα του νομοθέτη και η ανάγκη αυτού να εξασφαλίσει την ορθή αφαίρεση, αντιγραφή και αναπαραγωγή των κατασχεθέντων ψηφιακών δεδομένων, από πλευράς των ανακριτικών αρχών. Ο νομοθέτης αντιλαμβάνεται την ιδιαίτερη και ευαίσθητη φύση των ψηφιακών δεδομένων, τα οποία δύνανται εύκολα λόγω της φύσης τους να αλλοιωθούν, να παραποιηθούν ή ακόμη και να εξαφανιστούν συνεπεία κάποιου εσφαλμένου χειρισμού ή λόγω έλλειψης υλικοτεχνικών υποδομών από πλευράς των ανακριτικών Αρχών. Μια τέτοια εξέλιξη, είναι φανερό, πως θα καθίστατο καταστροφική, τόσο για τη συλλογή των πειστηρίων του εγκλήματος και την κατάφαση ή μη της τέλεσης αυτού (του εγκλήματος) ή της διάπραξης από τον συγκεκριμένο δράστη, όσο και για το γεγονός πως στα ψηφιακά αυτά δεδομένα ενδεχομένως να «κρύβεται» η υπερασπιστική γραμμή του κατηγορουμένου και η απόδειξη της αθωότητας του.

[26] Μαριάννα Κουδελή, Στρατιωτικός Δικαστής, Ζητήματα που άπτονται της κατάσχεσης ψηφιακών δεδομένων του άρθρου 265 του ΚΠΔ, Ηλεκτρονικό Έγκλημα, Θεοχάρης Ι Δαλακούρας, Εκδ. Νομική Βιβλιοθήκη, σελ. 528.

Για την επίτευξη όμως των ανωτέρω, ήτοι για την προσήκουσα αφαίρεση, αντιγραφή και αναπαραγωγή των ψηφιακών δεδομένων θα πρέπει τα αρμόδια τμήματα των ανακριτικών Αρχών να εφοδιαστούν με την απαραίτητη υλικοτεχνική υποδομή, καθώς και να προβούν σε προσλήψεις ατόμων και προσωπικού με ειδικές τεχνικές γνώσεις και εμπειρία επί του γνωστικού αντικειμένου της επιστήμης της πληροφορικής. Όλα τα ως άνω όμως συνεπάγονται κονδύλια, χρόνο και διαρκή επιμόρφωση των ανακριτικών Αρχών, προϋποθέσεις που ενδεχομένων να συνιστούν ανατρεπτικούς παράγοντες για την συχνότερη και τακτικότερη θέση σε εφαρμογή της διάταξης του άρθρου 265 ΚΠΔ στην πράξη.

Στο σημείο αυτό και στο θεωρητικό ερώτημα του αν κατά τη διάρκεια προσπάθειας των ανακριτικών αρχών να προβούν, χρησιμοποιώντας τα τεχνικά μέσα που διαθέτουν, σε κατάσχεση και αντιγραφή των ψηφιακών δεδομένων του υπόπτου ή του κατηγορουμένου, ζητήσουν από τον τελευταίο να τους συνδράμει παραχωρώντας τους, τους προσωπικούς κωδικούς ασφαλείας που είχε θέσει για την πρόσβαση στα ως άνω δεδομένα, μπορεί ο τελευταίος να αρνηθεί, η απάντηση που φαντάζει ως ορθότερη είναι πως δύναται να αρνηθεί να παραχωρήσει τους προσωπικούς του κωδικούς ασφαλείας, χωρίς αυτό να θεωρηθεί απείθεια απέναντι στις Αρχές ή στοιχείο αποδεικτικό της ενοχής του, αντιθέτως δε συνιστά νόμιμο δικαίωμά του που αποτελεί έκφραση της αρχής της μη αυτοενοχοποίησης του δράστη, που διέπει το σύνολο της ποινικής διαδικασίας.

Συνεχίζοντας, από τη διάταξη της τρίτης παραγράφου του άρθρου 265 ΚΠΔ, ορίζεται πως *«η κατάσχεση που διενεργείται κατά τις παρ. 1 και 2, βεβαιώνεται με ειδική έκθεση, η οποία αναφέρει ειδικώς τις ενέργειες της παρ. 2 που πραγματοποιεί εκείνος που διεξάγει την ανάκριση».* Από τα οριζόμενα στη διάταξη του ως άνω άρθρου συνάγεται πως ο διενεργών την ανάκριση οφείλει μετά την ολοκλήρωση της ανακριτικής πράξεως της κατάσχεσης, να συντάξει αναλυτική έκθεση στην οποία θα περιγράφει τις ενέργειες στις οποίες αυτός προέβη κατά τη διενέργεια της κατασχέσεως, ήτοι τις ενέργειες στις οποίες προέβη για την αφαίρεση και κατάσχεση του υλικού φορέα των ψηφιακών δεδομένων, για την αντιγραφή και αφαίρεση των ίδιων των ψηφιακών δεδομένων καθώς και τις ενέργειες στις οποίες προέβη για την αναπαραγωγή και επαλήθευση της αυθεντικότητας και της

ακεραιότητας των κατασχεθέντων ψηφιακών δεδομένων. Το ως άνω συνιστά ειδικότερη περίπτωση του άρθρου 241 εδ. γ ΚΠΔ, όπου ορίζεται πως, «για κάθε ανακριτική πράξη συντάσσεται έκθεση σύμφωνα με τους νόμιμους τύπους», και αποτελεί έκφανση της αρχής της μυστικότητας που διέπει την προδικασία, με την ταυτόχρονη διασφάλιση της αξιοπιστίας των διαδικασιών που ακολουθούνται, τα αποτελέσματα των οποίων θα διαδραματίσουν κομβικό ρόλο για την πορεία της ποινικής υποθέσεως.

Συνάγεται λοιπόν πως ο νομοθέτης θέτει ως προϋπόθεση της νομίμου διαδικασίας της κατάσχεσης ψηφιακών δεδομένων την σύνταξη, μετά την ολοκλήρωση αυτής (της κατασχέσεως), από πλευράς ανακριτικών αρχών ειδικής και εμπεριστατωμένης εκθέσεως, στην οποία θα παρατίθενται όλες εκείνες οι ενέργειες στις οποίες προέβησαν τα ανακριτικά όργανα από την αρχή και μέχρι την ολοκλήρωση της κατάσχεσης ψηφιακών δεδομένων. Η πρόβλεψη αυτή τίθεται προκειμένου να διασφαλίζεται η ορθότητα της διαδικασίας που ακολουθήθηκε κατά την επιχείρηση κατάσχεσης των ψηφιακών δεδομένων, καθώς λόγω της ιδιαίτερης και ευάλωτης φύσης τους, που κάνει την αλλοίωση, την παραποίηση και την καταστροφή τους ιδιαιτέρως εύκολη, συχνά θα μπορούσε να παρατηρηθεί το φαινόμενο της αμφισβήτησης των εξαχθέντων αποτελεσμάτων και της δημιουργίας του αισθήματος ανασφάλειας δικαίου και μη ορθής απονομής δικαιοσύνης.

Μάλιστα, εφόσον από τη διάταξη του άρθρου 266 ΚΠΔ, ορίζεται πως κατάσχεση μπορεί να διαταχθεί από το δικαστήριο σε κάθε στάδιο της δίκης και αυτεπαγγέλτως, συνάγεται πως αν της κατασχέσεως ψηφιακών δεδομένων, ακολουθήσει δεύτερη συμπληρωματική τέτοια κατάσχεση, δέον να ακολουθήσει και η σύνταξη δεύτερης συμπληρωματικής ειδικής έκθεσης του άρθρου 255 παρ. 3 ΚΠΔ. Η ανάγκη προς σύνταξη τέτοιας δεύτερης συμπληρωματικής εκθέσεως, συνάγεται από το πνεύμα του άρθρου 255 παρ. 3 ΚΠΔ, ήτοι από την ανάγκη του νομοθέτη να διασφαλίσει πως θα τηρηθούν όλες οι απαραίτητες προβλέψεις για την ορθή εφαρμογή των επιταγών του άρθρου 265 ΚΠΔ, αναφορικά με την διαδικασία κατάσχεσης, συλλογής και αξιοποίησης των ψηφιακών δεδομένων, που συνιστούν αντικείμενο του εγκλήματος και της ποινικής διαδικασίας εν τω συνόλω.

Στο σημείο αυτό άξια αναφοράς είναι η θέση που υποστηρίχθηκε δια της υπ' αριθμόν 6/2021 Γνωμοδοτήσεως του Αρείου Πάγου, με την οποία υποστηρίχθηκε η θέση «πως τα άυλα ψηφιακά δεδομένα που είναι αποθηκευμένα σε ένα σύστημα ή σε ένα μέσο αποθήκευσης δεδομένων ή σε ένα απομακρυσμένο σύστημα υπολογιστή στο σύνολό του ή σε μέρος αυτού ή σε ένα απομακρυσμένο μέσο αποθήκευσης υπολογιστή, αποτελούν μέρος του υλικού φορέα στον οποίο εμπεριέχονται, είτε πρόκειται για σύστημα υπολογιστή είτε για μέσο αποθήκευσης, από τη φύση δε του πράγματος και κατά λογική ακολουθία, τα ψηφιακά δεδομένα κατάσχονται ταυτόχρονα με τον περιέκτη υλικό φορέα, ανεξάρτητα από το είδος και την μορφή του, χωρίς να συντρέχει περίπτωση διακριτής κατάσχεσής τους και σύνταξης σε μεταγενέστερο χρόνο και διαφορετικό τρόπο ιδιαίτερης, εκτός αυτής που αφορά τον υλικό φορέα τους, σχετικής έκθεσης, συνακόλουθα δε ουδεμία ακυρότητα της συγκεκριμένης ανακριτικής πράξης, συναπτόμενη με τη νομιμότητα των κτηθέντων ως άνω αποδεικτικών μέσων, υπόκειται».[27] Από τα οριζόμενα στην ως άνω γνωμοδότηση του Αρείου Πάγου, συνάγεται πως κατόπιν σχετικού ερωτήματος που απευθύνθηκε στον Άρειο Πάγο, ο τελευταίος αποφάνθηκε πως όταν συντρέχει περίπτωση ταυτόχρονης κατασχέσεως του υλικού φορέα και τον άυλου ψηφιακού δεδομένου που ενσωματώνεται σε αυτόν, μόνη η έκθεση κατάσχεσης του υλικού φορέα καλύπτει και την κατάσχεση του άυλου ψηφιακού δεδομένου, χωρίς να συντρέχει ανάγκη και συνακόλουθος κίνδυνος δικονομικής ακυρότητας, αν παραληφθεί η παράλληλη σύνταξη της ειδικής εκθέσεως του άρ. 255 ΚΠΔ. Η θέση αυτή του Αρείου Πάγου, αμφισβητείται από άποψη δικονομικής ορθότητας, καθώς η υποχρέωση συντάξεως ειδικής έκθεσης κατάσχεσης στην περίπτωση κατάσχεσης ψηφιακών δεδομένων, πηγάζει ρητά από διάταξη νόμου (265 παρ. 3 ΚΠΔ) και από την προστασία της ιδιαίτερης φύσης των ψηφιακών δεδομένων. Εξάλλου η διακριτή φύση των ψηφιακών δεδομένων και του ενσώματου υλικού φορέα στον οποίο αυτά συνήθως περιέχονται, καταδεικνύεται από την ίδια την ξεχωριστή διάταξη νόμου που προβλέπει για αυτά (τα ψηφιακά δεδομένα) ειδικά.

