Πανεπιστήμιο Μακεδονίας
Τμήμα Εφαρμοσμένης Πληροφορικής

Δημοκρίτειο Πανεπιστήμιο Θράκης
Τμήμα Νομικής

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Η Ανακριτική Διερεύνηση Ηλεκτρονικών Εγκλημάτων.

Όρια και έκταση εφαρμογής της εγχώριας και διεθνούς πρακτικής υπό το φως των εγγυήσεων προστασίας των ατομικών δικαιωμάτων και της νομολογίας του ΕΔΔΑ.

Διπλωματική Εργασία

του

Θεόφιλου Συλβ. Παπαδόπουλου

mli 19009

Θεσσαλονίκη, Ιούλιος 2020

Θέμα Διπλωματικής:

Η Ανακριτική Διερεύνηση Ηλεκτρονικών Εγκλημάτων.

Όρια και έκταση εφαρμογής της εγχώριας και διεθνούς πρακτικής υπό το φως των εγγυήσεων προστασίας των ατομικών δικαιωμάτων και της νομολογίας του ΕΔΔΑ.

Θεόφιλου Συλβ. Παπαδόπουλου

mli 19009

e-mail: mli19009@uom.edu.gr

Διπλωματική Εργασία

που υποβάλλεται στα πλαίσια προγράμματος και για την εκπλήρωση ακαδημαϊκών απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΛΟΥ ΣΠΟΥΔΩΝ

ΣΤΟ

ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Θεοχάρης Ι. Δαλακούρας

…… από την τριμελή εξεταστική επιτροπή ……

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

ΠΕΡΙΛΗΨΗ

Σε ένα σύγχρονο περιβάλλον αξιολόγησης και της παραμικρής ακόμη πτυχής ανάμειξης των τεχνολογιών πληροφορικής κι επικοινωνιών, είναι σχεδόν στερεότυπο να γίνεται λόγος για εισβολή και ραγδαία ενσωμάτωση της τεχνολογίας στην καθημερινότητα. Πρόκειται για μια συνθήκη προσχώρησης, όπου ο μέσος άνθρωπος (και αναγκαστικά χρήστης) δεν έχει δυνατότητα επιλογής αλλά απλά συμμόρφωσης.

Μέσα σε αυτό το τεχνολογικό υπόβαθρο, καλείται να αφομοιωθεί η κοινωνία της πληροφορίας, να αξιοποιηθεί ως ατομική ελευθερία και να αξιολογηθεί στην τεχνική αλλά και την κοινωνιολογική της βάση. Μόνο που η βασική έννοια της ελευθερίας όπως και κάθε έννοια ελευθερίας, όπως οι συνταγματικώς κατοχυρωμένες ατομικές ελευθερίες, προαπαιτούν το ίδιο το υποκείμενο – φορέας του σχετικού δικαιώματος να έχει κατανοήσει την δομή και την ουσία της ώστε να εντοπίζει στην καθημερινότητά του τον ατομική σκληρό πυρήνα της ελευθερίας του.

Ως κοινωνική συνθήκη πλέον η ψηφιακή κοινότητα, λειτουργεί στις δομές της κάθε κοινωνίας, χωρίς να είναι απαλλαγμένη από παράνομες συμπεριφορές. Στον ψηφιακό αυτόν κόσμο η εγκληματική δράση λαμβάνει ειδικούς προσανατολισμούς, καινοφανείς μορφές, επιφέροντας ζημιογόνα αποτελέσματα πρωτόγνωρα αλλά και ουσιώδη. Με ιδιαίτερα χαρακτηριστικά την ταχύτητα και την έκταση της ζημίας που επέρχεται, η αντίδραση της συντεταγμένης πολιτείας σε επίπεδο νομικό και της κοινωνίας σε επίπεδο κοινωνιολογικό, είναι επιβεβλημένη.

Το ιδιαίτερο χαρακτηριστικό της διασυνοριακής εμφάνισης του ηλεκτρονικού εγκλήματος, όσα νομικά προβλήματα και αν δημιουργεί, επέβαλε την διεθνή συνεργασία, η οποία με την σειρά της καθόρισε πρωτόκολλα συμπεριφοράς και πλαίσια δράσης των αρχών για την καλύτερη καταπολέμησή του. Τμήμα της ερευνητικής αυτής δομής που άγει στην κρίση κάθε συμπεριφοράς από την ανεξάρτητη δικαστική αρχή, είναι και αυτό της προδικασίας.

Είναι το τμήμα της νόμιμης έρευνας, που εξασφαλίζει συνθήκες, διαδικασίες και καθορίζει ασφαλιστικές δικλείδες αναφορικά με το αποδεικτικό υλικό που είναι χρήσιμο για την αξιολόγηση της πράξης που ελέγχεται. Είμαστε στο περιβάλλον της προδικασίας σε μια ποινική δίωξη και στο κρίσιμο για την εξασφάλιση του αποδεικτικού υλικού στοιχείο της κατάσχεσης ως ανακριτικής πράξης. Στα πλαίσια αυτά και σε συμμόρφωση με την Σύμβαση της Βουδαπέστης ο έλληνας νομοθέτης με την εισαγωγή του νέου Κώδικα Ποινικής

Δικονομίας, καθόρισε ως διακριτή διαδικασία την κατάσχεση των ψηφιακών δεδομένων, διαδικασία την οποία διέκρινε από τις παραδοσιακές μορφές της κατάσχεσης.

Στην μελέτη αναπτύσσονται οι παράμετροι και οι ειδικές συνθήκες που αφορούν στην λειτουργία του ψηφιακού κόσμου μέσα στον οποίον παράγονται και διατηρούνται τα ψηφιακά δεδομένα, τα οποία συνδέονται με τις εγκληματικές συμπεριφορές στον κυβερνοχώρο. Ακολούθως αποδίδεται η πρακτική αντιμετώπιση των καταστάσεων αυτών και οι προβληματισμοί που ανακύπτουν αναφορικά με την προσπάθεια νομικού εξορθολογισμού της επιστήμης της πληροφορικής.

Οι σχετικές παρατηρήσεις συνδυάζονται με τις κρίσεις που κατά καιρούς έχει εκφέρει το Ευρωπαϊκό Δικαστήριο των δικαιωμάτων του ανθρώπου, αναφορικά με τα όρια και τα πλαίσια δράσης των αρχών στην σύγκρουσή τους με τις ατομικές ελευθερίες του ανθρώπου. Σε όλη την πορεία των σκέψεων που εκτίθενται γίνονται οι αναγκαίες αναφορές σε επιλογές ξένων δικαιϊκών συστημάτων.

Λέξεις κλειδιά: Ηλεκτρονικό Έγκλημα, Κυβερνοχώρος, Ποινικό Δίκαιο, Κώδικας Ποινικής Δικονομίας, Προδικασία, Ανάκριση, Κατάσχεση, Ψηφιακά πειστήρια, Ψηφιακά δεδομένα, Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου, κατηγορούμενος, υπεράσπιση, ατομικά δικαιώματα, Διεθνής Συνθήκη για το έγκλημα στον Κυβερνοχώρο.

Δήλωση περί λογοκλοπής

Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις που προβλέπονται από τις διατάξεις της παραγράφου 1 του Άρθρου 4.2 (Υποχρεώσεις Φοιτητών) του Κανονισμού Λειτουργίας του Δ.Π.Μ.Σ. «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ», δηλώνω υπεύθυνα ότι στη συγγραφή της διπλωματικής μου εργασίας, η οποία είναι προϊόν αποκλειστικά προσωπικής μου εργασίας, δεν εμπεριέχονται στοιχεία λογοκλοπής και γενικότερα δεν παραβιάζονται οι διατάξεις περί διανοητικής ιδιοκτησίας Δεν χρησιμοποιήθηκαν πηγές πέραν αυτών που περιλαμβάνονται στις βιβλιογραφικές αναφορές. Παρέχω τη συναίνεσή μου, ώστε ένα ηλεκτρονικό αντίγραφο της διπλωματικής εργασίας μου να υποβληθεί σε ηλεκτρονικό έλεγχο για τον εντοπισμό τυχόν στοιχείων προσβολής πνευματικής ιδιοκτησίας.

ABSTRACT

In a modern environment of evaluation and the slightest aspect of the mixing of information and communication technologies, it is almost a stereotype to talk about invasion and rapid integration of technology in everyday life.

In this technological background, it is called upon to assimilate the information society, to use it as individual freedom and to evaluate it in its technical and sociological basis. Only the basic concept of freedom, like any notion of freedom, such as constitutionally guaranteed individual freedoms, requires the subject-institution itself to have understood its structure and essence in order to identify its individual hard core in its daily life. of his freedom.

As a social condition, the digital community now operates in the structures of any society, without being free from illegal behaviors. In this digital world, criminal activity takes on special orientations, new forms, causing unintended and unprecedented damaging results. With particular characteristics of the speed and extent of the damage that occurs, the reaction of the coordinated state at the legal level and society at the sociological level is imperative.

The special feature of the cross-border appearance of cybercrime, no matter how many legal problems it creates, imposed international co-operation, which in turn set behavioral protocols and action frameworks for better control. Part of this research structure that judges every behavior by the independent judiciary is that of pre-trial detention.

It is part of the legal investigation, which ensures conditions, procedures and determines safety valves regarding the evidence that is useful for the evaluation of the act under review. We are in the pre-trial environment in a criminal prosecution and in the critical element of securing the evidence, the seizure as an investigative act. In this context and in compliance with the Budapest Convention, the Greek legislator, with the introduction of the new Code of Criminal Procedure, defined as a distinct process the seizure of digital data, a process which he distinguished from the traditional forms of seizure.

The study develops the parameters and specific conditions related to the operation of the digital world in which digital data are produced and maintained, which are associated with criminal behavior in cyberspace. The practical treatment of these situations and the concerns that arise regarding the attempt to legally rationalize the science of informatics are then attributed.

The relevant observations are combined with the crises that the European Court of Human Rights has from time to time expressed regarding the limits and frameworks of action of the authorities in their conflict with individual human freedoms. Throughout the course of the thoughts presented, the necessary references are made to choices of foreign legal systems.

Keywords: Cybercrime, Cyberspace, Criminal Law, Code of Criminal Procedure, Prejudice, Interrogation, Seizure, Digital Evidence, Digital Data, European Court of Human Rights, Defendant for Conviction, Defender of the Covenant, Human Rights, International Convention on the Crime of Cybercrime.

Κάποιες σκέψεις κι ευχαριστίες.

Δεν θα αξιολογήσω το κοινότυπο ή μη μιας καταγραφής όπως και αυτή εδώ. Είμαι όμως βέβαιος ότι είναι μια πηγαία ανάγκη του κάθε φοιτητή μετά από την εργώδη προσπάθεια για τη σύνταξη μιας διπλωματικής μελέτης, που ακαδημαϊκά άγει στην ολοκλήρωση ενός κύκλου σπουδών. Πρόκειται για μια ιδιόμορφη συνθήκη συγγραφής λίγο πριν το τέλος μιας περιόδου μαθητείας σε ένα ιδιαίτερα απαιτητικό πεδίο, όπως αυτό του συνδυασμού των επιστημών της νομικής και της πληροφορικής, μέσα από το καινοτόμο, για τα ακαδημαϊκά μας δεδομένα, Διιδρυματικό Πρόγραμμα Μεταπτυχιακών Σπουδών στο «Δίκαιο και την Πληροφορική».