Μετά το πέρας της διαδικασίας κατασχέσεως των ψηφιακών δεδομένων, προκειμένου να επιτευχθεί η αξιοποίηση αυτών, θα πρέπει να διεξαχθούν ορισμένες εργαστηριακές αναλύσεις και διατυπώσεις. Η ως

[27] Γνωμοδότηση ΑΠ υπ' αριθμόν 6/18.02.2021

άνω διαδικασία, ήτοι η εξέταση, επεξεργασία και ανάλυση των κατασχεθέντων ψηφιακών δεδομένων, με απώτερο σκοπό την σύνταξη εκθέσεως πραγματογνωμοσύνης, η οποία θα προσκομισθεί στις αρμόδιες Αρχές προκειμένου να αξιοποιηθεί επί της επίδικης υποθέσεως, ανατέθηκε δυνάμει του άρ. 30 του υπ΄ αριθμόν 178/2014 ΠΔ, αναφορικά με την «Οργάνωση Υπηρεσιών Ελληνικής Αστυνομίας» (όπως τροποποιήθηκε και ισχύει σήμερα), στο «Τμήμα Εξέτασης Ψηφιακών Πειστηρίων» της Διεύθυνσης Εγκληματολογικών Ερευνών. Το ως άνω Τμήμα, στα πλαίσια των αρμοδιοτήτων που του έχουν ανατεθεί, ενεργεί επί των κατασχεθέντων ψηφιακών δεδομένων, μεταξύ άλλων, ανάγνωση, ανάκτηση - επαναφορά, εξέταση, αποκρυπτογράφηση, ανάλυση, σύγκριση, επεξεργασία, καταγραφή δεδομένων ευρισκομένων σε αποθηκευτικούς ψηφιακούς χώρους τοπικών δικτύων ηλεκτρονικών υπολογιστών και περιφερειακών ή άλλων ειδικών σταθερών ή φορητών μέσων ψηφιακής αποθήκευσης δεδομένων, αποφαίνεται για τον τρόπο λειτουργίας λογισμικού ή ψηφιακού υλικού, διαπιστώνει την αλληλουχία των ενεργειών χρήσης λογισμικού ή υλικού και ενεργεί εξετάσεις για την εξακρίβωση του δημιουργού ή του χρήστη εφαρμογών ή δεδομένων επί ψηφιακών πειστηρίων, που είναι πρόσφορα προς ανάγνωση, ενεργεί εξετάσεις επί ηλεκτρονικών συσκευών ή άλλων ειδικών ηλεκτρονικών διατάξεων, οι οποίες είναι δυνατόν να αποθηκεύουν ψηφιακά δεδομένα, ενεργεί εξετάσεις επί κινητών τηλεφώνων και συσκευών εντοπισμού θέσης, ενεργεί εξειδικευμένες εξετάσεις, ανάγνωσης, ανάκτησης και αναλύσεις ψηφιακών δεδομένων επί τραπεζικών ή άλλων καρτών, ενεργεί εξετάσεις σε συστήματα τηλεπικοινωνιών, σε συσκευές λήψης δορυφορικού τηλεοπτικού ή αλλού σήματος τα οποία περιέχουν ψηφιακά δεδομένα προσφορά προς ανάγνωση κ.α.[28]

Στη συνέχεια, στην τέταρτη παράγραφο του υπό ανάλυση νέου άρθρου 265 ΚΠΔ, ορίζεται πως, «*Τα ψηφιακά δεδομένα που κατάσχονται διατηρούνται αποθηκευμένα καθ' όλη τη διάρκεια της ποινικής διαδικασίας σε ένα και μόνο υλικό μέσο αποθήκευσης που περιέχεται στη δικογραφία.*

[28] Αναστάσιος Χ. Παπαθανασίου, Αστυνομικός Υποδιευθυντής, ΜΔΕ, ΜΔΕ Πληροφορικής (ΠΑΠΕΙ), ΜΔΕ Ποινικών Επιστημών και Εγκληματολογίας (ΕΚΠΑ), ΜΔΕ Κυβερνοασφάλειας (ΠΑΔΑ), Υπ. ΔΝ Πληροφορικής (ΠΑΠΕΙ), κεφ. «13. Κυβερνοέγκλημα, Ψηφιακή εγκληματικότητα και κατάσχεση ψηφιακών δεδομένων», Ηλεκτρονικό Έγκλημα, Θεοχάρης Ι Δαλακούρας, Εκδ. Νομική Βιβλιοθήκη, σελ. 285 – 286.

Ασφαλές αντίγραφο αυτού ώστε να διασφαλίζεται η δυνατότητα ανάκτησης των δεδομένων που έχουν κατασχεθεί, σε περίπτωση απώλειας ή καταστροφής, σχηματίζεται κατά την κατάσχεσή τους και διατηρείται στο γραφείο πειστηρίων του πρωτοδικείου στο οποίο υποβάλλεται η δικογραφία και το οποίο παρέχει τις κατάλληλες εγγυήσεις φυσικής ασφάλειας και πρόσβασης σε εκείνους μόνο που ασκούν καθήκοντα στην υπόθεση. Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία.». Τα οριζόμενα στην ως άνω διάταξη, αναφορικά με την τήρηση και την φύλαξη των κατασχεθέντων ψηφιακών δεδομένων, συνιστούν μια ειδικότερη ρύθμιση του άρθρου 268 ΚΠΔ, που αφορά στην φύλαξη και στη σφράγιση των κατασχεθέντων ενσώματων – υλικών αντικειμένων και στον ορισμό μεσεγγυούχου. Εκ πρώτης όψεως και εκτιμήσεως, και αφού λάβει κανείς υπόψιν την ιδιαίτερή και άυλη φύση των κατασχεθέντων ψηφιακών δεδομένων, θα αποφανθεί πως εκ φύσεως είναι ασυμβίβαστα με τον θεσμό της μεσεγγύησης και πως η διάταξη αυτή δεν χωρεί εφαρμογής στην περίπτωση του του άρθρου 265 ΚΠΔ, καθώς τα ψηφιακά δεδομένα παραμένουν πάντοτε στη σφαίρα ελέγχου και κατοχής των αρμοδίων ανακριτικών αρχών και δεν παραδίδονται σε τρίτα πρόσωπα. Διαστέλλοντας όμως την οπτική μας επί του θέματος, και σκεπτόμενοι πως τα άυλα ψηφιακά δεδομένα, συνήθως εμπεριέχονται και ενσωματώνονται σε υλικούς φορείς, θα μπορούσε κανείς να καταλήξει στο συμπέρασμα πως, η διάταξη του άρθρου 268 ΚΠΔ, θα μπορούσε να τύχει αναλογικής εφαρμογής και στην περίπτωση των άυλων ψηφιακών δεδομένων, στην περίπτωση που για παράδειγμα ένας φορητός υπολογιστής, που εμπεριέχει τα κρίσιμα για την ποινική υπόθεση ψηφιακά δεδομένα, μπορεί, αν δεν συντρέχει περίπτωση περαιτέρω εξέτασής του, να παραδοθεί προς φύλαξη σε έναν έμπιστο μεσεγγυούχο. Ως τέτοιος (μεσεγγυούχος) θα μπορούσε να θεωρηθεί, ο ανακριτικός υπάλληλος, το δικαστικό συμβούλιο, ο γραμματέας, ενώ δεν αποκλείεται να αποδοθεί η ιδιότητα του μεσεγγυούχου και στον ίδιο των ύποπτο ή τον κατηγορούμενο. Σε κάθε περίπτωση, ο μεσεγγυούχος περιορίζεται στην φύλαξη του πράγματος, το οποίο υποχρεούται να παραδώσει οποτεδήποτε ζητηθεί από την δικαστική

αρχή, ενώ επί καταστροφής, βλάβης η υφαίρεσης του πράγματος απειλείται η ποινική κίρρωση του άρθρου 177 ΠΚ. [29]

Επιπρόσθετα στην παράγραφο πέντε (5) του ως άνω άρθρου 265 ΚΠΔ, ορίζεται πως *«Η πρόσβαση και η δυνατότητα αναπαραγωγής των ψηφιακών δεδομένων που κατάσχονται επιτρέπεται μόνο σε όσους ασκούν δικαστικά, εισαγγελικά και ανακριτικά καθήκοντα στην υπόθεση ή τους γραμματείς. Προς το σκοπό αυτό χρησιμοποιούνται τα κατάλληλα τεχνικά μέσα. Τέτοια μέσα είναι η κρυπτογράφηση και η χρήση κωδικών ασφαλείας για την πρόσβαση και αναπαραγωγή των κατασχεμένων ψηφιακών δεδομένων από το υλικό μέσο αποθήκευσης στο οποίο βρίσκονται αποθηκευμένα. Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία.»,* ενώ στην παράγραφο έξι (6) του ίδιου ως άνω άρθρου ορίζεται πως, « *Απαγορεύεται η δημιουργία και η διατήρηση αντιγράφων των ψηφιακών δεδομένων για οποιονδήποτε άλλον λόγο εκτός αν ο αρμόδιος εισαγγελέας ή ανακριτής ή συμβούλιο ή το δικαστήριο κρίνουν ότι τα κατασχεμένα ψηφιακά δεδομένα είναι αναγκαίο να περιληφθούν σε άλλη δικογραφία. Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία».*

Στις τις δύο τελευταίες παραγράφους του άρθρου 265 ΚΠΔ ορίζονται περιοριστικά τα πρόσωπα τα οποία τα οποία δύνανται να έχουν πρόσβαση στα κατασχεθέντα ψηφιακά μέσα μετά την ολοκλήρωση της διαδικασίας κατασχέσεώς τους από τις αρμόδιες ανακριτικές αρχές, καθώς τα ειδικά και συγκεκριμένα μέσα που δύνανται να χρησιμοποιούνται από τα ως άνω πρόσωπα κατά τη διάρκεια της πρόσβασής τους σε αυτά, ενώ τέλος ορίζονται περιοριστικά οι περιπτώσεις εκείνες κατά τις οποίες δύναται να δημιουργηθεί και να διατηρηθεί αντίγραφο εκ των κατασχεθέντων ψηφιακών δεδομένων.

Ερώτημα στο σημείο αυτό τίθεται για το αν υπάρχει η δυνατότητα των διαδίκων και κυρίως του υπόπτου – κατηγορουμένου πρόσβασης και λήψης αντιγράφων από το κρίσιμο ψηφιακό αποδεικτικό υλικό, καθώς από την διατύπωση των παραγράφων 5 και 6 του άρθρου 265 ΚΠΔ, μπορεί

[29] Γιάννης Ναζίρης, Επίκουρος Καθηγητής ΑΠΘ, Δικηγόρος, ΠοινΔικ, [Νομική Βιβλιοθήκη], ISSN:1108-2755, τομ.24 τευχ.247 [2021] σελ.178-194.

κανείς να δημιουργήσει ερμηνευτική σύγχυση ως προς την δυνατότητα ή μη των διαδίκων να έχουν πρόσβαση σε αυτά. Και αυτό γιατί στις εν λόγω παραγράφους γίνεται ρητή αναφορά σε δυνατότητα πρόσβασης και αναπαραγωγής δεδομένων και δημιουργίας αντιγράφων που συνοδεύουν την δικογραφία μόνο σε όσους ασκούν δικαστικά, εισαγγελικά και ανακριτικά καθήκοντα στην υπόθεση ή στους γραμματείς. Σε μία πρώτη ανάγνωση, η γραμματική αυτή διατύπωση, δεν αφήνει κανένα περιθώριο διαφορετικής ερμηνείας περί των προσώπων που έχουν δυνατότητα πρόσβασης σε αυτά. Είναι φανερό όμως, ότι, ενόψει των διατάξεων των άρθρων 100 ΚΠΔ και 107 ΚΠΔ, αλλά και του άρθρου 244 παρ. 1 εδ. β' ΚΠΔ, τα οποία διασφαλίζουν το θεμελιώδες δικαίωμα πρόσβασης στο σύνολο της δικογραφίας, αφενός για τον κατηγορούμενο, αφετέρου για τον παριστάμενο προς υποστήριξη της κατηγορίας, δε νοείται απαγόρευση πρόσβασης και λήψης αντιγράφου των ψηφιακών δεδομένων της δικογραφίας για τους διαδίκους, από το χρονικό σημείο που για τον καθένα από αυτούς, από τα ως άνω άρθρα επιτρέπεται, όπως και από το λοιπό δηλαδή μη ψηφιακό υλικό της δικογραφίας. Μία ερμηνεία που θα απέκλειε τη δυνατότητα πρόσβασης σε αυτό θα ήταν εξάλλου ευθέως αντίθετη, ιδίως αναφορικά με την περίπτωση του κατηγορουμένου, με το άρθρο 6 παρ. 1 και 3 στ. α' και β' της ΕΣΔΑ.[30] Ο σκοπός εξάλλου του νομοθέτη του νέου άρθρου 265 ΚΠΔ δεν τεκμαίρεται πως ήταν ο περιορισμός των δικαιωμάτων που απολαμβάνει ο κατηγορούμενος δυνάμει των λοιπών άρθρων του Κώδικα Ποινικής Δικονομίας, αντιθέτως μάλιστα ο σκοπός που φέρεται να είχε, και ο οποίος σκοπός διατρέχει το σύνολο του χαρακτήρα του νέου άρθρου 265 ΚΠΔ, δεν είναι άλλος από την προστατευτική του διάθεση απέναντι στον ιδιαίτερο και ευαίσθητο χαρακτήρα της φύσης των ψηφιακών δεδομένων. Πρόθεση συνεπώς του νομοθέτη, μέσα από την περιοριστική απαρίθμηση των ατόμων που θα έχουν πρόσβαση στα κατασχεθέντα ψηφιακά δεδομένα συνιστά η προστασία τους από οποιαδήποτε αλλοίωση, παραποίηση και καταστροφή, με απώτερο σκοπό την ορθή απονομή δικαιοσύνης και της διατήρησης όλων των διατυπώσεων της δίκαιης δίκης.

Μια διαφορετική πάντως προσέγγιση από αυτήν που επιλέχθηκε από τον νομοθέτη, με σκοπό τη διασφάλιση των κατασχεθέντων ψηφιακών

[30] Μαριάννα Κουδελή, Στρατιωτικός Δικαστής, Ζητήματα που άπτονται της κατάσχεσης ψηφιακών δεδομένων του άρθρου 265 του ΚΠΔ, Ηλεκτρονικό έγκλημα, επιμέλεια Θεοχάρης Ι Δαλακούρας, σελ. 528.

δεδομένων και της «εύθραυστης» φύσης αυτών, θα μπορούσε να αποτελέσει, όχι η εξαντλητική απαρίθμηση των ατόμων που δύνανται να έχουν πρόσβαση στα δεδομένα αυτά, αλλά ο ορισμός των προϋποθέσεων και η ανάθεση της δυνατότητας δημιουργίας και χορήγησης αντιγράφων σε μια ειδική ομάδα δικαστηριακών υπαλλήλων, που θα φέρουν εξειδικευμένες τεχνικές γνώσεις, και την ταυτόχρονη φερεγγυότητα και αξιοπιστία των δημοσίων υπαλλήλων, ώστε να δημιουργούν αντίγραφα ψηφιακών δεδομένων, χωρίς να κινδυνεύουν να καταστραφούν ή να αλλοιωθούν τα πρωτότυπα που φυλάσσονται. Με τον τρόπο αυτόν θα υπήρχε «ισάξια» δικονομική αντιμετώπιση των υλικών και των άυλων ψηφιακών δεδομένων, με την παράλληλη εξασφάλιση της ιδιαίτερης φύσης και της ευαλωτότητας των τελευταίων.

4. Ελλείψεις του νέου άρθρου 265 ΚΠΔ

Διατρέχοντας τη γραμματική διατύπωση του άρθρου 265 ΚΠΔ, καθώς και τις λοιπές διατάξεις του Τρίτου Κεφαλαίου του Δεύτερου Τμήματος του Κώδικα Ποινικής Δικονομίας, διαπιστώνουμε πως, δεν έχει τεθεί από τον νομοθέτη πρόβλεψη αναφορικά με την τύχη των κατασχεθέντων ψηφιακών δεδομένων, μετά το πέρας της ποινικής διαδικασίας και της έκδοσης της «τελειωτικής απόφασης», καθώς επίσης και πρόβλεψη ανάλογη της διάταξης του άρθρου 269 παρ. 3 ΚΠΔ για την δυνατότητα άρσης της κατασχέσεως που έχει επιβληθεί επί ψηφιακών δεδομένων.

Από τη διάταξη του άρθρου 266 παρ. 2 εδ. β’ ορίζεται πως, «Για την τύχη των πραγμάτων ή των εγγράφων που κατασχέθηκαν, αποφασίζει το δικαστήριο σύμφωνα με το άρθρο 372 ΚΠΔ», ενώ από τη διάταξη του άρθρου 372 ΚΠΔ ορίζεται πως «Με την τελειωτική απόφαση οι διάδικοι που ηττήθηκαν στη δική καταδικάζονται στα έξοδα. Με την ίδια απόφαση το δικαστήριο διατάσσει να αποδοθούν στον ιδιοκτήτη τα πράγματα που αφαιρέθηκαν και τα πειστήρια, όσα κατασχέθηκαν ή παραδόθηκαν κατά την ανάκριση και δεν έγινε άρση της κατάσχεσης τους σύμφωνα με το άρθρο 269. Διατάσσει επίσης την δήμευση των αντικειμένων που πρέπει να δημευτούν».

Αρχικά, αναφορικά με τη διάταξη του άρθρου 269 παρ. 3 ΚΠΔ, όπου ορίζεται πως, «σε κάθε περίπτωση το δικαστικό συμβούλιο ή το δικαστήριο μπορεί να διατάξει να αρθεί η κατάσχεση, αν δεν είναι πιθανόν ότι από αυτό το λόγο θα δημιουργηθούν δυσχέρειες στην εξακρίβωση της αλήθειας», και της δυνατότητας ή μη να τύχει αναλογικής εφαρμογής στην περίπτωση κατάσχεσης άυλων ψηφιακών δεδομένων, ορίζεται πως η ιδιαίτερη φύση των ψηφιακών δεδομένων, με τον άυλο χαρακτήρα που αυτά φέρουν, έχει ως αποτέλεσμα η αίτηση για άρση της κατασχέσεως, να κινδυνεύει να χαρακτηριστεί ως αίτηση άνευ αντικειμένου. Δεν θα μπορούσε βέβαια να υποστηριχθεί το ίδιο και για τον υλικό φορέα στον οποίο αυτά (τα ψηφιακά δεδομένα) ενσωματώνονται. Σε περίπτωση λοιπόν, όπου έχει τελεστεί «συγκατάσχεση», ήτοι παράλληλη κατάσχεση του υλικού – ενσώματου φορέα – αντικειμένου και των άυλων ψηφιακών δεδομένων, θα μπορούσε δυνάμει αναλογικής εφαρμογής του άρθρου 269 παρ. 3 ΚΠΔ, να ζητηθεί η απόδοση του ενσώματου υλικού αντικειμένου, επί του οποίου ενσωματώνεται το κρίσιμο ψηφιακό δεδομένο. Αναφορικά δε με την περίπτωση των άυλων δεδομένων, κατά διασταλτική ερμηνεία και αναλογική εφαρμογή της διάταξης του άρθρου 269 παρ. 3 ΚΠΔ, θα μπορούσε να ζητηθεί η διαγραφή και καταστροφή των αντιγράφων που δημιουργήθηκαν από τις αρμόδιες ανακριτικές αρχές στα πλαίσια άσκησης των καθηκόντων τους και της εφαρμογής του άρθρου 265 ΚΠΔ. Η πρακτική αυτή θα μπορούσε να αποτελέσει μια πλασματική «άρση κατασχέσεως» για τα άυλα ψηφιακά δεδομένα.