Προσωπικά φτάνοντας στον τερματισμό ενός ακόμη (αυτήν την φορά ακαδημαϊκού) Μαραθωνίου, σύμμεικτα κινούνται γύρω μου στιγμές ενδιαφέροντος για νέα γνωστικά πεδία, που συγκρούονται με ώρες φόρτισης υπό το βάρος των πιεστικών επαγγελματικών προγραμμάτων μου. Ώρες εργασίας σε ένα πολύ ενδιαφέρον και ολοκαίνουργιο παράθυρο στον κόσμο, με τις ανάλογες δυσχέρειες στην κατανόησή του καθώς διατηρώ ακαδημαϊκές καταβολές από έναν πολύ διαφορετικό χώρο, αυτόν της νομικής.

Και κάπου εδώ μια στάση ζωής μέσα από τις γνωριμίες με εξαιρετικούς φίλους (θα τους αδικούσα αν τους περιόριζα στον χαρακτηρισμό συμφοιτητές), από τους οποίους, ας μου επιτραπεί εδώ, έχοντας μεγάλη ηλικιακή απόσταση, από την συντριπτική τους πλειοψηφία, διδάχθηκα ότι ο ακαδημαϊκός χώρος έχει ανεξίτηλη φρεσκάδα και μονοσήμαντη πορεία προς την βελτίωση, όποτε και αν τον συναντήσεις στην ζωή σου, η οποία τηρεί τους ρυθμούς που εσύ της επιτρέπεις. Κοντά σε αυτό το άριστο περιβάλλον βάσης, η πορεία προς την ειδική γνώση στηρίχθηκε σε εξαιρετικούς καθ(οδηγ)ητές. Κάποιους ίσως του στενοχώρησα, ίσως δεν ανταποκρίθηκα στις απαιτήσεις τους, εκείνοι όμως ξεπέρασαν τις δικές μου προσδοκίες. Με τις άοκνες, πεισματικές και σοβαρές προσπάθειές τους μου δίδαξαν νέα ερευνητικά πεδία, με δέχθηκαν ως ισότιμο ακαδημαϊκό πολίτη και μου συμπεριφέρθηκαν άριστα. Είναι στιγμές που αν τις καταγράψω λεπτομερώς ομολογουμένως η συγκίνηση, από σεβασμό και μόνο, δεν θα επέτρεπε την ολοκλήρωση των σκέψεων.

Φυσικά όλα αυτά δεν θα μπορούσαν να λειτουργήσουν χωρίς την άριστη λειτουργία του προγράμματος υπό την Διεύθυνση της κας Ευγενίας Αλεξανδροπούλου – Αιγυπτιάδου. Ως ελάχιστη ηθική υποχρέωση προς την Διευθύνουσα κα Καθηγήτρια θέλω να δηλώσω ότι έμαθα, και έμαθα πολλά, χρήσιμα και ενδιαφέροντα και ως ελάχιστη υποχρέωσή μου, θα

επιμείνω στην προαγωγή του επιστημονικού λόγου στο οικείο ερευνητικό πεδίο του μεταπτυχιακού αυτού.

Ιδιαίτερες ευχαριστίες οφείλω στον επιβλέποντα καθηγητή κ. Θεοχάρη Δαλακούρα, που με τις καίριες παρατηρήσεις του, την αμέριστη συμπαράστασή του και την άριστη επιστημονική του καθοδήγηση, με οδήγησε στην εκπόνηση της μελέτης αυτής. Θέλω να πιστεύω ότι λειτούργησα αντάξια στην εμπιστοσύνη που μου έδειξε με την ανάθεση της συγκεκριμένης εργασίας και της αρωγής που μου παρείχε.

Φτάνοντας λοιπόν εδώ, θα κλείσω τις σκέψεις αυτές με έναν παραλληλισμό. Η χαρά και ο ενθουσιασμός για τον τερματισμό μου αυτόν μου φέρνει συνειρμούς ψυχικής ανάτασης κατά την ώρα του τερματισμού μου στο Καλλιμάρμαρο στον πρώτο μου Αυθεντικό Μαραθώνιο δρόμο. Όπως κι εκεί η στιγμή του μεταλλείου ήταν εξίσου έντονη με όλες τις άλλες στιγμές, της εκκίνησης, της διαδρομής όσο και της εισόδου στο στάδιο. Έτσι κι εδώ το πρώτο μάθημα στο εργαστήριο 334, μέχρι την τελευταία εξέταση στο ακροατήριο 13 είναι στιγμές αποκτήματα. Καμιά δεν ξεχωρίζω και είναι όλες ανεξίτηλα χαραγμένες στην καρδιά μου.

Από καρδιάς ένα μεγάλο ευχαριστώ.

Θεσσαλονίκη, Ιούλιος 2020

Και μια Αφιέρωση...

Όταν γράφονται αυτές εδώ οι αράδες η μελέτη είναι ακόμη σε παραγωγική διεργασία. Εκέφες εδώ, σημειώσεις εκεί και λίγο παραπέρα μια κούπα με καφέ. Τίποτε όμως δεν θα μπορούσε να αυτοτελέσει αρχή, μέση και τέλος χι αυτήν την μελέτη και για όλη μου την μαθητεία, αν δεν είχα την στήριξη των προσώπων στα οποία την αφιερώνω.

Στην ανάσα και πνοή μου αυτό το 1998, τον γιο μου και γιό μου Σιλβέστρο – Θεμιστοκλή...

Στην καρδιά μου αυτό το 2002, την ψυχή μου και κόρη μου Καλλιόπη...

Αλλά και στην παντοτινή αγάπη μου Ελένη που μου τους χάρισε...

Σας λατρεύω και σας ευχαριστώ

ΔΙΑΤΑΞΗ ΥΛΗΣ

1. ΕΙΣΑΓΩΓΙΚΗ ΑΝΑΦΟΡΑ

i. Προεισαγωγή.

Κοινή παραδοχή αποτελεί το γεγονός ότι οι κοινωνίες μας ψηφιοποιούνται ολοένα και περισσότερο. Ο ρυθμός των τεχνολογικών εξελίξεων και ο τρόπος επεξεργασίας των δεδομένων προσωπικού χαρακτήρα επηρεάζουν σε καθημερινή βάση τον καθένα από εμάς με πολλούς και διάφορους τρόπους[1].

Σε ένα σύγχρονο περιβάλλον αξιολόγησης και της παραμικρής ακόμη πτυχής ανάμειξης των τεχνολογιών πληροφορικής κι επικοινωνιών, είναι σχεδόν στερεότυπο να γίνεται λόγος για εισβολή και ραγδαία ενσωμάτωση της τεχνολογίας στην καθημερινότητα. Εισβολή διότι η εμφάνιση κάθε νέας τεχνολογίας δεν απαιτεί, ή πολύ περισσότερο, δεν επιτρέπει, την προηγούμενη επεξεργασία, αποδελτίωση και ανάλυσή της, με σκοπό την αποδοχή της από την κοινωνία. Πρόκειται για μια συνθήκη προσχώρησης, όπου ο μέσος άνθρωπος (και αναγκαστικά χρήστης) δεν έχει δυνατότητα επιλογής αλλά απλά συμμόρφωσης. Πώς θα μπορούσε λ.χ. να ανταπεξέλθει μια επαγγελματική δραστηριότητα εκτός περιβάλλοντος διαδικτύου; Ποια η ανταγωνιστικότητα ενός επιτηδευματία, που επιλέγει να επιχειρεί χωρίς ένα smartphone; Πώς μπορεί ένας δημοσιογράφος να λειτουργεί σήμερα, αποξενωμένος από εφαρμογές κοινωνικής δικτύωσης, οι οποίες ολοένα και περισσότερο αποτελούν πλέον πεδίο ενδυνάμωσης του πολιτικού προφίλ των ανθρώπων επιχειρούν από τις εξουσιαστικές θέσεις; Ραγδαία δε ενσωμάτωση, διότι κάθε αναβάθμιση της τεχνολογίας καθιστά ξεπερασμένη και σχεδόν ανενεργή κάθε προηγούμενη έκδοσή της, με αναπόδραστη συνέχειά της την επικαιροποίηση κάθε εφαρμογής. Το «σχεδόν ανενεργή» αναφέρεται στην αδυναμία (εκτιμώ τεχνηέντως δοσμένη) υποστήριξης των νέων δυνατοτήτων της εφαρμογής.

Και μέσα σε αυτό το τεχνολογικό υπόβαθρο, καλείται να αφομοιωθεί η κοινωνία της πληροφορίας, να αξιοποιηθεί ως ατομική ελευθερία και να αξιολογηθεί στην τεχνική αλλά και την κοινωνιολογική[2] της βάση. Μόνο που η βασική έννοια της ελευθερίας και κάθε

[1] Βλ. Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, εκδ. 2018, σελ. 3 σε https://www.coe.int/dataprotection

[2] Βλ. *Ειρ. Καμπερίδου*, Ψηφιακές δεξιότητες και ψηφιακός αποκλεισμός: Γεφυρώνοντας το έμφυλο ψηφιακό χάσμα (Digital skills and digital exclusion: Bridging the gender digital divide), αλλά και γενικότερα σε

έννοια ατομικού δικαιώματος, όπως οι συνταγματικώς κατοχυρωμένες ατομικές ελευθερίες, προαπαιτούν το ίδιο το υποκείμενο – φορέας του σχετικού δικαιώματος να έχει κατανοήσει την δομή και την ουσία της ώστε να εντοπίζει στην καθημερινότητά του τον ατομικό σκληρό πυρήνα της ελευθερίας του. Αυτό το τελευταίο με την σειρά του απαιτεί βαθιά κατανόηση και φυσικά κτήση των σχετικών εφοδίων αντίληψης της λειτουργίας του δικαιώματος στην κοινωνία της πληροφορίας

Έτσι με την σειρά αναδεικνύεται ως κρίσιμος ο *ψηφιακός γραμματισμός*[3], ο οποίος αποτελεί πρόκληση αλλά και στοίχημα των νέων κοινωνικών δομών, παριστάμενος ως βασική προϋπόθεση εισαγωγής – προετοιμασίας της κοινότητας για τον ψηφιακό *ανθρωπισμό*[4]. Στην επερχόμενη εικονική κοινωνία, όπου οι παραδοσιακές δομές και δεσμοί αντικαθίστανται από αλγορίθμους, με κινδυνολογούμενη την βιολογική μετάλλαξή του ανθρώπου σ' ένα, κατά συνθήκη ανοχής, αποδεκτό είδος, αυξάνονται οι απαιτήσεις, όχι απλά να προσαρμοστούμε βαθμιαία στην τεχνική εξέλιξη, αλλά να συμβιβαστούμε με τον απώτερο σκοπό, που είναι η ενσωμάτωσή μας σε αυτήν, διότι το αντίστροφο εκτιμώ ότι και τεχνικά είναι ανέφικτο αλλά και ηθικά ανεπίτρεπτο.

Φυσικά όπως σε κάθε εποχή σταθμό στην ιστορία του ανθρώπινου γένους, τον αρχικό ενθουσιασμό για το επίτευγμα διαδέχεται ένας αγώνας δρόμου και ανταγωνισμού με διαρκείς βελτιώσεις στην καινοτόμα συνθήκη και αναβαθμίσεις στην εκάστοτε παρεχόμενη υπηρεσία. Οι τεχνολογίες πληροφοριών και επικοινωνιών, ως πρακτική διείσδυση με αγοραστική δυναμική κυρίως[5], δεν θα μπορούσαν να αποτελέσουν εξαίρεση. Ας μην λησμονείται το γεγονός ότι μελετητές αναφέρονται στην εισβολή των καινοτόμων τεχνολογιών αιχμής, ως

πρακτικά 6ου Τακτικού Συνεδρίου της ΕΚΕ, «Η Κοινωνιολογία και ο Δημόσιος Ρόλος της στην Εποχή της Μεταμόρφωσης του Κόσμου», Ελληνική Κοινωνιολογική Εταιρεία, 2018.