Η ίδια ως άνω συλλογιστική θα τύχει εφαρμογής και για την τύχη των άυλων ψηφιακών δεδομένων, που κατασχέθηκαν από τα αρμόδια ανακριτικά όργανα στα πλαίσια των διαδικασιών του άρθρου 265 ΚΠΔ, μετά το πέρας της ποινικής διαδικασίας και της έκδοσης «τελειωτικής» απόφασης. Τα οριζόμενα στο άρθρο 372 ΚΠΔ, ήτοι η απόδοση στον ιδιοκτήτη τους των πραγμάτων που αφαιρέθηκαν και των πειστηρίων, καθώς και όσων κατασχέθηκαν ή παραδόθηκαν κατά την ανάκριση και δεν έγινε άρση της κατάσχεσης τους σύμφωνα με το άρθρο 269, μπορούν να εφαρμοστούν μόνο επί του υλικού ενσώματου φορέα των κατασχεθέντων ψηφιακών δεδομένων, ενώ ως ήδη ελέχθη, η ως άνω διάταξη δεν μπορεί να εφαρμοστεί, λόγω της άυλης υπόστασής τους, επί των κατασχεθέντων ψηφιακών δεδομένων καθαυτών, παρά μόνο ερμηνευτικά, αναλογικά και διασταλτικά να ζητηθεί η διαγραφή των δημιουργηθέντων αντιγράφων επί του αρχικού ψηφιακού δεδομένου, και η ολική και πλήρης καταστροφή

αυτού, προκειμένου να ειρηνεύσει η ευρύτερη σφαίρα κατοχής και ιδιοκτησίας του κατηγορουμένου.

Η δε πρόβλεψη για τη δήμευση των περιουσιακών στοιχείων του κατηγορουμένου στην περίπτωση της καταδίκης αυτού, όπως ορίζεται στη διάταξη του άρθρου 373 παρ. 3 και 4, όπου ορίζεται πως *« 3. Σε περίπτωση καταδίκης, αν τα δεσμευμένα περιουσιακά στοιχεία προέρχονται άμεσα ή έμμεσα από την αξιόποινη πράξη και συνιστούν την περιουσιακή ζημία που υπέστη το θύμα, αποδίδονται στο τελευταίο. Διαφορετικά διατάσσεται η δήμευσή τους, εφόσον αυτή προβλέπεται από τις κείμενες διατάξεις. 4. Το δικαστήριο μπορεί να περιορίσει τη δήμευση σε μέρος των δεσμευμένων περιουσιακών στοιχείων. Στην περίπτωση αυτή αίρει κατά τα λοιπά τη δέσμευση και διατάσσει κατά το σκέλος της αυτό την απόδοση των περιουσιακών στοιχείων στον ιδιοκτήτη τους.»* και πάλι όπως έχει γίνει αντιληπτό, δεν μπορεί να εφαρμοστεί επί των άυλων ψηφιακών δεδομένων, λόγω της μη υλικής φύσης και υπόστασης αυτών, παρά μόνο επί του υλικού φορέα που τα ενσωματώνει, ακολουθώντας την ίδια ως άνω αναλυθείσα και εκτεθείσα συλλογιστική.

Διαπιστώνουμε λοιπόν, δυνάμει όλων των ως άνω εκτεθέντων, πως τα δικονομικά κενά που καταλείπονται από τη γραμματική διατύπωση του άρθρου 265 ΚΠΔ, που αφορά στην κατάσχεση ψηφιακών δεδομένων, μπορούν ερμηνευτικά και αναλογικά να καλυφθούν, μόνον αναφορικά με τον υλικό φορέα στον οποίο ενσωματώνεται το ψηφιακό δεδομένο, από τη γραμματική διατύπωση των λοιπών άρθρων του Κώδικα Ποινικής Δικονομίας, που προβλέπουν τα όσα ορίζεται να γίνουν και να τηρηθούν στα πλαίσια των διαδικασιών της ανακριτικής διαδικασίας της κατάσχεσης επί υλικού αντικειμένου ή εγγράφου. Όσων δε αφορά τα ψηφιακά δεδομένα καθαυτά, η αίτηση για αναλογική εφαρμογή των ως άνω διατάξεων κινδυνεύει να χαρακτηριστεί άνευ αντικειμένου, ενώ για μπορέσει να τύχει εφαρμογής στην πράξη, θα πρέπει να οδηγεί στην διαγραφή και καταστροφή του αντιγράφου που δημιουργήθηκε, στα πλαίσια της ανακριτικής πράξης, επί του πρωτοτύπου ψηφιακού δεδομένου.

5. Διαχρονικό Δίκαιο – Χρονικό όριο εφαρμογής της διάταξης του άρθρου 265 ΚΠΔ

Με τη θέσπισης της νεότερης και ειδικότερης διάταξης νόμου του άρθρου 265 ΚΠΔ, αναφορικά με την κατάσχεση ψηφιακών δεδομένων, η οποία πλέον συνυπάρχει με τις διατάξεις της κατάσχεσης υλικών – ενσωμάτων αντικειμένων και εγγράφων, οι οποίες στο παρελθόν τύγχαναν αναλογικής εφαρμογής στις περιπτώσεις όπου εγείρονταν ζήτημα κατάσχεσης άυλων ψηφιακών δεδομένων, εγείρονται τα ακόλουθα ζητήματα:

Αρχικά, σύμφωνα με τη μεταβατική διάταξη του άρθρου 590 παρ. 1 εδ. α ΚΠΔ ορίζεται πως, «οι υποθέσεις που εκκρεμούν σε οποιοδήποτε στάδιο της ποινικής διαδικασίας και σε οποιοδήποτε βαθμό συνεχίζονται σύμφωνα με τις διατάξεις του παρόντος κώδικα», ήτοι εν προκειμένω, σύμφωνα με τις διατάξεις του νέου τροποποιημένου άρθρου 265 ΚΠΔ που τέθηκε σε ισχύ τη 01.07.2019. Συνεπώς όλες οι υποθέσεις που εκκρεμούν ενώπιον οποιουδήποτε ελληνικού δικαστηρίου από την θέσπιση του νέου άρθρου 265 ΚΠΔ και την θέση αυτού σε ισχύ, θα εκδικάζονται σύμφωνα με τα ειδικότερα προβλεπόμενα στη διάταξη αυτή νόμου, όπως επίσης, αυτονόητο τυγχάνει πως η ανωτέρω διάταξη θα τύχει εφαρμογής και σε όλες τις περιπτώσεις που από τη θέση του ως άνω άρθρου σε ισχύ και στο εξής προκύπτουν και αφορούν στην ανάγκη κατασχέσεις ψηφιακών δεδομένων στα πλαίσια της ποινικής διαδικασίας. Προβλέπεται πάντως ότι η διαδικαστικές πράξεις που διενεργήθηκαν υπό τον προϊσχύσαντα κώδικα ποινικής δικονομίας παραμένουν ισχυρές, χωρίς η νεότερες ρυθμίσεις να επιδρούν στο κύρος τους αναδρομικά και χωρίς να απαιτείται ασφαλώς επανάληψη τους.[31] Συνεπώς όλες οι διαδικαστικές πράξεις που τελέστηκαν επί ψηφιακών δεδομένων, κατά αναλογική εφαρμογή των άρθρων περί κατασχέσεως υλικών αντικειμένων και εγγράφων, όταν δεν είχε ακόμη τεθεί σε ισχύ το νέο άρθρο 265, διατηρούν το κύρος και την ισχύ τους χωρίς να υφίσταται περίπτωση ακυρότητας επ' αυτών. Τέλος κατά ορθότερη εκδοχή θα πρέπει να αναγνωριστεί αναδρομική εφαρμογή και σε κανόνες που έτσι κι αλλιώς όφειλαν να διέπουν τις ανακριτικές πράξεις

[31] Γιάννης Ναζίρης, Επίκουρος Καθηγητής ΑΠΘ, Δικηγόρος, ΠοινΔικ, [Νομική Βιβλιοθήκη], ISSN:1108-2755, τομ.24 τευχ.247 [2021] σελ.178-194.

και υπό το προϊσχύσαντα Κώδικα Ποινικής Δικονομίας, έστω και ελλείψει ρητής πρόβλεψης. Κατά συνέπεια, η πρόβλεψη σχετικά με την εφαρμογή αναλογικότητας μολονότι δεν περιλαμβάνεται ρητά στο πλαίσιο του νέου κώδικα ποινικής δικονομίας θα πρέπει να γίνει δεκτό ό,τι αφορά και σε πράξεις που είχαν διενεργηθεί υπό τον προϊσχύσαντα κώδικα Ποινικής Δικονομίας, συνιστώντας, κατά κάποιον τρόπο ερμηνευτικό νόμο.[32]

6. Θεμελιώδεις εγγυήσεις κατά τη διαδικασία συλλογής, πρόσβασης ανάκτησης και επεξεργασίας των ψηφιακών δεδομένων

Η έρευνα, ανάκτηση και κατάσχεση των άυλων ψηφιακών δεδομένων, ως πειστηρίων εγκλημάτων, στα πλαίσια της διάταξης του άρθρου 265 ΚΠΔ , λόγω της ιδιαιτερότητας της φύσης, τόσο των δεδομένων καθαυτών, όσο και του τρόπου και της διαδικασίας ανάκτησής τους, θα πρέπει να διέπονται και να διασφαλίζονται από τη συνδρομή ορισμένων ουσιαστικών και δικονομικών εγγυήσεων. Η οποιαδήποτε αναζήτηση τέτοιων δεδομένων που βρίσκονται αποθηκευμένα, είτε σε ηλεκτρονικούς υπολογιστές και άλλα μέσα αποθήκευσης, είτε σε παρόχους ηλεκτρονικών και διαδικτυακών υπηρεσιών, συνιστά επέμβαση στο δικαίωμα της ιδιωτικής ζωής και στην προστασία των δεδομένων προσωπικού χαρακτήρα[33] του ατόμου.

Από τη διάταξη του άρθρου 8 της ΕΣΔΑ, αναφορικά με το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής, ορίζεται πως *«1. Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του. 2. Δεν επιτρέπεται να υπάρξη επέμβασις δημοσίας αρχής εν τη ασκήσει του δικαιώματος τούτου, εκτός εάν η επέμβασις αύτη προβλέπεται υπό του νόμου και αποτελεί μέτρον το οποίον, εις μίαν δημοκρατικήν κοινωνίαν, είναι αναγκαίον δια την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημερίαν της χώρας, την προάσπισιν της τάξεως και την πρόληψιν*

[32] Γιάννης Ναζίρης, Επίκουρος Καθηγητής ΑΠΘ, Δικηγόρος, ΠοινΔικ, [Νομική Βιβλιοθήκη], ISSN:1108-2755, τομ.24 τευχ.247 [2021] σελ.178-194.

[33] Αλέξανδρος Ι Καργιόπουλος, Ηλεκτρονικό Έγκλημα, Θεοχάρης Ι Δαλακούρας, Εκδ. Νομική Βιβλιοθήκη, κεφ. 12- Ανακριτικές πράξεις επί ψηφιακών δεδομένων: Δικαιικοί άξονες και προβληματισμοί, Συλλογή, Πρόσβαση, Ανάκτηση και Επεξεργασία Ψηφιακών Δεδομένων, σελ. 203.