[3] Βλ. *Δ. Σπανός, Α. Σοφός, Β. Οικονόμου*, Οι συνέπειες ως προς τον ψηφιακό γραμματισμό των μαθητών σε περιβάλλον ενός φορητού υπολογιστή ανά μαθητή, https://economu.wordpress.com/11-2/.

[4] Βλ. ενδεικτικά *Θ. Τάσης*, Ψηφιακός Ανθρωπισμός, Εικονιστικό υποκείμενο και τεχνητή νοημοσύνη, εκδ. Αρμός 2019. *Th. Porter*, History of Psychology, Vol 21(4), Nov 2018, 369-373, *Silvia Barnová, Slávka Krásna*, Digital Humanism in Education – Meaningful Use of Digital Technologies, 2nd International EMI Entrepreneurship & Social Sciences Congress, 09-11 November 2018, Cappadocia, https://www.researchgate.net/profile/Silvia_Barnova/publication/330345608_Digital_Humanism_in_Education_-_Meaningful_Use_of_Digital_Technologies/links/5c3a15efa6fdccd6b5a752ec/Digital-Humanism-in-Education-Meaningful-Use-of-Digital-Technologies.pdf.

[5] Βλ. *N. Shaukata, S.M. Alia, C.A. Mehmooda, B. Khana, M. Jawadb, U. Farida, Z. Ullaha, S.M. Anwarc, M. Majidd*, A survey on consumers empowerment, communication technologies, and renewable generation penetration within Smart Grid, Renewable and Sustainable Energy Reviews, Volume 81, Part 1, January 2018, Pages 1453-1475, https://www.researchgate.net/profile/Zahid_Ullah2/publication/317621899_A_survey_on_consumers_empowerment_communication_technologies_and_renewable_generation_penetration_within_Smart_Grid/links/5b9e8dc5a6fdccd3cb5dd08b/A-survey-on-consumers-empowerment-communication-technologies-and-renewable-generation-penetration-within-Smart-Grid.pdf

μια *νέα βιομηχανική επανάσταση*[6]. Η λειτουργική δομή του παγκόσμιου ιστού[7], του διαδικτύου[8], της πληθώρας των εφαρμογών αλλά και του συνόλου των πληροφοριών, ενσωματώθηκε στην καθημερινή κοινωνική διαβίωση, αποτέλεσε βάση για την αναμόρφωση των ανθρωπίνων συμπεριφορών και, όπως ήταν λογικά ακόλουθο, επηρέασε το σύνολο των ανθρωπίνων δραστηριοτήτων.

Η συγκεκριμένη προεισαγωγή ίσως είχε τον χαρακτήρα μιας *ενθουσιώδους όσο και εντυπωσιακής προλόγησης* πολλά έτη πριν. Πλην όμως, τα τελευταία έτη, μάλλον αποτελεί μια κοινά αποδεκτή συνθήκη, που, με όχι καθορισμένο τρόπο, αλλά με βεβαιότητα, αντιμετωπίζεται ως το αναμενόμενο στο άμεσο μέλλον. Την ίδια στιγμή οι τεχνολογίες πληροφορικής κι επικοινωνιών ως τεχνολογία αιχμής νοούμενες, από μόνα τους είναι μια μεταβλητή συνθήκη, που με τη σειρά της ξεκαθαρίζει ότι όροι όπως στατικότητα, σταθερότητα και μονιμότητα, είναι ξένοι στο σχετικό γλωσσάρι της πληροφορικής.

Η αναμονή στα όρια της προσμονής για κάθε επόμενη εξέλιξη έχει πάντοτε το στοιχείο του θαυμασμού, της περιέργειας αλλά και του αιφνιδιασμού πολλές φορές. Κατά μια προσλαμβάνουσα έκφανση της καθημερινής αντίληψης των επιτευγμάτων της, οι τεχνολογίες αιχμής έχουν την δυναμική της διαρκούς βελτίωσης, της ανάπτυξης, της ανατροπής αλλά και του εντυπωσιασμού της κοινότητας, τόσο σε επίπεδο επιστημόνων όσο και σε επίπεδο χρηστών. Η δυναμική τους αυτή δίνει την αίσθηση μιας ταχύτατης εναλλαγής, που στοχεύει, μεταξύ άλλων, στον αμυντικό αφοπλισμό του μέσου χρήστη, ούτως ώστε η ανάγκη κατανόησης των νέων δεδομένων να θέτει ταχύτατα σε αδράνεια ή λησμοσύνη τις χθεσινές απορίες ή ενστάσεις αναφορικά με τις σκοπιμότητες στις οποίες αποβλέπουν.

Η πληροφορία που συσσωρεύεται σε καθημερινή βάση, ανάμεικτη με απορίες κι ερωτήματα, που πρωτίστως στοχεύουν στην κατανόηση λειτουργίας κι εφαρμογής (πολλές φορές άκριτα και καταχρηστικά) των νέων δεδομένων και ακολούθως στην ερμηνεία τους,

---

[6] Βλ. *M Yar, KF Steinmetz*, Cybercrime and society, SAGE 2019, σελ. 4., https://books.google.gr/books?id=_nN7DwAAQBAJ&printsec=frontcover&hl=el&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

[7] Βλ. Παγκόσμιος ιστός και Internet συχνά θεωρούνται το ίδιο πράγμα. Η αντίληψη αυτή είναι λανθασμένη καθώς ο ιστός αποτελεί μία μόνο εφαρμογή του Internet. Για την ακρίβεια, την δημοφιλέστερη. Σε αντίθεση με το Internet, που έχει και υλική υπόσταση, ο ιστός δεν έχει, μιας και αποτελείται από πακέτα πληροφορίας. Η τεχνολογία του ιστού καθιστά δυνατή την δημιουργία "υπερκειμένων", μία διασύνδεση δηλαδή πάρα πολλών μη ιεραρχημένων στοιχείων που παλαιότερα ήταν απομονωμένα. Τα στοιχεία αυτά μπορούν να πάρουν και άλλες μορφές πέραν της μορφής του γραπτού κειμένου, όπως εικόνας και ήχου. βλ. και https://el.wikipedia.org/wiki/.

[8] Βλ. Βλ. *Cl. Hewson, D.W. Stewart*, Internet Research Methods, 2016, https://onlinelibrary.wiley.com/doi/full/10.1002/9781118445112.stat06720.pub2, D. Miller and D. Slater, The Internet, An Ethnographic Approach, Oxford 2000, https://dourish.com/~dourishc/classes/readings/MillerSlater-InternetChapter1.pdf, https://el.wikipedia.org/wiki.

αποτελεί μέγεθος δυσθεώρητο ως προς την επεξεργασία και τους απαραίτητους προς διάθεση πόρους, την ίδια όμως στιγμή είναι μια απαραίτητη υπηρεσία – παροχή των σύγχρονων κοινοτήτων προς τα μέλη τους.

Ο τρόπος, με τον οποίον οι τεχνολογίες αιχμής, επηρεάζουν την οικονομική, κοινωνική, κοινωνιολογική, πολιτιστική, ηθική, πολιτική, εργασιακή, αλλά και τεχνική[9] δομή των κοινοτήτων, είναι πολύπλευρη[10], πολυσχιδής, πολυεπίπεδη και πολυσήμαντη. Φυσικά η περαιτέρω ενασχόληση, με την έννοια της εμβάθυνσης σε όλες αυτές τις πτυχές της τεχνολογικής παρουσίας στην κοινότητα, εκφεύγει των ορίων της παρούσας μελέτης. Μέσα όμως σε όλο αυτό το τεχνολογικό καινοτόμο γίγνεσθαι[11], οι όροι και παράμετροι λειτουργικής ενσωμάτωσής τους, δεν παύει σε μια συντεταγμένη κοινωνία να είναι έργο του νομοθέτη. Κανόνες δικαίου, πολλές φορές ή σε αρκετά σημεία, λειτουργώντας ως ένα αταίριαστο σύμμεικτο με τον καθορισμό τεχνικών και τεχνολογικών κανόνων και ορισμών, συνθέτουν ένα πλαίσιο εξορθολογισμού των νέων τεχνολογιών, όχι πάντοτε ακριβές, ασφαλές και καλότεχνο.

Χρήση και υπερβολή των τεχνολογιών αιχμής είναι η γνωστή σχέση δράσης και αντίδρασης στον κοινωνικό στίβο, που παρουσιάζεται στη διαχείριση κι εφαρμογή πολλών ανθρωπίνων επιτευγμάτων, σε μια συσχέτιση δικαιώματος και παρανομίας ή κατάχρησης. Μέχρι και σήμερα οι νέες τεχνολογίες, ως κατεξοχήν ανθρώπινο δημιούργημα, ενσωματώνουν πάντα αυτόν τον κίνδυνο μιας αρνητικής παράστασης στις κοινωνικές δομές, μέσα από μη εκλογικευμένες χρήσεις, ή μέσα από χρήσεις τεχνολογικά αποδεκτές και εφαρμόσιμες αλλά για σκοπούς πολύ διαφορετικούς από εκείνους για τους οποίους προορίστηκαν κατά την ανάπτυξή τους. Όλα βέβαια τα παραπάνω αποκτούν μια πιο πολύπλοκη διάσταση αν αναλογιστεί κανείς ότι πλέον εξελικτικό παράγοντα στα νέα δεδομένα και τις νέες τεχνολογικές δομές καλείται να διαδραματίσει ρόλο και η τεχνητή νοημοσύνη.

---

[9] Βλ. *Chr. Stergiou, K. Psannis, Br. Gupta, Yut. Ishibashi*, Security, Privacy and Efficiency of Sustainable Cloud Computing for Big Data and IoT, 2018, https://www.researchgate.net/profile/Kostas_Psannis/publication/325767407_Security_Privacy_Efficiency_of_Sustainable_Cloud_Computing_for_Big_Data_IoT/links/5b2c12564585150d23c1a958/Security-Privacy-Efficiency-of-Sustainable-Cloud-Computing-for-Big-Data-IoT.pdf

[10] Βλ. *Ι. Αγγελή*, Διαδίκτυο και ποινικό δίκαιο, ΠοινΧρον 2000, σελ. 676, με τις εκεί υποσημειώσεις και παραπομπές ειδικότερα δε με αναφορά στις σημειώσεις αρ. 8 έως και 16.

[11] Βλ. *Chr. Stergiou and K. Psannis*, Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: a survey, 2017, international journal of network management, Int. J. Network Mgmt, Published online in Wiley Online Library (wileyonlinelibrary.com) DOI: 10.1002/nem.1930,

Καθώς κοιτάζουμε μπροστά, σε έναν κόσμο αναπτυσσόμενης πανταχού πληροφορικής, η πρόκληση της εγκληματολογικής διαδικασίας, όπως η απόκτηση δεδομένων (λογική και φυσική) και η εξαγωγή και ανάλυση δεδομένων αυξάνεται σε αυτόν τον χώρο.

Το Internet of Anything (IoA)[12] φέρνει οτιδήποτε και όλα online σε μια σύνδεση και αλληλεπίδραση, που δημιουργεί μια έκρηξη συνδεδεμένων συσκευών, από ψυγεία, αυτοκίνητα και drone, έως έξυπνα σμήνη, έξυπνα συμπλέγματα αντικειμένων, έξυπνα κτίρια, πόλεις κοκ. Είναι απαραίτητη η έρευνα για τον προσδιορισμό μεθόδων για την εκτέλεση ψηφιακής ιατροδικαστικής ανάλυσης με βάση το Internet of Things (IoT). Ο διαφαινόμενος μακροπρόθεσμος στόχος είναι η ανάπτυξη ψηφιακών ιατροδικαστικών προτύπων και μοτίβων, τα οποία μπορούν να χρησιμοποιηθούν ως μέρος της συνολικής ασφάλειας IoT και IoA και να βοηθήσουν σε έρευνες που βασίζονται σε IoT.

Εδώ λοιπόν γίνεται λόγος για την χρήση των τεχνολογιών πληροφορικής κι επικοινωνιών στα πλαίσια μιας δράσης ή συμπεριφοράς, που ελέγχεται από πλευράς νομιμότητας και ειδικότερα συμπεριφορές αξιόποινης. Κινούμαστε πλέον στον χώρο του ηλεκτρονικού εγκλήματος.

ii. Ο προβληματισμός στην διαχείριση του ερευνητικού αντικειμένου.

Όταν καλείται ένας επιστήμονας να λειτουργήσει βάσει της επιστημοσύνης του, να αξιολογήσει και να αξιολογηθεί η εργασία του πάνω σε ένα αντικείμενο διαφορετικό, ή σε μια πιο δύσκολη συνθήκη, ξένο σε σχέση με το κατεξοχήν γνωστικό του αντικείμενο, εκεί σαφώς και κάθε προβληματισμός αποκτά άλλες διαστάσεις. Όταν λοιπόν καλείται ένας νομικός να αξιολογήσει μια συνθήκη της πληροφορικής τότε τα δύο αντικείμενα που πρέπει να συλλειτουργήσουν είναι γνώσεις και παραστάσεις αφ' ενός από το νομικό κόσμο και αφ' ετέρου από το πεδίο πληροφορικής και των τεχνολογιών αναφορικά με τον ειδικότερο τομέα των ηλεκτρονικών επικοινωνιών και των δικτύων. Για την περίπτωση της νομικής, υπάρχει ιδιαιτερότητα καθόσον αν αφαιρούσε κανείς την ιατρική, όλες οι άλλες επιστημονικές διαδρομές φαίνεται να συγκλίνουν με την έννοια ότι παρίστανται περισσότερο ή λιγότερο η καθεμιά ως συνθήκες συλλειτουργούσες. Ενδεικτικά αναφερόμενο, αλλά σημειολογικά

[12] Βλ. *Áine MacDermott, Th. Baker, Qi Shi*, IoT Forensics: Challenges For The IoA Era, https://www.google.com/search?q=IoT+Forensics%3A+Challenges+For+The+IoA+Era&rlz=1C1NDCM_enGR841GR841&oq=IoT+Forensics%3A+Challenges+For+The+IoA+Era&aqs=chrome..69i57.1845j0j8&sourceid=chrome&ie=UTF-8.

διδόμενο, το γεγονός ότι δεν πρέπει να λησμονούμε το πεδίο της φυσικής επιστήμης στην διαχείριση της μεταφοράς πακέτων κατά τον διαχωρισμό σε στρώματα (layers)[13], όπου το φυσικό στρώμα φέρεται να είναι το τελευταίο της συγκρότησης του πακέτου από τον αποστολέα για την μεταφορά αλλά και το πρώτο για την διακίνηση προς τον παραλήπτη. Η απόσταση της φυσικής από την πληροφορική δεν μπορεί να συγκριθεί με την αντίστοιχή της με τη νομική επιστήμη.

Τα πράγματα γίνονται ιδιαίτερα έντονα όταν την σχετική ζεύξη γνώσεων και μάλιστα όχι στο ίδιο επίπεδο επάρκειας κατά συνήθη συνθήκη, καλείται να λειτουργήσει δικαστικός λειτουργός, ή ανακριτικός υπάλληλος, με τις εξουσιαστικές και δραστικές συνέπειες των θεσμικών του ενεργειών να καθορίζουν κυριολεκτικά τύχες ανθρώπων και να χαράζουν (για να μην πω να προδιαγράφουν) την δικαστική διαχείριση των αντικειμένων, που ανέδειξε η ανακριτική έρευνα.

Κάπου εδώ έχουν την θέση τους και οι θεωρητικοί προβληματισμοί αναφορικά με την προσέγγιση νομικών θεμάτων στον κυβερνοχώρο, στοιχείο, που ενέχει την προϋπόθεση όχι μόνο νομικών γνώσεων αλλά και τεχνικών γνώσεων σε ζητήματα δικτύωσης και ζητήματα που αφορούν τους ηλεκτρονικούς υπολογιστές και τα πληροφοριακά συστήματα[14]. Και μάλιστα σε επάρκεια τέτοια που ο δικαστής να μην παρακολουθεί απλά την κατάθεση του μάρτυρα με ειδική γνώση ή του πραγματογνώμονα αλλά να μπορεί να αξιολογήσει σχετικά, να θέσει ερωτήματα, να διεισδύσει στην κατάθεση και να την αξιολογήσει στα πλαίσια της δικονομικής αρχής της ηθικής απόδειξης, που κρατεί στο ποινικό δικονομικό μας σύστημα αναφορικά με το κεφάλαιο της απόδειξης αλλά και την με αυτό συνεχόμενη και συσχετιζόμενη ειδική κι εμπεριστατωμένη αιτιολόγηση των δικαστικών αποφάσεων, όπως επιβάλλει το Σύνταγμα και ο νόμος[15]. Διαφορετικά την δικανική κρίση δεν την παρέχει ο δικαστής αλλά ο πραγματογνώμονας και κάτι τέτοιο φυσικά δεν είναι αποδεκτό, πρωτίστως δε δεν είναι νόμιμο και συνταγματικά ανεκτό.

iii. Μια ακόμη πτυχή του προβλήματος.

[13] Ενδεικτική αναφορά σε *Σ. Πετρίδου*, ΤΠΕ – το πρωτόκολλο του Παγκόσμιου ιστού HTTP, την οποία επ ευκαιρία ευχαριστώ, όπως και όλους τους καθηγητές μου στο ΔΠΜΣ «Δίκαιο & Πληροφορική», για την διδασκαλία τους αλλά και την άριστη και ανθρώπινη αντιμετώπισή τους προς ένα ακροατήριο που γνώριζε λίγα έως καθόλου σχετικά με την πληροφορική.

[14] Βλ. *Ι. Αγγελής*, Διαδίκτυο και ποινικό δίκαιο, ΠοινΧρον 2000, σελ. 675.

[15] Βλ. σχετικά τα άρθρα 93 παρ. 3 του Συντάγματος και 139 Κ.Π.Δ. αναφορικά με την ειδική και εμπεριστατωμένη αιτιολογία, η έλλειψη της οποίας ιδρύει τον, από το άρθρο 510 παρ. 1 στοιχ. Δ του Κ.Π.Δ., λόγο αναιρέσεως,

Σε όλους αυτούς τους προβληματισμούς πρέπει να προστεθεί και να αποτελέσει σημείο αναφοράς και στο δεδομένο των συγκρουσιακών σχέσεων, που δημιουργούνται μέσα από την χρησιμοποίηση του διαδικτύου για τέλεση αξιοποίνων πράξεων από την μια και την θεσμοθέτηση κανόνων για την ορθή λειτουργία των ηλεκτρονικών επικοινωνιών σε θεσμικό πλαίσιο και με προσανατολισμό τις δικλείδες ασφαλείας αναφορικά με την τήρηση του τηλεπικοινωνιακού απορρήτου ως θεμελιώδη ατομική ελευθερία[16]. Δυνάμεις εξ ίσου ισχυρές και με έντονη παρουσία στην καθημερινότητα, ως επαπειλούμενος κίνδυνος η πρώτη και ως κατεστημένη πρακτική η δεύτερη συνθήκη.

Το πρόβλημα από την συσχέτιση αυτήν αφορά στα προσκόμματα και τους νομικούς φραγμούς που συναντά ο ερευνητής στον άνισο αγώνα καταδίωξης του δράστη μιας εγκληματικής συμπεριφοράς, που διέρχεται από το περιβάλλον των τεχνολογιών πληροφορικής κι επικοινωνιών. Ενώ λοιπόν ο δράστης κινείται χωρίς κανέναν φραγμό πλην των τεχνολογικών, ο διώκτης του είναι υποχρεωμένος να σταματά και να ανακατευθύνει τις ενέργειές του, όπου συναντά φραγμό, συνήθως αναφορικά με το απόρρητο για τις επικοινωνίες και τα δεδομένα που τηρούνται σε δομημένο αρχείο. Ο αγώνας αυτός τελείται με άνισους όρους και με ιδιαίτερες απαιτήσεις από την κοινωνία που ζητά όλο και περισσότερο ασφάλεια[17], ιδίως τώρα που με τις διαρκείς αναρτήσεις των κοινωνών στα μέσα κοινωνικής δικτύωσης, τα προσωπικά τους δεδομένα εκτίθενται περισσότερο.

iv. Εισαγωγικές αναφορές στο ηλεκτρονικό έγκλημα.

Η εισβολή των τεχνολογιών πληροφορικής κι επικοινωνιών στην ατομική δραστηριότητα των μελών της κοινότητας, έχει προσλάβει τόσο σημαντική θέση στην καθημερινή πρακτική ώστε αποκτά μορφή συμπεριφοράς, που πλέον αντιμετωπίζεται ως προέκταση της καθημερινής κοινωνικής δράσης των μελών της κοινότητας. Η χρήση των εφαρμογών κοινωνικής δικτύωσης, του διαδικτυακού ηλεκτρονικού ταχυδρομείου, υπηρεσιών άμεσης ανταλλαγής μηνυμάτων και εφαρμογών με σκοπό την επικοινωνία, την οικονομική ζωή, την σύναψη συμβάσεων, την εκτέλεση τραπεζικών συναλλαγών (πολλές φορές με σημαντικής έκτασης υλικό αντικείμενο), την εργασία, την *ψηφιακή επαφή* με άλλους ανθρώπους και την απόκτηση πληροφοριών είναι κάποιες από τις συμπεριφορές

[16] Βλ. Ν 2225/1994, όπως ισχύει σήμερα αλλά και *Ι. Αγγελή*, Διαδίκτυο και ποινικό δίκαιο, ΠοινΧρον 2000, σελ. 676.

[17] Βλ. *Majid Yar, Kevin F. Steinmetz*, Cybercrime and Society, 2019, Sage, 23 επ., https://books.google.gr/books?hl=el&lr=&id=gpuHDwAAQBAJ&oi=fnd&pg=PP1&ots=flxXmdBzKT&sig=gMydzWI_DkWYDgVgZkS-huQSJOQ&redir_esc=y#v=onepage&q&f=true

αυτές, που τις εντοπίζουμε με ολοένα αυξανόμενο ρυθμό, τουλάχιστον στο σύνολο του αναπτυγμένου κόσμου.