ποινικών παραβάσεων, την προστασίαν της υγείας ή της ηθικής, ή την προστασίαν των δικαιωμάτων και ελευθεριών άλλων», στη συνέχεια από τη διάταξη του άρθρου 7 του Χάρτη Θεμελιωδών δικαιωμάτων της Ευρωπαϊκής Ένωσης, αναφορικά με τον σεβασμό της Ιδιωτικής και οικογενειακής ζωής του ατόμου ορίζεται πως, *«Κάθε πρόσωπο έχει δικαίωμα στο σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και των επικοινωνιών του»,* ενώ τέλος από τη διάταξη του άρθρου 8 του Χάρτη Θεμελιωδών δικαιωμάτων της Ευρωπαϊκής Ένωσης, αναφορικά με την προστασία των δεδομένων προσωπικού χαρακτήρα, ορίζεται πως, *«Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν. 2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους».*

Από τον συνδυασμό των ως άνω διατάξεων των ευρωπαϊκών κειμένων που περικλείουν αξιώσεις και προτροπές από πλευράς της Ευρωπαϊκής Ενώσεως, για ενσωμάτωση θεμελιωδών αρχών και εγγυήσεων στις έννομες τάξεις των κρατών μελών, και από τις αρχές της αναλογικότητας, της αναγκαιότητας σκοπού, της ορθής απονομής δικαιοσύνης και της δίκαιης δίκης που διέπουν την απονομή της ποινικής δικαιοσύνης στο σύνολό της, συνάγονται οι δικονομικοί και ουσιαστικοί περιορισμοί και οι εγγυήσεις που πρέπει να διέπουν μεταξύ άλλων και την ανακριτική πράξη της κατάσχεσης ψηφιακών δεδομένων του άρθρου 265 ΚΠΔ. Οι ανακριτικοί υπάλληλοι θα πρέπει με γνώμονα τις ως άνω διατάξεις και αρχές να διασφαλίζουν την τήρηση του κανόνα δικαίου (rule of law), δηλαδή να ορίζεται ακριβώς το εύρος των αρμοδιοτήτων και των ενεργειών, στις οποίες μπορούν να προβαίνουν οι αρχές, και να αποτρέπεται οποιαδήποτε αυθαιρεσία. Στο πλαίσιο αυτό απαιτείται, δηλαδή, ειδική νομική βάση που να προβλέπει ειδικώς τις δικονομικές ενέργειες των αρχών και το πεδίο εφαρμογής τους και ειδικότερες εγγυήσεις για την διασφάλιση των δικαιωμάτων των ελευθεριών των φυσικών προσώπων.[34] Οι αρμόδιοι ανακριτικοί υπάλληλοι θα πρέπει να

[34] Αλέξανδρος Ι Καργιόπουλος, Ηλεκτρονικό Έγκλημα, Θεοχάρης Ι Δαλακούρας, Εκδ. Νομική Βιβλιοθήκη, κεφ. 12- Ανακριτικές πράξεις επί ψηφιακών δεδομένων: Δικαιικοί άξονες και προβληματισμοί, Συλλογή, Πρόσβαση, Ανάκτηση και Επεξεργασία Ψηφιακών Δεδομένων, σελ. 204.

είναι εφοδιασμένοι με σαφείς κατευθύνσεις των ορίων των ενεργειών στις οποίες δύνανται και πρέπει να προβούν, ενώ κατά τη διαδικασία της πρόσβασης και κατ' επέκταση της έρευνας, κατάσχεσης και επεξεργασίας των ψηφιακών δεδομένων του υπόπτου ή κατηγορουμένου, θα πρέπει να δρουν με απόλυτο γνώμονα την αρχή της αναλογικότητας και της αναγκαιότητας σκοπού, και να προβαίνουν στην κατάσχεση και επεξεργασία μόνον των ψηφιακών δεδομένων εκείνων του προσώπου που κρίνονται ως απαραίτητα και αξιοποιήσιμα στα πλαίσια της ποινικής υπόθεσης που ερευνάται, προξενώντας στον ύποπτο ή τον κατηγορούμενο την μικρότερη δυνατή «ζημία» και παραβίαση στην ιδιωτική του ζωή. Η φύση του ψηφιακού κόσμου στον οποίον τηρούνται τα πειστήρια ενός εγκλήματος που διαπράχθηκε στον κυβερνοχώρο, είναι τόσο ευαίσθητη και ευάλωτη, ώστε η ευλαβική τήρηση των γραμματικών επιταγών των σχετικών άρθρων νόμων και των αρχών που διέπουν το σύνολο της ποινικής διαδικασίας κρίνεται ως επιβεβλημένη.

Πλούσια είναι εξάλλου η νομολογία του ΕΔΔΑ και του ΔΕΕ που αφορά στην προστασία των δικαιωμάτων της ιδιωτικής, προσωπικής και οικογενειακής του ατόμου, όπως αυτές ορίστηκαν ανωτέρω, αποσκοπώντας στην εξασφάλιση της τήρησής τους από πλευράς των κρατών μελών. Χαρακτηριστική, μεταξύ άλλων είναι η υπ' αριθμόν Νο 61064/10, 13 Φεβρουαρίου 2018 απόφαση του ΕΔΔΑ στην υπόθεση Ivashchenko v. Russia, στην οποία το Δικαστήριο διαπίστωσε παραβίαση του άρθρου 8. Στη συγκεκριμένη υπόθεση οι τελωνειακές αρχές της Ρωσίας κατέσχεσαν μια φωτογραφική μηχανή και έναν φορητό υπολογιστή ενός φωτογράφου και αντέγραψαν τα δεδομένα που ήταν αποθηκευμένα στον σκληρό δίσκο της μηχανής σε εξωτερικό μέσο αποθήκευσης και σε έξι DVDs. Εν συνεχεία τα εξέτασαν με τη συνδρομή πραγματογνώμονα ώστε να διαπιστώσουν αν περιείχαν «εξτρεμιστικό υλικό». Οι ρωσικές τελωνειακές αρχές ενήργησαν σύμφωνα με τον τελωνειακό κώδικα και τις διατάξεις που αφορούσαν την επιθεώρηση αγαθών και αντικειμένων και εφάρμοσαν τις διατάξεις αυτές για τον φορητό υπολογιστή και τα ψηφιακά δεδομένα. Ωστόσο το ΕΔΔΑ δεν θεώρησε επαρκείς τις διατάξεις αυτές, ούτε την υπόλοιπη νομοθεσία, γιατί

ακριβώς δεν περιείχαν σαφή νομική βάση που να επέτρεπε στις αρχές την αντιγραφή των ψηφιακών δεδομένων από τα κατασχεθέντα πειστήρια.[35]

Η διασφάλιση των ως άνω εγγυήσεων δε, έχουν διατυπωθεί εξάλλου και στην Οδηγία 2016/680/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, η οποία παρουσιάστηκε και στην αρχή της παρούσας μελέτης, και η οποία ενσωματώθηκε από τον νομοθέτη στην ελληνική έννομη τάξη, δια της θεσπίσεως και θέσης σε ισχύ του νέου άρθρου 265 ΚΠΔ. Συγκεκριμένα στην παράγραφο υπ' αριθμόν 26 της ως άνω υπ' αριθμόν 2016/680/ΕΕ Οδηγίας, ορίζεται πως αξιώνεται από τα κράτη μέλη, πως *«κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σύννομη, θεμιτή και διαφανής σε σχέση με τα φυσικά πρόσωπα τα οποία αφορά και να πραγματοποιείται μόνο για συγκεκριμένους σκοπούς που προβλέπονται από το νόμο».* Ενώ στις παραγράφους υπ' αριθμόν 27 και 28 της ίδιας ως άνω Οδηγίας, ορίζεται πως *«Για την πρόληψη, διερεύνηση και τη δίωξη ποινικών αδικημάτων, οι αρμόδιες αρχές πρέπει να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα που συλλέγονται στο πλαίσιο της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης συγκεκριμένων ποινικών αδικημάτων και πέραν του πλαισίου αυτού, ώστε να κατανοούν καλυτέρα τις εγκληματικές δραστηριότητες και να προβαίνουν σε συσχετισμούς μεταξύ διαφορετικών διαπιστωθέντων ποινικών αδικημάτων».* (αρ. 27 Οδηγίας 2016/680/ΕΕ). Επιπλέον επισημαίνεται πως, *«Για να τηρείται η ασφάλεια σε σχέση με την επεξεργασία και να αποτρέπεται η επεξεργασία κατά παραβίαση της παρούσας οδηγίας, τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο ώστε να εξασφαλίζεται το ενδεδειγμένο επίπεδο ασφάλειας και εμπιστευτικότητας, μεταξύ άλλων με την αποτροπή της μη εξουσιοδοτημένης πρόσβασης σε δεδομένα προσωπικού χαρακτήρα ή τη χρήση τους και στον εξοπλισμό που χρησιμοποιείται για την επεξεργασία, λαμβανομένων υπόψη του επιπέδου της διαθέσιμης τεχνολογίας, του κόστους εφαρμογής σε σχέση με τους κινδύνους και τη φύση των δεδομένων προσωπικού χαρακτήρα που πρέπει να προστατευτούν».* (αρ. 28 Οδηγίας 2016/680/ΕΕ).

[35] Αλέξανδρος Ι Καργιόπουλος, Ηλεκτρονικό Έγκλημα, Θεοχάρης Ι Δαλακούρας, Εκδ. Νομική Βιβλιοθήκη, κεφ. 12- Ανακριτικές πράξεις επί ψηφιακών δεδομένων: Δικαιικοί άξονες και προβληματισμοί, Συλλογή, Πρόσβαση, Ανάκτηση και Επεξεργασία Ψηφιακών Δεδομένων, σελ. 204

Συνεπώς, η διαδικασία της κατασχέσεως ψηφιακών δεδομένων, κατά τα ορισθέντα στην ως άνω Οδηγία και την νομολογία, απαιτείται να περιβάλλεται με τις κατάλληλες εγγυήσεις κατά τυχόν αυθαιρεσιών. Τέτοιες είναι η προηγούμενη δικαστική έγκριση, η τήρηση αρχείου καταγραφής, ο περιορισμός της πρόσβασης μόνο σε εξουσιοδοτημένο προσωπικό, μέτρα κατά της τυχαίας απώλειας και καταστροφής ψηφιακών δεδομένων κτλ.[36]. Για τους ως άνω λόγους άλλωστε κρίθηκε ως επιβεβλημένη από τον νομοθέτη η ενσωμάτωση των αξιώσεων μεταξύ άλλων και της ως άνω Οδηγίας στην ελληνική έννομη τάξη και οδηγηθήκαμε στην θέσπιση του νέου άρθρου 265 ΚΠΔ, αναφορικά με την κατάσχεση ψηφιακών δεδομένων, έναντι των πρακτικών τις αναλογικής εφαρμογής των διατάξεων νόμων για την κατάσχεση υλικών – ενσώματων αντικειμένων που ακολουθούνταν πριν τη θέση σε εφαρμογή του ν. 4620/2019.