Οι υπηρεσίες αυτές συνδέουν εκατοντάδες εκατομμύρια χρήστες μεταξύ τους, μέσω των ηλεκτρονικών συσκευών που διαθέτει ο καθένας. Επίσης, οι παροχές αυτές παράγουν σημαντικά οφέλη για την οικονομική και την κοινωνική ευημερία των χρηστών σε όλο τον κόσμο. Όπως όμως ορθά επεσήμανε η Ευρωπαϊκή Επιτροπή[18], είναι επίσης δυνατή η κατάχρηση των υπηρεσιών αυτών, καθώς μπορούν να αποτελέσουν εργαλεία για τη διάπραξη ή τη διευκόλυνση εγκλημάτων, μεταξύ των οποίων και σοβαρά εγκλήματα όπως τρομοκρατικές επιθέσεις, ή δράσεις με έντονο ηθικό αποτροπιασμό.

Και αν το τεχνολογικό επίτευγμα της ζεύξης στην επικοινωνία είναι η μια εξόχως εντυπωσιακή συνθήκη αυτού του πολυσύνθετου δεδομένου, η ηθική και κοινωνιολογική διαχείριση της ενσωμάτωσης των νέων δομών επικοινωνίας στην κοινωνική δράση, είναι μια εξίσου ενδιαφέρουσα και κρίσιμη στην διαχείρισή της παράμετρος, η οποία, εκτιμώ, δεν έχει τύχει της ανάλογης προσοχής.

Η αντίρροπη διαδρομή μεταξύ ταχύτητας στην διακίνηση και διαχείριση δεδομένων από την μια και της ασφάλειας και καθορισμού θεσμικών πλαισίων κατά την χρήση των σχετικών εφαρμογών και κατά την διαχείριση των δεδομένων, είναι η κερκόπορτα μέσα από την οποία η *ψηφιακή κακοβουλία* διαμορφώνει νέες εγκληματικές μορφές ή μεταλλάσσει παραδοσιακές μορφές εγκληματικής συμπεριφοράς.

Όταν συμβαίνει κάτι τέτοιο, οι ίδιες οι προαναφερόμενες υπηρεσίες και εφαρμογές είναι συχνά η μόνη βάση από την οποία οι ερευνητές μπορούν να βρουν ενδείξεις για να προσδιορίσουν ποιος διέπραξε ένα έγκλημα, να συλλέξουν αποδεικτικά στοιχεία τα οποία μπορούν να αξιολογηθούν από την αρχή που διεξάγει την έρευνα για την εξιχνίαση της πράξης και να αξιοποιηθούν εν τέλει στο δικαστήριο[19].

Η ερευνητική πρόκληση για την σύνταξη και υποβολή της παρούσας μελέτης, στην βάση των σχετικών κανόνων που αφορούν την δικονομική χρήση και αξιοποίηση των ψηφιακών πειστηρίων στην ποινική δίκη, αναγκαστικά διέρχεται από την καταγραφή της

[18] Βλ. Πρόταση της Ευρωπαϊκής Επιτροπής, «Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις, Στρασβούργο, 17.4.2018, COM(2018) 225 final σε https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0008.02/DOC_1&format=PDF

[19] Βλ. Πρόταση της Ευρωπαϊκής Επιτροπής, «Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις, ο.π.

εμφάνισης των θέσεων κατηγοριοποίησης της εγκληματικής δράσης μέσα στο περιβάλλον των νέων τεχνολογιών. Έννοιες και όροι όπως ηλεκτρονικό έγκλημα, δικτυακό έγκλημα, κυβερνοέγκλημα, αρχίζουν και καταλαμβάνουν ξεκάθαρο και ουσιαστικό χώρο στο πλαίσιο των σχετικών αναζητήσεων.

2. ΓΕΝΙΚΕΣ ΑΝΑΦΟΡΕΣ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

i. Εννοιολογικός προσδιορισμός του ηλεκτρονικού εγκλήματος

Η μορφή της εγκληματικής συμπεριφοράς, που απασχολεί στην μελέτη αυτήν και σχετίζεται με τα ψηφιακά πειστήρια και τα ψηφιακά δεδομένα, διαμορφώνει από μόνη της, ως οντότητα, μια εικόνα σχετικά με τις δυσχέρειες, τις οποίες αντιμετωπίζει και καλείται να επιλύσει ο μελετητής. Πρόκειται για μια μελέτη ενός ποινικού φαινομένου που διεκδικεί ιδιαίτερο χώρο στην επιστημονική έρευνα, τόσο λόγω των τεχνικών ιδιαιτεροτήτων που εγείρονται αλλά και λόγω του σημαντικού αντικτύπου[20] που φέρνει στην κοινότητα. Εγκλήματα όπως η κοινή απάτη, η απάτη με υπολογιστή, η παράνομη επέμβαση σε πληροφοριακά συστήματα, η προσβολή του απορρήτου των επικοινωνιών, η παιδική πορνογραφία, η προαγωγή ανηλίκων στην πορνεία, η παραχάραξη, παράνομη βία, απειλή, εκβιασμός, παρενόχληση, καταδίωξη, παράνομο στοίχημα, χειραγώγηση αθλητικών αγώνων, εγκλήματα κατά της περιουσίας είναι μια σειρά από αξιόποινες συμπεριφορές, οι οποίες απαντώνται, ολοένα και συχνότερα, να τελούνται στον ψηφιακό κόσμο[21].

Σημειολογικά αναφέρεται ότι η επιστημονική κοινότητα είχε ιδιαίτερες επιστημονικές τοποθετήσεις αναφορικά με τον καθορισμό της έννοιας του ηλεκτρονικού εγκλήματος, ώστε το Μάιο του 2007, η Ευρωπαϊκή Επιτροπή εξέδωσε ανακοίνωση σχετικά με μια «γενική πολιτική για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο»[22], επισημαίνοντας ότι δεν υπήρξε ούτε ένας συμφωνημένος ορισμός του εγκλήματος στον κυβερνοχώρο. Εκεί πρότεινε έναν τριπλό ορισμό για τον καθορισμό του ηλεκτρονικού εγκλήματος, όπου συμπεριέλαβε α) παραδοσιακές μορφές εγκληματικότητας όπως η απάτη ή η πλαστογραφία, έστω και αν διαπράττονται μέσω ηλεκτρονικών συστημάτων, δίκτυα επικοινωνιών και

[20] Βλ. *R. Anderson, Chr. Barton, R. Boehme, R. Clayton, M. J.G. van Eeten, M. Levi, T. Moore, St. Savage*, Measuring the Cost of Cybercrime, https://www.econinfosec.org/archive/weis2012 /papers/Anderson_WEIS2012.pdf, *R. Anderson, R. Boehme, R. Clayton, and T. Moore*. Security Economics and the Internal Market. January 2008, http://www.enisa.europa.eu/act/sr/reports/ econ-sec/economics-sec, *Er. Brynjolfsson and Ad. Saunders*. Wired For Innovation: How Information Technology Is Reshaping the Economy. The MIT Press, October 2009, *Canalys Inc.* Enterprise security market to exceed $22 billion in 2012, December 2011. http://www.canalys.com/static/press_release/2011/canalys-pressrelease-201211-enterprise-security-market-exceed-22-billion-2012.pdf, Communications Fraud Control Association. 2011 global fraud loss survey. http://www. cfca.org/fraudlosssurvey/, 2011.

[21] Βλ. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, «Electronic Crime Scene Investigation, A Guide for First Responders, Second Edition», https://www.econinfosec.org/ archive/weis2012/papers/Anderson_WEIS2012.pdf

[22] Βλ. European Commission. «Towards a general policy on the fight against cyber crime», May 2007. COM(2007) 267 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF.

συστήματα πληροφοριών, β) τη δημοσίευση παράνομου περιεχομένου σε ηλεκτρονικά μέσα (π.χ. υλικό σεξουαλικής κακοποίησης παιδιών ή υποκίνηση φυλετικού μίσους) και γ) εγκλήματα μοναδικά για τα ηλεκτρονικά δίκτυα, π.χ. επιθέσεις κατά συστημάτων πληροφοριών, άρνηση υπηρεσίας (denial of Service) και hacking[23].

Το πολύπλοκο και δυσθεώρητο μέγεθος του ηλεκτρονικού εγκλήματος αναφορικά με τις δομές και τις εξελικτικές μορφές με τις οποίες καταλαμβάνει το ποινικό ενδιαφέρον των συντεταγμένων χωρών, τονίζεται με έμφαση στα διάφορα fora όπου και ειδικότεροι εννοιολογικοί προσδιορισμοί καταλαμβάνουν χώρο. Οι όροι περιλαμβάνουν έγκλημα που σχετίζεται με υπολογιστές, έγκλημα ηλεκτρονικών υπολογιστών, έγκλημα στο διαδίκτυο, ηλεκτρονικό έγκλημα, ψηφιακό έγκλημα, τεχνολογικό έγκλημα, έγκλημα τεχνολογίας αιχμής, διαδικτυακό έγκλημα, ηλεκτρονικό έγκλημα, κατάχρηση υπολογιστών και έγκλημα στον κυβερνοχώρο, που είναι και το ευρέως διαδιδόμενο[24].

Αυτά λοιπόν τα εγκλήματα μπορούν κατά μια πρώτη διαφοροποίηση να διαχωριστούν αφ' ενός στα εγκλήματα που διαπράττονται με τη χρήση ηλεκτρονικού υπολογιστή και αφ' ετέρου στα εγκλήματα που διαπράττονται μέσω του διαδικτύου, αποτελώντας μια ειδικότερη μορφή του ηλεκτρονικού εγκλήματος[25].

Κατά μια άποψη[26] το ηλεκτρονικό έγκλημα παρουσιάζεται ως νέα μορφή εγκλήματος που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών, ως μια νέα εκδοχή των *παραδοσιακών* εγκληματικών συμπεριφορών που πλέον διαπράττονται με υπολογιστή, άλλως ως εγκληματική συμπεριφορά, που εκδηλώνεται με τη συμμετοχή με οποιονδήποτε τρόπο ενός ηλεκτρονικού υπολογιστή ή ενός πληροφοριακού συστήματος[27]. Αναφορικά τώρα με το περιβάλλον τέλεσής του, το ηλεκτρονικό έγκλημα διακρίνεται i) σε συμπεριφορές που «λειτουργούν» τόσο στο κοινό περιβάλλον όσο και στο διαδίκτυο, λ.χ. η κλοπή προϊόντος πνευματικής ιδιοκτησίας, μια δυσφημιστική διάδοση, ii) σε εγκλήματα που διαπράττονται αποκλειστικά σε περιβάλλον ηλεκτρονικού υπολογιστή χωρίς τη χρήση διαδικτύου, λ.χ. το

[23] Βλ. *R. Anderson, Chr. Barton, R. Boehme, R. Clayton, M. J.G. van Eeten, M. Levi, T. Moore, St. Savage*, Measuring the Cost of Cybercrime, 2012, http://www.med.a51.nl/sites/default/files/pdf/Anderson_ WEIS2012.pdf

[24] Βλ. *Ali Alkaabi, G. Mohay, Adr. McCullagh, and N. Chantler*, Dealing with the Problem of Cybercrime, σε Digital Forensics and Cyber Crime, Second International ICST Conference ICDF2C 2010 Abu Dhabi, UnitedArab Emirates, October 4-6, 2010, σελ. 12 επ.

[25] Βλ. *Θ. Δαλακούρας*, Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν 4411/2016), σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2018, 3 επ.,

[26] Βλ. *Θ. Δαλακούρας*, Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν 4411/2016), ο.π., σελ. 4.

[27] Βλ. *Δ. Κιούπης*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 41 επ.

έγκλημα του άρθρου 370Β ΠΚ (Παράνομη πρόσβαση σε σύστημα πληροφοριών ή σε δεδομένα), 370Δ § 1 ΠΚ (χωρίς δικαίωμα αντιγραφή ή χρησιμοποίηση προγραμμάτων υπολογιστών), iii) σε εγκληματικές δράσεις που διαπράττονται στο διαδίκτυο (κυβερνοχώρο) και χαρακτηρίζονται ως cyber crimes, λ.χ. η ψηφιακή διάδοση παιδικού πορνογραφικού υλικού στο internet (αρ. 348 Α ΠΚ).

Σε ειδικότερες αναφορές φέρονται ως οι κυριότεροι τύποι εγκλημάτων υπολογιστών, ταξινομημένοι ως[28]: εγκλήματα «λευκού κολάρου» (όπου οι υπολογιστές χρησιμοποιούνταν για αποθήκευση και χειρισμό στα πλαίσια χειραγώγησης δεδομένων, με απομακρυσμένη πρόσβαση), βίαια εγκλήματα (προμελετημένος σχεδιασμός με χρήση υπολογιστών), τρομοκρατία (σχεδιασμός, επικοινωνία και συλλογή πληροφοριών σχετικά με τον στόχο), κατασκοπεία (παρακολούθηση και επικοινωνία με χρήση υπολογιστών), παραποίηση (μεθόδευση και σχεδιασμός με χρήση υπολογιστών), διακίνηση ναρκωτικών (διαχείριση βάσης δεδομένων πελατών, προμηθευτών και οικονομικών) και πορνογραφία γενικότερα (αποθήκευση μεγάλου όγκου βίντεο και φωτογραφιών σε ψηφιακές συσκευές).

Παραπέρα τα *κυβερνοεγκλήματα* διακρίνονται από το κεντρικό σημείο αναφοράς τους, το οποίο είναι η διάπραξή τους σε περιβάλλον ηλεκτρονικού υπολογιστή και δη διασυνδεδεμένου σε σύστημα πληροφοριών[29]. Αυτός, σε μια βασική, και γενικού γνωστικού επιπέδου αναφορά, είναι μια μηχανή κατασκευασμένη κυρίως από ψηφιακά ηλεκτρονικά κυκλώματα και δευτερευόντως από ηλεκτρικά και μηχανικά συστήματα, και έχει ως σκοπό να επεξεργάζεται πληροφορίες[30], που είναι διαμορφωμένες σε ψηφιακή δομή. Είναι ένα αυτοματοποιημένο, ηλεκτρονικό, ψηφιακό επαναπρογραμματιζόμενο σύστημα γενικής χρήσης, το οποίο μπορεί να επεξεργάζεται δεδομένα βάσει ενός συνόλου προκαθορισμένων οδηγιών, των εντολών που συνολικά ονομάζονται *πρόγραμμα*, με άλλα λόγια προκαθορισμένα στάδια (βήματα) βασικής δράσης. Οι υπολογιστικές μηχανές, στις οποίες γίνονται οι ανωτέρω αναφορές, εμφανίζονται σε διαφόρους μορφότυπους, ήτοι ως προσωπικοί υπολογιστές, smartphones, φορητοί υπολογιστές, tablets κοκ.

---

[28] Βλ. S. Srinivasan, Digital Forensics Curriculum in Security Education, Journal of Information Technology Education: Volume 12, 2013 Innovations In Practice, http://www.jite.informingscience.org/documents/Vol12/JITEv 12IIPp147-157Srinivasan1232.pdf

[29] Βλ. *Γ. Μπουρμάς*, Η νομιμότητα των ερευνών σε ηλεκτρονικά δίκτυα και δεδομένα στις περιπτώσεις εγκλημάτων στον κυβερνοχώρο, ΠοινΔνη 2019, σελ. 557, *Ι. Αγγελής*, Διαδίκτυο και ποινικό δίκαιο, ΠοινΧρον 2000, σελ. 676.

[30] Βλ. *R.W Hockney, C.R Jesshope*, Parallel Computers 2: Architecture, Programming and Algorithms, https://books.google.gr/books?hl=el&lr=&id=7ZKpDwAAQBAJ&oi=fnd&pg=PP9&dq=computers&ots=D1JyJyHoLr&sig=viqiosf2r2tI6H7rdb4sNRCs4mU&redir_esc=y#v=onepage&q=computers&f=false, https://el.wikipedia.org/wiki/%CE%97%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C%CF%82_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE%CF%82

Στην βάση αυτή, τα εγκλήματα διακρίνονται σε *γνήσια πληροφοριακά*, που τελούνται μέσω ηλεκτρονικού υπολογιστή, σε εγκλήματα με *ψηφιακό περιεχόμενο*, που σχετίζονται με την διακίνηση αρχείων παρανόμου ψηφιακού περιεχομένου, μέσω πληροφοριακών συστημάτων και σε εγκλήματα *κατά των πληροφοριακών συστημάτων* καθεαυτών, οπότε η αναγωγή στην περίπτωση αυτήν γίνεται στην προσβολή της εμπιστευτικότητας[31], ακεραιότητας[32] και διαθεσιμότητας των πληροφοριακών πόρων, που τυγχάνουν διαχείρισης από τα προσβεβλημένα συστήματα πληροφοριών[33].

Μέσα στις προαναφερόμενες εννοιολογικές προσεγγίσεις και αποδόσεις του όρου *ηλεκτρονικό έγκλημα* θα μπορούσε να ενταχθεί γενικά κάθε παράνομη συμπεριφορά και εγκληματική δράση η οποία τελείται με την χρήση των τεχνολογιών αιχμής στο έδαφος της εφαρμογής τεχνολογιών πληροφορικής και ηλεκτρονικής επικοινωνίας. Εκ των θεμελιωδών στοιχείων για τον τελικό χαρακτηρισμό είναι η χρησιμοποίηση της ψηφιακής τεχνολογίας και των δομών της, ήτοι ηλεκτρονικοί υπολογιστές, πληροφοριακά συστήματα και διαδίκτυο είτε τοπικά δίκτυα στα οποία είναι διασυνδεδεμένοι ηλεκτρονικοί υπολογιστές και πληροφορικά συστήματα[34].

ii. Χαρακτηριστικά του ηλεκτρονικού εγκλήματος

Στα κύρια χαρακτηριστικά του ηλεκτρονικού εγκλήματος πρωτεύουσα θέση έχει ο χαρακτηρισμός του ως εγκλήματος *αποστάσεως*[35]. Μάλιστα η κατεξοχήν μορφή του ηλεκτρονικού εγκλήματος, αυτή της εγκληματικής δράσης στον κυβερνοχώρο, μπορεί να ενεργηθεί οπουδήποτε στον κόσμο υπάρχει σύνδεση σε δίκτυο ηλεκτρονικής επικοινωνίας, κείθεν δε στο διαδίκτυο. Αυτή η συνθήκη με την σειρά της δημιουργεί το πολυσύνθετο ζήτημα της τοπικής αρμοδιότητας των αρχών που καλούνται να επιληφθούν για την

[31] Προσβασιμότητα μόνο με δικαίωμα και βάσει των θεμελιωδών αρχών για την προστασία των δεδομένων, μόνο στο μέτρο του αναγκαίου και από περιορισμένο αριθμό προστηθέντων εκείνου που φέρει την ευθύνη τήρησης του σχετικού αρχείου.

[32] Τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που να εγγυάται την ενδεδειγμένη ασφάλειά τους, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα») σε Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, εκδ. 2018, https://www.coe.int/dataprotection, *Β. Κάτος*, Ψηφιακά Πειστήρια, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 65 επ.

[33] Βλ. *Θ. Δαλακούρας*, Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν 4411/2016), ο.π., σελ. 5.

[34] Βλ. *An. Papathanasiou, Al. Papanikolaou, V. Vlachos, K. Chaikalis, M. Dimou, M. Karadimou and V. Katsoula,* Legal and Social Aspects of Cyber Crime in Greece, ResearchGate 2015, https://www.researchgate.net/publication/260390705

[35] Βλ. *Δ. Κιούπης*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, σελ. 41 επ.

εξιχνίασή του και την αναζήτηση των δραστών. Το ζήτημα οξύνεται από την ίδια την πραγματικότητα που θέλει την *τηλεπικοινωνιακή ψηφιακή ζεύξη* να τελείται με όρους και συνθήκες ξένες προς τον δράστη – χρήστη, με αποτέλεσμα η *ψηφιακή τοποθεσία* που φιλοξενεί την παράνομη συμπεριφορά να είναι άγνωστη ακόμη και στον ίδιο κατά τον χρόνο δράσης, ή να αφορά τοποθέτηση σε δικαιϊκό χώρο όπου η *εγκληματική απόχρωση* της συμπεριφοράς να μεταλλάσσεται.

Από τα παραδείγματα της θεωρίας ενδεικτικά αναφέρεται η περίπτωση αποστολής μέσω εφαρμογής κοινωνικής δικτύωσης από την Ελλάδα ψηφιακού υλικού, που κυκλοφορεί καθόλα νόμιμα στην χώρα μας, στο smartphone αποδέκτη, που έχει την κατοικία του στην Ελλάδα, ο οποίος όμως κατά τον χρόνο λήψης του ψηφιακού υλικού βρίσκεται σε χώρα στην οποία το ίδιο υλικό είναι παράνομο[36] (λ.χ. ιδιαίτερες απαγορεύσεις σε αναφορές και διακίνηση σε μια μουσουλμανική χώρα υλικού που κρίνεται ανήθικο).

Χαρακτηριστικό επίσης των εγκλημάτων αυτών είναι η *ταχύτητα*[37] και η *ευκολία*[38] στην διάπραξή τους. Ευκολία καθόσον η επιχείρησή τους μπορεί να γίνει από *ασφαλές* για τον δράστη περιβάλλον της δικής του επιλογής και σαφώς με την πολυτέλεια της επιλογής του χώρου από όπου θα επιχειρηθεί η *ψηφιακή έφοδος*. Στις περιπτώσεις των εγκλημάτων αυτών περισσότερη σημασία έχει η καλή δικτύωση (ταχύτητα διάδοσης) και λιγότερη σημασία έχει η γεωγραφική θέση. Ο δράστης «βλέπει» το θύμα από παντού. Οι δυνατότητες των λειτουργικών των ηλεκτρονικών υπολογιστών σήμερα, εξασφαλίζουν την ολοκλήρωση της δράσης στον ελάχιστο απαιτούμενο χρόνο, ο οποίος σύμφωνα με τις παραδοσιακές έννοιες και αντιλήψεις για την πράξη στο ποινικό δίκαιο, είναι και σε απόλυτη μέτρηση, ελάχιστος,

Το στοιχείο της ανωνυμίας στις εγκληματικές δράσεις είναι συνυφασμένο με την τακτική διαφυγής του δράστη. Τον σχεδιασμό, που ακολουθεί την ολοκλήρωση της εγκληματικής ενέργειας και εντάσσεται στην σχετική στρατηγική, την οποία κατέστρωσε ο δράστης είτε ενεργεί μόνος είτε επιχειρεί ως μέλος ομάδας, προκειμένου να αποφύγει την αποκάλυψη και την ταυτοποίηση με την πράξη του που σαφώς δεν αναμένει να μείνει κρυφή. Η κάλυψη των στοιχείων του προσώπου ενός δράστη ληστείας σε τράπεζα σαφώς και δεν στοχεύει στην μη αποκάλυψη της πράξης του (αυτό ίσως να είναι και αντίθετο με τον όλο

[36] Βλ. *Δ. Κιούπης*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, ο.π. σελ. 47 επ., *Δ. Κιούπη*, Δημοσίευση ιστοσελίδων με αξιόποινο περιεχόμενο, ΠοινΛογ 2001, 398.
[37] Βλ. *Γ. Μπουρμάς*, Η νομιμότητα των ερευνών σε ηλεκτρονικά δίκτυα και δεδομένα στις περιπτώσεις εγκλημάτων στον κυβερνοχώρο, ΠοινΔνη 2019, σελ. 557.
[38] Βλ. *Ι. Αγγελής*, Διαδίκτυο και ποινικό δίκαιο, ΠοινΧρον 2000, σελ. 677.