7. Ο τόπος τέλεσης του διαδικτυακού εγκλήματος.

Με τον όρο διαδικτυακό έγκλημα ή έγκλημα στον κυβερνοχώρο, ως ανωτέρω ελέχθη, νοείται τόσο η αξιόποινη εκείνη πράξη που τελέστηκε μέσω του διαδικτύου, ενώ τυποποιείται και ως «παραδοσιακό» έγκλημα του φυσικού – υλικού χώρου, όσο και η αξιόποινη εκείνη πράξη η οποία έχει ως αντικείμενο και εξ ορισμού στρέφεται κατά ενός υπολογιστή ή ενός πληροφορικού συστήματος[37]. Για την κατάφαση λοιπόν της συνδρομής ενός διαδικτυακού εγκλήματος απαιτείται η κατάφαση τέλεσης μιας αξιόποινης πράξης και η παράλληλη «εμπλοκή» στη διάπραξη αυτής ενός υπολογιστή ή ενός πληροφοριακού συστήματος. Ο υπολογιστής ή το πληροφοριακό σύστημα δύναται να είναι είτε το μέσο για τη διάπραξη του εγκλήματος, είτε να αποτελεί τον «στόχο», ήτοι τον αποδέκτη της εγκληματικής συμπεριφοράς. Το διαδικτυακό έγκλημα εμφανίζει ένα κεντρικό χαρακτηριστικό, που παρουσιάζει ιδιαίτερο ενδιαφέρον για το

[36] Αλέξανδρος Ι Καργιόπουλος, Ηλεκτρονικό Έγκλημα, Θεοχάρης Ι Δαλακούρας, Εκδ. Νομική Βιβλιοθήκη, κεφ. 12- Ανακριτικές πράξεις επί ψηφιακών δεδομένων: Δικαιικοί άξονες και προβληματισμοί, Συλλογή, Πρόσβαση, Ανάκτηση και Επεξεργασία Ψηφιακών Δεδομένων, σελ. 204

[37] Άρθρο 13, παρ. 1 περ. στ' ΠΚ: Πληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών.

ποινικό δίκαιο. Είναι πάντοτε έγκλημα αποστάσεως, αφού αλλού εκδηλώνεται η συμπεριφορά του δράστη και αλλού το (ενδεχόμενο) αξιόποινο αποτέλεσμα. Μάλιστα, καθώς από την φύση της χρησιμοποιούμενης τεχνολογίας τα δεδομένα διακινούνται παντού όπου υπάρχει δυνατότητα διαδικτυακής πρόσβασης, πολύ συχνά το διαδικτυακό έγκλημα αποκτά διασυνοριακό χαρακτήρα, καθώς οι τόποι τέλεσης του εγκλήματος εντοπίζονται σε περισσότερα κράτη.[38]

Αναφορικά με τον τόπο τέλεσης των αξιόποινων πράξεων, στα άρθρα 5 έως 11 του ισχύοντος Ποινικού Κώδικα, απαντώνται οι διατάξεις που αφορούν στα τοπικά όρια ισχύος των ποινικών νόμων. Συγκεκριμένα στο άρθρο 5 παρ. 1 ΠΚ, όπου και καθιερώνεται η αρχή της εδαφικότητας, ορίζεται πως, «οι ελληνικοί ποινικοί νόμοι εφαρμόζονται σε όλες τις πράξεις που τελέστηκαν στο έδαφος της επικράτειας, ακόμη και από αλλοδαπούς. Επίσης εφαρμόζονται και στις πράξεις συμμετοχής που τελέστηκαν στο έδαφος της ελληνικής επικράτειας, αν η κύρια πράξη, για την οποία δεν υπάρχει δικαιοδοσία των ελληνικών ποινικών δικαστηρίων, είναι αξιόποινη και κατά τους ελληνικούς ποινικούς νόμους». Στη συνέχεια, στο άρθρο 16 του Ποινικού Κώδικα ορίζει πως, «τόπος τέλεσης της πράξης θεωρείται ο τόπος όπου ο υπαίτιος διέπραξε ολικά ή μερικά την αξιόποινη ενέργεια ή παράλειψη, καθώς και ο τόπος όπου επήλθε ή, σε περίπτωση απόπειρας, έπρεπε να επέλθει σύμφωνα με την πρόθεσή του το αποτέλεσμα». Με τον ως άνω ορισμό υιοθετείται από πλευράς του νομοθέτη η «αρχή της ενότητας της πράξης», ήτοι ως τόπος τέλεσης της αξιόποινης πράξης λογίζεται τόσο ο τόπος όπου ενήργησε ο δράστης, όσο και ο τόπος που επήλθε το αξιόποινο αποτέλεσμα ή που αυτό (το αποτέλεσμα) έπρεπε να επέλθει σε περίπτωση απόπειρας του εγκλήματος.

Το διαδικτυακό έγκλημα από την φύση του, στην πλειοψηφία των περιπτώσεων που τελείται, χαρακτηρίζεται από διαφορετικό τόπο εκδήλωσης της αξιόποινης συμπεριφοράς του δράστη και διαφορετικό τόπο επί του οποίου επέρχεται το αξιόποινο αποτέλεσμα. Το ως άνω, όταν πρόκειται για περιπτώσεις που η αξιόποινη συμπεριφορά και το επερχόμενο εγκληματικό αποτέλεσμα περιορίζονται στα στενά όρια της ελληνικής επικράτειας, απλώς δημιουργεί πλείονες τόπους τέλεσης του εγκλήματος. Ζήτημα γεννάται όταν η προαναφερθείσα απόσταση

[38] Δημήτριος Κιούπης, Αναπλ. Καθηγητής ΕΚΠΑ, Δικηγόρος, Κεφ. « Ο τόπος τέλεσης του διαδικτυακού εγκλήματος», «Ηλεκτρονικό Έγκλημα», επιμέλεια Θεοχάρης Ι Δαλακούρας, Εκδ. Νομική Βιβλιοθήκη.

επεκτείνεται πέραν των εθνικών ορίων και συνόρων, κυρίως αναφορικά με τις ανακριτικές πράξεις που δέον να λάβουν χώρα.

Ορθώς ο νέος Ποινικός Κώδικας κατήργησε την τρίτη παράγραφο του άρθρου 5 ΠΚ, η οποία είχε προστεθεί με το άρθρο 2 του ν. 4267/2014 και ίσχυσε μέχρι τις 30.06.2019, δυνάμει της οποίας οριζόταν πως, «Όταν η πράξη τελείται μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, τόπος τέλεσης θεωρείται και η ελληνική επικράτεια, εφόσον στο έδαφος της παρέχεται πρόσβαση στα συγκεκριμένα μέσα, ανεξάρτητα από τον τόπο εγκατάστασης τους». Δυνάμει της ως άνω διατάξεως θεωρούνταν ως τόπος τέλεσης του διαδικτυακού εγκλήματος η ημεδαπή, με μόνο κριτήριο την παροχή πρόσβασης από αυτήν στον δράστη στα συγκεκριμένα μέσα, ήτοι την παροχή πρόσβασης στο διαδίκτυο, χωρίς να λαμβάνονται υπόψιν οι αντίστοιχες διατάξεις για την αρχή της εδαφικότητας αναφορικά των μη ψηφιακών εγκλημάτων, ήτοι χωρίς να απασχολεί αν επρόκειτο για Έλληνα πολίτη που προβαίνει σε τέλεση διαδικτυακού εγκλήματος στην αλλοδαπή, ή για αλλοδαπό που στρέφεται δια διαδικτυακού εγκλήματος κατά Έλληνα πολίτη, ή αν ο υπολογιστής μέσω του οποίου τελέστηκε η αξιόποινη πράξη βρισκόταν στην Ελλάδα, ή αν τα δεδομένα αποθηκεύτηκαν σε server εντός της ελληνικής επικράτειας κτλ.

Πλέον, μετά την κατάργηση της ως άνω διατάξεως, για την στοιχειοθέτηση του τόπου τέλεσης ενός διαδικτυακού εγκλήματος, ακολουθούνται τα όσα ορίζονται αναφορικά με τον τόπο τέλεσης ενός φυσικού εγκλήματος. Είναι εσφαλμένο να μιλούμε γενικώς και αορίστως περί τόπου τέλεσης διαδικτυακού εγκλήματος, καθώς θα πρέπει να εξειδικεύσουμε ad hoc την αξιόποινη πράξη και στη συνέχεια να την εντάξουμε σε κατηγορίες εγκλημάτων. Άλλος ο τόπος τέλεσης ενός διαδικτυακού εγκλήματος αποτελέσματος και άλλος ενός διαδικτυακού εγκλήματος αφηρημένης διακινδύνευσης,[39] στα ως άνω συνηγορεί και η ιδιαιτερότητα της χρήσης των διαφόρων τεχνολογικών μέσων, όπου πολλές φορές το αποτέλεσμα μιας επικοινωνίας μέσω της οποίας τελείται η αξιόποινη πράξη έχει έναν συγκεκριμένο αποδέκτη (π.χ. αποστολή υβριστικού μηνύματος κατά συγκεκριμένου αποδέκτη, ή εξαπάτηση συγκεκριμένου ατόμου μέσω υπολογιστή), και άλλες αφορά έναν αόριστο και απρόσωπο αριθμό ατόμων, τα οποία θα αποκτήσουν πρόσβαση στην

[39] Δημήτριος Κιούπης, Αναπλ. Καθηγητής ΕΚΠΑ, Δικηγόρος, Κεφ. « Ο τόπος τέλεσης του διαδικτυακού εγκλήματος», «Ηλεκτρονικό Έγκλημα», επιμέλεια Θεοχάρης Ι Δαλακούρας, Εκδ. Νομική Βιβλιοθήκη.