σχεδιασμό του πολλές φορές) αλλά στην απόκρυψη των προσωπικών στοιχείων που θα οδηγήσουν στην ταυτοποίηση και σύνδεσή του με την πράξη.

Στην περίπτωση του ηλεκτρονικού εγκλήματος η *ανωνυμία*[39] παρέχεται by default μέσα από τις δυνατότητες που παρέχουν οι εφαρμογές λ.χ. κοινωνικής δικτύωσης (προφανώς για την προσέλκυση ενδιαφέροντος χρηστών)[40]. «*Η ανωνυμία είναι η ασπίδα από την τυραννία της πλειοψηφίας*». Με αυτήν την φράση, το Ανώτατο Δικαστήριο των ΗΠΑ θέλησε το 1995 (υπόθεση McIntyre v. Ohio Elections Commission) [41] να τονίσει την συμβολή του ανώνυμου λόγου στην εύρυθμη λειτουργία της δημοκρατίας, για να συμπληρώσει, μόλις δύο χρόνια μετά (υπόθεση Reno v. ACLU)[42], ότι η συνταγματική προστασία της ανωνυμίας (Πρώτη Τροποποίηση στο Σύνταγμα των ΗΠΑ)[43] περιλαμβάνει και το Διαδίκτυο (internet). Περαιτέρω κατά το Δικαστήριο του Στρασβούργου (υπόθεση Editorial Board of Pravoye Delo and Shtekel v. Ουκρανίας, 5.5.2011)[44], το διαδίκτυο είναι ένα *νόμιμο forum άσκησης της ελευθερίας του ανώνυμου λόγου*. Αναμφισβήτητα, προς την παραπάνω κατεύθυνση οδήγησε και το ίδιο το διαδίκτυο, προσφέροντας – περισσότερο από κάθε άλλο forum – ποικίλα μέσα ανωνυμίας, ιδίως δε τα blogs, τα chart rooms και τα e-mails[45].

Η ανωνυμία που παρέχεται εξ ορισμού στην διαδικτυακή χρήση, σε συνδυασμό με το πολυσχιδές σύστημα που αφορά στην διαχείριση των ηλεκτρονικών επικοινωνιών σε τεχνικό

---

[39] Βλ. *Β. Κάτος*, Ψηφιακά Πειστήρια, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2018, 65 επ.

[40] Βλ. *Γ. Κακαβούλης*, Η ανωνυμία στο Διαδίκτυο, https://www.homodigitalis.gr/posts/1908. Η ανωνυμία σαφώς και δεν είναι σε κάθε περίπτωση κάτι αρνητικό. Αποτελεί θεμελιώδες στοιχείο των δημοκρατιών, που σέβονται και προωθούν την ελευθερία της έκφρασης και το διάλογο. Το δικαίωμα στον ανώνυμο λόγο ενισχύει την επιθυμία των πολιτών να εκφράσουν τις απόψεις τους δημόσια, ανεξάρτητα από το θάρρος τους ή το πόσο δημοφιλείς είναι οι απόψεις τους. Ο ανώνυμος λόγος ενισχύει τη συμμετοχή στα κοινά. Έτσι, είναι δυνατό να εκφραστούν απόψεις της μειονότητας και απόψεις που έρχονται σε αντίθεση με την εξουσία ή ασκούν κριτική σε αυτή. Η έκφραση στο Διαδίκτυο είναι επίσης ανώνυμη. Όμως, η ανωνυμία δεν προφυλάσσει μόνο τον καλό λόγο, δηλαδή το λόγο που προάγει τη δημοκρατία και το διάλογο. Προστατεύει και τον ψευδή, παράνομο, ανήθικο και προσβλητικό λόγο. Είτε αφορά σε πολιτικές, οικονομικές, κοινωνικές, ακόμη και καλλιτεχνικές συζητήσεις, τέτοια παραδείγματα κακού λόγου, υπάρχουν παντού στο διαδίκτυο. Η ασφάλεια που προσφέρει η ανωνυμία ωθεί πολλούς χρήστες του Διαδικτύου σε χρήση χυδαίου, προσβλητικού ή ψευδούς λόγου. Το φαινόμενο του εκφοβισμού (bulling) μέσω του διαδικτύου έχει ως αιτία –μεταξύ άλλων- και τη δυνατότητα των χρηστών του Διαδικτύου να αποκρύψουν την πραγματική τους ταυτότητα.

[41] Βλ. The SUPREME COURT of the UNITED STATES No. 93-986, Joseph McIntyre, executor of estate of Margaret McIntyre, deceased, petitioner v. OHIO ELECTIONS COMMISSION on writ of certiorari to the supreme court of ohio [April 19, 1995], https://www.law.cornell.edu/supct/html/93-986.ZO.html

[42] Βλ. The SUPREME COURT of the UNITED STATES No. 96-511, Reno, Attorney General Of The United States, et al. v. AMERICAN CIVIL LIBERTIES UNION et al, appeal from the united states district court for the eastern district of Pennsylvania, Argued March 19, 1997-Decided June 26, 1997, https://www.aclu.org/legal-document/supreme-court-decision-reno-v-aclu-et-al.

[43] Βλ. FIRST AMENDMENT - Freedom of Religion, Speech, Press, Assembly, and Petition, Passed by Congress September 25, 1789. Ratified December 15, 1791. The first 10 amendments form the Bill of Rights, https://constitutioncenter.org/interactive-constitution/amendment/amendment-i

[44] Βλ. Case of editorial board of Pravoye Delo and Shtekel v. Ukraine, (application no. 33014/05) – judgment – strasbourg - 5 may 2011 – final, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-104685%22]}.

[45] Βλ. *Γ. Κιστάκις*, Η ανωνυμία στο Διαδίκτυο, https://www.kathimerini.gr/726387/opinion/epikairothta/arxeio-monimes-sthles/h-anwnymia-sto-diadiktyo

αλλά και νομικό επίπεδο, δημιουργούν μια πολλαπλή συνθήκη, που πολλές φορές οδηγεί σε αδιέξοδα, όχι τόσο λόγω τεχνικών όσο κυρίως νομικών φραγμών[46].

Άλλο χαρακτηριστικό του ηλεκτρονικού εγκλήματος είναι ο *διασυνοριακός*[47] του χαρακτήρας και η σχετική δυσχέρεια στην εξιχνίασή του, εκ του λόγου αυτού, πέρα από τους λόγους που εκτέθηκαν προηγουμένως και τοποθετούνται σε άλλη βάση. Είναι κατά μια εκπεφρασμένη άποψη «έγκλημα χωρίς πατρίδα»[48]. Δεν υιοθετώ, αλλά απλά παραθέτω, ως οφείλω, την θέση αυτή, καθόσον οι βασικές αρχές του καθορισμού του τόπου τέλεσης της πράξης υφίστανται κατά βάση και δίνουν ένα σημείο αναφοράς, με εξαίρεση τις περιπτώσεις μερικής ή πλήρους τεχνικής συμμετοχής στην τέλεση της πράξης απομακρυσμένου εξυπηρετητή, όπου και πάλι ερμηνευτικά δίδονται τεχνικά συνεπείς και νομικά προσεγμένες λύσεις[49].

Η προπαρασκευή αλλά και η τεχνολογική δυνατότητα διαφορετικής διασύνδεσης του δράστη δημιουργούν ένα πολύμορφο πεδίο στο οποίο διεκδικούν εφαρμογή διαφορετικές νομοθεσίες[50], κρίσεις διαφορετικών δικαιοδοτικών οργάνων, με ενδεχόμενη διακοπή στην συνέχεια της διατήρησης του αξιοποίνου χαρακτήρα της ελεγχόμενης συμπεριφοράς κατά την παρακολούθηση των *εδαφικών* διαδρομών της πορείας, που ακολούθησε η ελεγχόμενη ως αξιόποινη ηλεκτρονική δράση. Όταν γίνεται λόγος για διακοπή, ουσιαστικά, του αξιοποίνου του χαρακτήρα της πράξης, η αναφορά έγκειται στην διαφορετικότητα των δικαιϊκών τάξεων, με αποτέλεσμα στην μια περίπτωση η πράξη να αξιολογείται ως αξιόποινη ενώ σε μια από τις λοιπές εμπλεκόμενες και διεκδικούσες εδαφική αρμοδιότητα, η πράξη να μην αξιολογείται ποινικά.

iii. Ο τρόπος συμπεριφοράς του εγκληματία στο ηλεκτρονικό έγκλημα.

Σημαντικά στοιχεία για την επιστημονική αναζήτηση που θα ακολουθήσει, αντλούμε από τα δεδομένα, που θα μας δώσουν κάποιες πρόχειρες αναφορές σχετικά με το μοτίβο

[46] Βλ, σχετικά αρ. 4 Ν 2225/1994, όπως αυτή ισχύει μετά από τις επάλληλες τροποποιήσεις της με τους Ν 3606/2007, Ν 3666/2008, Ν 3658/2009, Ν 4012/2012, Ν 4198/2013, Ν4254/2014, Ν 4267/2014, 4411/2016 και Ν 4416/2016, αλλά και το ΠΔ 47/2005, βλ. σχετικά και την ΓνωμΕισΑΠ 2/2017, ΒΔ Νόμος.

[47] Βλ. *Γ. Μπουρμά*, Η νομιμότητα των ερευνών σε ηλεκτρονικά δίκτυα και δεδομένα στις περιπτώσεις εγκλημάτων στον κυβερνοχώρο, ΠοινΔνη 2019, σελ. 557, *Δ. Κιούπης*, Ποινικό Δίκαιο και internet, σειρά ΠΟΙΝΙΚΑ, Νο 57, σελ 27.

[48] Βλ. *Ι. Αγγελή*, Διαδίκτυο και ποινικό δίκαιο, ΠοινΧρον 2000, σελ. 677.

[49] Βλ. . *Δ. Κιούπης*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 61 επ., *Δ. Κιούπης*, Ποινικό Δίκαιο και internet, σειρά ΠΟΙΝΙΚΑ, Νο 57, σελ 27.

[50] Βλ. *An. Papathanasiou, Al. Papanikolaou, V. Vlachos, K. Chaikalis, M. Dimou, M. Karadimou and V. Katsoula*, Legal and Social Aspects of Cyber Crime in Greece, ResearchGate 2015, https://www.researchgate.net/publication/260390705

συμπεριφοράς του δράστη των εγκληματικών μορφών, που μας απασχολούν εδώ. Γνωρίζοντας ή προσεγγίζοντας το εγκληματικό προφίλ[51] του προσώπου, που βρίσκεται πίσω από την ανωνυμία και κάπου στον κόσμο μέσα, ο ερευνητής μπορεί να έχει στην φαρέτρα του *κάτι* αντί για το *τίποτα*. Όλες οι τεχνολογικές μέθοδοι, που κρατούν στον χώρο της πληροφορικής, επιτρέπουν σε έναν καλό γνώστη της πληροφορικής και της ασφάλειας δικτύων, το μεν να δρα ανενόχλητος, το δε να κρύβεται, εξαφανίζοντας τα ψηφιακά του ίχνη. Συνηγορούν στην ενίσχυση της ανωνυμίας όλα σχεδόν τα χαρακτηριστικά του ηλεκτρονικού εγκλήματος, που αναφέρθηκαν προηγουμένως, ήτοι, ευκολία στην τέλεση, δράση υπό καθεστώς ανωνυμίας, ταχύτητα κλπ.