πληροφορία που συνιστά αξιόποινη πράξη μέσω διαδικτύου (π.χ. πρόσβαση σε ιστοσελίδα, ή πρόσβαση σε αναρτημένη δημοσίευση σε μέσα κοινωνικής δικτύωσης). Συνεπώς για την στοιχειοθέτηση των τόπων τέλεσης του διαδικτυακού εγκλήματος θα πρέπει να ακολουθούνται όσα ισχύουν γενικώς για τον τόπο τέλεσης των φυσικών, μη ψηφιακών εγκλημάτων, ήτοι να λαμβάνεται υπόψιν το είδος της τελεσθείσας αξιόποινης πράξης σε συνδυασμό με την ιδιαιτερότητα της υπό κρίση μορφής διαδικτυακής επικοινωνίας. Στην προσπάθεια δε για την δημιουργία ενός γενικότερου κανόνα, αναφορικά με τον τόπο τέλεσης του ψηφιακού εγκλήματος, θα μπορούσε να οριστεί πως κάθε εθνική έννομη τάξη στο διεθνοποιημένο διαδικτυακό περιβάλλον, δέχεται καταρχήν εφαρμογή της αρχής της εδαφικότητας με τις ακόλουθες διακρίσεις: α) Όταν ο χρήστης αναρτά δεδομένα στα οποία τρίτοι με δικές τους πράξεις αποκτούν πρόσβαση, τόπος τέλεσης της πράξης του χρήστη, είναι ο τόπος φυσικής παρουσίας του χρήστη κατά τον χρόνο ανάρτησης των δεδομένων και ο τόπος αποθήκευσης των δεδομένων στους διακομιστές εφόσον ο χρήστης γνωρίζει τον τόπο αποθήκευσης, β) όταν ο χρήστης στέλνει τα δεδομένα σε τρίτους, τόπος τέλεσης της αξιόποινης πράξης είναι επιπρόσθετα και ο τόπος που επήλθε το τυχόν αποτέλεσμα (βλάβη ή συγκεκριμένος κίνδυνος)[40]. Στο σημείο αυτό δέον να σημειωθεί πως, το ζήτημα του τόπου τέλεσης του διαδικτυακού εγκλήματος που ξεπερνά τα όρια της ημεδαπής, χρήζει ενοποιημένης και γενικής ρυθμίσεως δια διεθνούς συμβάσεως που θα περιέχει παγκοσμίως αποδεκτούς κανόνες ρύθμισης.

7.1 Διενέργεια ανακριτικών πράξεων για έρευνα και κατάσχεση ψηφιακών δεδομένων που είναι αποθηκευμένα στην αλλοδαπή.

Παρότι από τις διατάξεις του ισχύοντος Ποινικού Κώδικα, και συγκεκριμένα από τις διατάξεις των άρθρων 5 έως 8 ΠΚ και του άρθρου 16 ΠΚ, προβλέπεται σε συγκεκριμένες, ειδικώς στα ως άνω άρθρα ορισμένες, περιπτώσεις, η εφαρμογή των ουσιαστικών ποινικών νόμων της ελληνικής έννομης τάξης, σε πράξεις οι οποίες τελέστηκαν στην αλλοδαπή, εντούτοις η ως άνω δυνατότητα δεν εκτείνεται και επί των

[40] Δημήτριος Κιούπης, Αναπλ. Καθηγητής ΕΚΠΑ, Δικηγόρος, Κεφ. « Ο τόπος τέλεσης του διαδικτυακού εγκλήματος», «Ηλεκτρονικό Έγκλημα», επιμέλεια Θεοχάρης Ι Δαλακούρας, Εκδ. Νομική Βιβλιοθήκη.

ανακριτικών πράξεων, όπως συνάγεται από τη διάταξη του άρθρου 277 παρ. 1 ΚΠΔ, όπου ορίζεται πως *«το ένταλμα σύλληψης που εκδίδεται με νόμιμο τύπο είναι εκτελεστό σε όλη την επικράτεια»*, ενώ για την αντίστοιχη πρακτική στην αλλοδαπή, θα έπρεπε να εφαρμοστούν οι διατάξεις για την έκδοση ή το ευρωπαϊκό ένταλμα σύλληψης.

Από τον συνδυασμό του ως άνω αρ. 5 παρ. 1 ΠΚ αναφορικά με την αρχή της εδαφικότητας, και του άρθρου 16 ΠΚ αναφορικά με την αρχή της ενότητας, προκύπτει ότι, ως ψηφιακή εδαφικότητα ενός διαδικτυακού εγκλήματος που επιφέρει ορισμένο αποτέλεσμα, ορίζεται και ο τόπος όπου επήλθε το αξιόποινο αποτέλεσμα πέρα από τον τόπο της ψηφιακής δράσης του υπαιτίου (με το αποτέλεσμα να περιλαμβάνει τόσο την έννοια της βλάβης όσο και της διακινδύνευσης, την έννοια του τελικού αλλά και του ενδιάμεσου αποτελέσματος). Έτσι λοιπόν, εάν ο δράστης ενός διαδικτυακού εγκλήματος είχε πρόσβαση σε τραπεζικά στοιχεία, σε προσωπική σελίδα μέσων κοινωνικής δικτύωσης (Facebook, Instagram κλπ.) ή σε ιστοσελίδες της Ελλάδας, πέρα από τον φυσικό χώρο όπου βρίσκεται ο υπολογιστής του, του τόπου όπου ενδεχομένως αποθήκευσε τα κλαπέντα στοιχεία ή δεδομένα, εφόσον η βλάβη προκαλείται σε κάτοικο Ελλάδος, τότε τόπος τέλεσης της ψηφιακής εγκληματικής πράξης είναι και η Ελλάδα. Συνεπώς, ως ψηφιακή εδαφικότητα θα μπορούσε να οριστεί η δικαιοδοσία του εκάστοτε κράτους σε άυλο περιβάλλον που συνδέεται στενά με την εδαφική επικράτεια του εν λόγω κράτους.[41]

Στην περίπτωση λοιπόν που κριθεί αναγκαίο να επιχειρηθεί από πλευράς των ελληνικών ανακριτικών αρχών, ανακριτική πράξη, στα πλαίσια της διάταξης του νέου άρθρου 265 ΚΠΔ, ήτοι η έρευνα και κατάσχεση ψηφιακών δεδομένων, τα οποία βρίσκονται αποθηκευμένα πέρα από τα ως άνω ορισθέντα όρια της ψηφιακής εδαφικότητας του ελληνικού κράτους, τεκμαίρεται πως οι ελληνικές ανακριτικές αρχές δεν διαθέτουν την απαιτούμενη δικαιοδοσία να τις πράξουν και θα πρέπει να καταφύγουν στις πάγιες πρακτικές της δικαστικής συνεργασίας.

Μια διαφορετική πρακτική που θα μπορούσε να υιοθετηθεί, και αφορά στις δικαιούμενες ενέργειες κατά τις ως άνω περιπτώσεις, η οποία όμως δεν τυγχάνει εφαρμογής στην ελληνική έννομη τάξη, είναι η

[41] Φωτεινή Μπάλα, Αστυνομικός, Υποψ. Διδάκτωρ Δημοσίου Διεθνούς Δικαίου της Νομικής του Δ.Π.Θ, Ψηφιακή εδαφικότητα – Τόπος τέλεσης εγκλήματος μέσω διαδικτύου, https://www.lawspot.gr/nomika-nea/psifiaki-edafikotita-topos-telesis-egklimatos-meso-diadiktyoy

απευθείας ανακριτική πράξη, ήτοι η αναζήτηση στοιχείων που βρίσκονται στην αλλοδαπή απομακρυσμένα. Η ως άνω πρακτική υιοθετείται από το άρθρο 88ter του Βέλγικου Κώδικα Ποινικής Δικονομίας, όπου επιτρέπει την διενέργεια ανακριτικών πράξεων (έρευνα) σε άλλον υπολογιστή που είναι διασυνδεδεμένος με υπολογιστή που βρίσκεται στο Βέλγιο, ακόμη και αν ο πρώτος βρίσκεται σε άλλο κράτος. Ειδικότερα όταν τα αρχεία στον υπολογιστή βρίσκονται εκτός της βελγικής επικρατείας προβλέπεται ότι αντιγράφονται. Βασικό κριτήριο της λύσης αυτής, είναι η δυνατότητα πρόσβασης στον άλλον υπολογιστή[42]. Η ως άνω πρακτική πηγάζει άλλωστε ευθέως από τη διάταξη του άρθρου 32 της Σύμβασης της Βουδαπέστης, αναφορικά με τη «διασυνοριακή πρόσβαση σε αποθηκευμένα δεδομένα υπολογιστή, μετά από συναίνεση ή σε περίπτωση που αυτά είναι διαθέσιμα στο κοινό», όπου ορίζεται ότι, «Κάθε Συμβαλλόμενο Μέρος μπορεί, χωρίς την εξουσιοδότηση του άλλου Συμβαλλομένου Μέρους: α. να έχει πρόσβαση σε αποθηκευμένα δεδομένα υπολογιστή που είναι διαθέσιμα στο κοινό (ανοικτή πηγή), ασχέτως της γεωγραφικής θέσης των δεδομένων, ή β. να αποκτήσει πρόσβαση ή να λάβει, μέσω ενός συστήματος υπολογιστή στην επικράτειά του, δεδομένα υπολογιστή που είναι αποθηκευμένα σε άλλο Συμβαλλόμενο Μέρος, εάν το Συμβαλλόμενο Μέρος λάβει την νόμιμη και οικειοθελή συναίνεση του προσώπου που έχει την νόμιμη εξουσία να γνωστοποιεί τα δεδομένα στο Συμβαλλόμενο Μέρος μέσω του συστήματος υπολογιστή του. Η ως άνω αξίωση και προτροπή, δεν ενσωματώθηκε επί του παρόντος στην ελληνική έννομη τάξη.

Επαγωγικά όμως σκεπτόμενοι και λαμβάνοντας υπόψιν όσα ως άνω εκτέθηκαν αναφορικά με την αρχή της εδαφικότητας και του ορισμού της ψηφιακής εδαφικότητας, η ως άνω πρακτική θα μπορούσε να θεωρηθεί παραβίαση της αρχής του άρθρου 5 παρ. 1 ΚΠΔ, και των αντίστοιχων διατάξεων του κράτους στον οποίο βρίσκεται ο «απομακρυσμένος» υπολογιστής, ήτοι παραβίαση της αρχής της εδαφικότητας, καθώς θα διενεργούνταν επί της ουσίας η ανακριτική πράξη της έρευνας και κατάσχεσης ψηφιακού δεδομένου, στο «ψηφιακό» έδαφος άλλου κράτους.

[42] Αλέξανδρος Ι Καργιόπουλος, Ηλεκτρονικό Έγκλημα, Θεοχάρης Ι Δαλακούρας, Εκδ. Νομική Βιβλιοθήκη, κεφ. 12- Ανακριτικές πράξεις επί ψηφιακών δεδομένων: Δικαιικοί άξονες και προβληματισμοί, Συλλογή, Πρόσβαση, Ανάκτηση και Επεξεργασία Ψηφιακών Δεδομένων, σελ. 216.

8. Επίλογος
8.1. Σύνοψη – Συμπεράσματα

Λαμβάνοντας υπόψιν τα όσα ως άνω εκτέθηκαν, η θέσπιση στην ελληνική έννομη τάξη της ανακριτικής πράξης της κατάσχεσης ψηφιακών δεδομένων του άρθρου 265 ΚΠΔ, υπήρξε επιβεβλημένη όχι μόνο δια των Οδηγιών και των Συμβάσεων προερχόμενων από τον χώρο της Ευρωπαϊκής Ενώσεως, αλλά επιταγή της ίδιας της δραματικής αλλαγής στο σύνολο των πτυχών και εκφάνσεων της ανθρώπινης δραστηριότητας που προέρχεται από την ραγδαία τεχνολογική πρόοδο και ανάπτυξη. Πλέον η κάθε δραστηριότητα του ατόμου αφήνει πίσω της ένα ψηφιακό αποτύπωμα, γεγονός που καθώς η τεχνολογία και η κοινωνία εξελίσσεται θα καταλαμβάνει όλο και μεγαλύτερο έδαφος. Η ως άνω εξέλιξη δεν θα μπορούσε σε καμία περίπτωση να αφήσει ανεπηρέαστο τον τομέα του ποινικού δικαίου και της ποινικής δικονομίας. Σε πλείονες περιπτώσεις, εάν όχι στο σύνολο των περιπτώσεων, των ποινικών (και όχι μόνο) υποθέσεων των τελευταίων χρόνων, ακόμη και πριν την θέση σε ισχύ του νέου άρθρου 265 ΚΠΔ, παρατηρείται πως χρησιμοποιούνται ως πειστήρια ψηφιακά δεδομένα, είτε από υπερασπιστικής πλευράς του κατηγορουμένου, ως πειστήρια αθωότητας, είτε στα πλαίσια των ανακριτικών πράξεων για την στοιχειοθέτηση του εγκλήματος, είτε ακόμη και περιπτώσεις που το έγκλημα συνίσταται σε προσβολή αυτών των ψηφιακών δεδομένων ή τελείται δια αυτών.

Η ύπαρξη, πριν τη θέση σε ισχύ του ν. 4620/2019, νομοθετικού κενού αναφορικά με την έρευνα, κατάσχεση και επεξεργασία των ψηφιακών δεδομένων, δημιουργούσε ανασφάλεια δικαίου, ενώ μπορεί να οδηγούσε και σε παραβίαση θεμελιωδών δικαιωμάτων του κατηγορουμένου, αναφορικά με την επεξεργασία των προσωπικών του δεδομένων, αλλά και την ακρίβεια και αξιοπιστία των ψηφιακών μέσων που κατάσχονταν, χωρίς να τηρούνται ειδικές διαδικασίες και διατυπώσεις, τόσο κατά την κτήση, όσο και κατά την αποθήκευση και φύλαξη τους. Το ως άνω θα μπορούσε να πλήξει το δικαίωμα του κατηγορουμένου στην υπεράσπισή του, στην διαφύλαξη του τεκμηρίου αθωότητας του, καθώς και στην ορθή απονομή δικαιοσύνης και στην δίκαιη δίκη.

Για όλους τους ως άνω λόγους εξάλλου, κρίνεται ως αναγκαία, ως ήδη επισημάνθηκε στην αρχή της παρούσας, η θέσπιση ειδικής διατάξεως

νόμου που θα ρυθμίζει ειδικά τις προϋποθέσεις και τις διατυπώσεις που πρέπει να τηρηθούν αναφορικά με την ψηφιακή έρευνα.

8.2 Πιθανές Μελλοντικές τροποποιήσεις επί του νέου άρθρου 265 ΚΠΔ

Η θέση σε ισχύ του νέου άρθρου 265 ΚΠΔ, ήρθε να καλύψει την ύπαρξη νομοθετικού κενού, να εξασφαλίσει την ορθότητα στη διαδικασία έρευνας, κατάσχεσης και επεξεργασίας των ψηφιακών δεδομένων, καθώς και να διασφαλίσει την ασφάλεια στην φύλαξή και αποθήκευσή τους καθ' όλη τη διάρκεια της ποινικής διαδικασίας, ώστε αυτά (τα ψηφιακά δεδομένα) να διατηρηθούν αναλλοίωτα και ακέραια, στοχεύοντας με τον τρόπο αυτό στην ορθή απονομή δικαιοσύνης.

Από την θέσπιση όμως και διατύπωση του άρθρου αυτού μέχρι την εφαρμογή του στην πράξη, γεννώνται ορισμένα πρακτικά – διαδικαστικά ζητήματα, τα οποία θα πρέπει να ληφθούν υπόψιν από πλευράς των ελληνικών αρχών. Θα πρέπει αρχικά οι υποδομές των ανακριτικών αρχών της χώρας να εφοδιαστούν με σύγχρονο εξοπλισμό, ο οποίος θα πρέπει να τυγχάνει διαρκώς ανανεούμενος, ώστε να ακολουθεί την τεχνολογική πρόοδο και ανάπτυξη, και με τον τρόπο αυτό να διασφαλίζεται η ασφάλεια και η ακεραιότητα στην κατάσχεση, λήψη και αναπαραγωγή των ψηφιακών δεδομένων. Επιπλέον, και οι ίδιες οι ανακριτικές αρχές θα πρέπει να επανδρωθούν με προσωπικό ειδικής και ιδιαίτερης τεχνογνωσίας, το οποίο προσωπικό μάλιστα, θα πρέπει να επιμορφώνεται διαρκώς και να εκπαιδεύεται, ώστε να ακολουθεί τις επιταγές τις ραγδαίας τεχνολογικής προόδου. Σε αντίθετη περίπτωση θα καταστρατηγείται η εφαρμογή του άρθρου 265 ΚΠΔ, με αποτέλεσμα την συνεχή επέλευση δικονομικών ακυροτήτων της διαδικασίας.

Τέλος το ίδιο το κείμενο του άρθρου 265 ΚΠΔ, δέον να εμπλουτιστεί, ώστε αρχικώς να προβλέπει ρητά και να συμπεριλάβει και άλλες μορφές υλικών – ενσώματων αντικειμένων, που τυγχάνουν φορείς άυλων ψηφιακών δεδομένων, πέραν του ηλεκτρονικού υπολογιστή, όπως είναι έξυπνα ρολόγια, το σύνολο των έξυπνων συσκευών, των tablets κτλ., καθώς τα ψηφιακά δεδομένα που συλλέγονται από τις ως άνω πηγές, μπορούν να αποδειχθούν κομβικά στις έρευνες επί ποινικών υποθέσεων, δεδομένα τα οποία με το άρθρο 265 ΚΠΔ, όπως σήμερα ισχύει, μπορούν

μόνο με αναλογική εφαρμογή της διάταξης να αξιοποιηθούν, με τον κίνδυνο πρότασης δικονομικής ακυρότητας της διαδικασίας, είτε να επιτραπεί μόνον η κατάσχεση του υλικού – ενσώματου αντικειμένου στο οποίο ενσωματώνονται κατά τις διατάξεις 260 επ. ΚΠΔ. Επιπλέον, δέον να υπάρξει πρόβλεψη για πρόσβαση στα κατασχεθέντα ψηφιακά δεδομένα και η λήψη αντιγράφων αυτών από πλευράς του κατηγορουμένου και του παριστάμενου προς υποστήριξη της κατηγορίας, δικαιώματα που αναγνωρίζονται στα ως άνω πρόσωπα αναφορικά με ενσώματα – υλικά τμήματα της σχηματισθείσας δικογραφίας, όπως είναι τα έγγραφα. Ενώ τέλος, ο νομοθέτης θα πρέπει στο μέλλον να μεριμνήσει, ώστε ρητώς να συμπεριλάβει στο σώμα της διατάξεως του άρθρου 265 ΚΠΔ, πρόβλεψη αναφορικά με την τύχη των κατασχεθέντων ψηφιακών δεδομένων μετά το πέρας της ποινικής διαδικασίας, και στην αθώωσης ή της καταδίκης του κατηγορουμένου.

Βιβλιογραφία

- Ηλεκτρονικό Έγκλημα, επιμέλεια Θεοχάρης Ι Δαλακούρας, Εκδ. Νομική Βιβλιοθήκη, 2023
- ΠοινΔικ, [Νομική Βιβλιοθήκη], ISSN:1108-2755, τομ.24 τευχ.247 [2021] σελ.178-194
- ΠοινΔικ, [Νομική Βιβλιοθήκη], 3/2021 σελ.178-194
- Γνωμοδότηση ΑΠ 6/2021
- Αιτιολογική Έκθεση στο σχέδιο Νόμου με τίτλο «ΚΥΡΩΣΗ ΚΩΔΙΚΑ ΠΟΙΝΙΚΗΣ ΔΙΚΟΝΟΜΙΑΣ», 03.06.2019
- Αιτιολογική Έκθεση στο σχέδιο Νόμου, «Κύρωση της σύμβασης του συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο και του πρόσθετου πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω συστημάτων υπολογιστών – μεταφορά στο ελληνικό δίκαιο της οδηγίας 2013 / 40 / ΕΕ του ευρωπαϊκού κοινοβουλίου και του συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005 / 222 / ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις», Κεφάλαιο Α’, Β. Η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, σελ. 6.
- Η ΑΠΟΔΕΙΚΤΙΚΗ ΔΙΑΔΙΚΑΣΙΑ ΚΑΤΑ ΤΟΝ ΝΕΟ ΚΩΔΙΚΑ ΠΟΙΝΙΚΗΣ ΔΙΚΟΝΟΜΙΑΣ ΚΑΙ ΤΙΣ ΜΕΤΕΠΕΙΤΑ ΤΡΟΠΟ-ΠΟΙΗΣΕΙΣ ΤΟΥ, Θεοχάρης Ι. Δαλακούρας, https://www.esdi.gr/wpcontent/uploads/2022/seminars/10/zitimata-neou-PK/dalakouras_2022.pdf

- ΨΗΦΙΑΚΗ ΕΠΟΧΗ ΚΑΙ ΔΙΚΑΙΟΣΥΝΗ, ΣΥΓΧΡΟΝΕΣ ΜΟΡΦΕΣ ΕΓΛΗΜΑΤΙΚΟΤΗΤΑΣ, Λάμπρος Σ. Τσόγκας, Αντιεισαγγελέας Εφετών Θράκης, http://www.esdi.gr/nex/images/stories/pdf/epimorfosi/2021/tsogas_2021.pdf

- https://www.lawspot.gr/nomika-nea/psifiaki-edafikotita-topos-telesis-egklimatos-meso-diadiktyoy