Ο τρόπος δράσης λοιπόν στα εγκλήματα αυτά αναδεικνύει άτομο με επάρκεια γνώσεων στην τεχνολογία των ηλεκτρονικών υπολογιστών και των πληροφοριακών συστημάτων καθώς και των ζητημάτων που αφορούν ασφάλεια δικτύων, αλλά και των τεχνικών δομών της ηλεκτρονικής επικοινωνίας. Ένας ταχύς και ρωμαλέος δράστης δεν είναι αρκετός από μόνος του, ή καλύτερα ίσως είναι και ακατάλληλος αν στερείται των ειδικών γνώσεων που απαιτούνται. Αναφέρθηκα σε μια τέτοια μορφή δράστη καθόσον αυτή ικανοποιεί τα πρότυπα εγκληματικής μορφής σε πολλά από τα παραδοσιακά εγκλήματα, για να αναδειχθεί και στο στοιχείο αυτό η απόσταση και η διάκριση του ηλεκτρονικού εγκλήματος.

Ανάλογα τώρα με τα παραγωγικά αίτια της βούλησής τους, οι δράστες αυτοί κατηγοριοποιούνται καταρχήν στα άτομα που έχουν ως αυτοσκοπό την αναζήτηση κι εκμετάλλευση αδυναμιών στα μέτρα ασφαλείας των πληροφορικών συστημάτων, με σκοπό την υπέρβαση όλων των φραγμών ώστε να φτάσουν στα δεδομένα του συστήματος, ήτοι στόχος και αυτοσκοπός είναι η εισβολή στο σύστημα χωρίς κανένα περαιτέρω σχεδιασμό. Πρόκειται για το προφίλ του hacker[52]. Και αν σήμερα ο όρος χρησιμοποιείται με αρνητικό πρόσημο, αυτό δεν ήταν έτσι πάντοτε, καθόσον στην αρχική του χρήση, περί το 1960 !, ο χαρακτηρισμός, γνωστός τότε ασφαλώς σε μια περιορισμένη στον αριθμό των μελών της φουτουριστική επιστημονική ελίτ, αναφερόταν σε άτομο με τεχνολογικές ικανότητες, δημιουργικότητα, διεισδυτικότητα, καινοτόμες σκέψεις και αξιόπιστο[53]. Εξ άλλου ο όρος

[51] Βλ. *Ι. Αγγελής*, Διαδίκτυο και ποινικό δίκαιο, ΠοινΧρον 2000, σελ. 677.

[52] Βλ. *Θ. Δαλακούρας*, Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν 4411/2016), ο.π., σελ. 8 με τις εκεί παραπομπές. *Ι. Αγγελή*, Διαδίκτυο και ποινικό δίκαιο, ΠοινΧρον 2000, σελ. 677, *Majid Yar, Kevin F. Steinmetz*, Cybercrime and Society, 2019, Sage, 23 επ., https://books.google.gr/books?hl=el&lr=&id=gpuHDwAAQBAJ&oi=fnd&pg=PP1&ots=flxXmdBzKT&sig=gMydzWI_DkWYDgVgZkS-huQSJOQ&redir_esc=y#v=onepage&q&f=true.

[53] Βλ. *Majid Yar, Kevin F. Steinmetz*, Cybercrime and Society, 2019, Sage, 53 επ., https://books.google.gr/books?hl=el&lr=&id=gpuHDwAAQBAJ&oi=fnd&pg=PP1&ots=flxXmdBzKT

«Hack» αναφέρεται στην αγγλική γλωσσολογία, στην αρχική του ερμηνεία, ως *ικανότητα επίλυσης προβλημάτων*[54]. Η δράση τους δεν είναι πάντα ανήθικη και αξιόποινη καθόσον υπάρχουν περιπτώσεις, που άτομα με τις δεξιότητες ενός hacker προσλαμβάνεται από τον ίδιο τον εκπρόσωπο της οντότητας, προκειμένου να αναδείξει προβλήματα στα συστήματα ασφαλείας των ηλεκτρονικών αρχείων με αποτέλεσμα τελικά να εντοπιστούν τα προβλήματα ασφαλείας και εν τέλει να προταθούν λύσεις.

Σε άλλη μορφή δράσης η *εισβολή*, με την έννοια της παράκαμψης των συστημάτων ασφαλείας και απορρήτου, είναι η προπαρασκευαστική συμπεριφορά για την επίτευξη του στόχου που είναι η πρόκληση βλάβης στο σύστημα ή η πρόκληση βλάβης, συνήθως οικονομικής, με έναν από τους πολλούς τρόπους που έχει αναδείξει η ανακριτική και δικαστηριακή πρακτική. Η οικονομική αυτή βλάβη εκλαμβάνεται ως μια πολυεπίπεδη δομή, που ξεπερνά την έννοια μια λογιστικής προσέγγισης. Εδώ η αναφορά γίνεται στον τύπο του cracker[55].

Η δράση των εγκληματιών του κυβερνοχώρου αποδίδεται με τα επτά σημεία στην Cyber-Kill-Chain, που φέρεται να αποδίδει την σπονδυλωτή δράση μέσα από την αναγνώριση και στόχευση μέσα από επιλογή από λίστα με διευθύνσεις ηλεκτρονικού ταχυδρομείου ή μέσων κοινωνικής δικτύωσης (reconnaissance), εξοπλισμό με τη σύνδεση ενός μεταφορτούμενου κακόβουλου λογισμικού (weponization), παράδοση (delivery) συνήθως με την μορφή e-mail, μετά την μεταφόρτωση του κακόβουλου λογισμικού ακολουθεί η εκμετάλλευση (exploitation) ενός ευπαθούς συστήματος ή και του ίδιου του χρήστη με παραπλάνηση, προκειμένου να ενεργοποιηθεί το κακόβουλο λογισμικό ώστε να ακολουθήσει η εγκατάστασή (instalation) του στο ψηφιακό περιβάλλον του χρήστη. Η εντολή και ο έλεγχος (command and control) είναι το βήμα, κατά το οποίο αφού συνδεθεί ο υπολογιστής στο διαδίκτυο, είναι δυνατή η απομακρυσμένη ενεργοποίηση της εντολής για την προσβολή. Από εδώ και πέρα, αφού προηγηθούν τα έξι στάδια, ο δράστης μπορεί να

&sig=gMydzWI_DkWYDgVgZkS-huQSJOQ&redir_esc=y#v=onepage&q&f=true, *St Levy*, Hackers: Heroes of the Computer Revolution, 1984

[54] To "Hack" [verb] = to manage to deal successfully with something, στο Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/hack.

[55] Βλ. *I. Αγγελής*, Διαδίκτυο και ποινικό δίκαιο, ΠοινΧρον 2000, σελ. 678, επίσης αναφορικά με τις διαφορές cracker – hacker σε https://coolweb.gr/diafora-hacker-cracker/, *Ar. Karataş, S. Şahin,* A Review on Social Bot Detection Techniques and Research Directions, 2016, https://www.researchgate.net/profile/Serap_Sahin2/publication/322853694_A_Review_on_Social_Bot_Detection_Techniques_and_Research_Directions/links/5a72d272a6fdcc53fe131e99/A-Review-on-Social-Bot-Detection-Techniques-and-Research-Directions.pdf, J. *Ratkiewicz, M. Conover, M. Meiss, B. Gonçalves, A. Flammini, and F. Menczer,* «Detecting and Tracking Political Abuse in Social Media," ICWSM, vol. 11, pp. 297-304, 2011.

ενεργήσει και να πραγματώσει (actions and objectives) τον σκοπό του αντλώντας στοιχεία και δεδομένα από το περιβάλλον του χρήση – θύματος[56].

Να σημειωθεί ότι ο εντοπισμός ενός θύματος από τον δράστη μπορεί να διέρχεται από ενεργή συμμετοχή του θύματος (active reconnaissance), λ.χ. μέσα από την δράση του και την ψηφιακή του κίνηση και αναζητήσεις ή και χωρίς αυτήν (passive reconnaissance), με την ανάκτηση στοιχείων μέσα από δομές συγκέντρωσης ηλεκτρονικών δεδομένων[57].

Όπως προκύπτει από την εξελικτική πορεία των πραγμάτων, οι ικανότητες των εγκληματιών πολύ δύσκολα βρίσκουν εμπόδιο και φράγμα από τις επιλογές στην ασφάλεια των δικτύων και των δεδομένων κι έτσι οι σχετικές προβλέψεις του Ι. Αγγελή για το πορφίλ των δραστών του ηλεκτρονικού εγκλήματος το 2020[58], μάλλον ξεπεράστηκαν πολύ νωρίτερα. Θα διατηρήσω αποστάσεις από την θέση ότι ο εγκληματίας του ηλεκτρονικού εγκλήματος πρέπει να έχει κοινωνική θέση και οικονομική επιφάνεια[59], όπως αυτές εκφράστηκαν στην σχετική, σημαντική για την εποχή της, ανάλυση του προαναφερομένου μελετητή. Οι θέσεις αυτές ίσως να είχαν κάποια άλλη αντιληπτική δυνατότητα των πραγμάτων την εποχή εκείνη, σήμερα όμως δεν μπορούν να υποστηριχθούν πειστικά, από την στιγμή που ανήλικοι μεν δράστες, ικανότατοι όμως περί την χρήση των ηλεκτρονικών υπολογιστών και την χρήση του διαδικτύου, αντιλαμβάνονται άριστα τον κυβερνοχώρο σε όλες του τις διαστάσεις και δυνατότητες[60] και ελίσσονται με ευχέρεια, ακρίβεια και ανωνυμία, αλλά και με στρατηγική καταστροφής των ψηφιακών ιχνών τους.

Όπως γίνεται αντιληπτό οι ανωτέρω καταγραφές στόχο έχουν αποκλειστικά και μόνο μια εισαγωγή στην προβληματική του χώρου με αναφορά στο συνολικό υπόστρωμα όπου αναφύεται. Το ηλεκτρονικό έγκλημα αναγκαστικά παρακολουθεί και κινείται στα πλαίσια των καινοτόμων και σχεδόν καθημερινών εξελίξεων αλλά κι επεκτάσεων του διαδικτύου και του παγκόσμιου ιστού. Η καθημερινή δε αναφορά γίνεται τουλάχιστον στον υπερβάλλοντα

---

[56] Βλ. *Αν. Γκιουζέπας*, ΓΕΕΘΑ/Διεύθυνση Κυβερνοάμυνας στο 2ο Ετήσιο Συνέδριο Ασφάλειας Ψηφιακών Συστημάτων, 2016, https://www.youtube.com/watch?v=48gLcE_-dQY&t=410s

[57] Όπως Electronic Data Gathering, Analysis and Retrieval (EDGAR), Google Hacking, Internet Corporation for Assigned Names and Numbers (ICANN) και Internet Assigned Numbers Authority (IANA).

[58] Βλ. *Ι. Αγγελής*, Διαδίκτυο και ποινικό δίκαιο, ΠοινΧρον 2000, σελ. 678, υπό αρ. 5.

[59] Βλ. *E. Casey*, Digital Evidence and Computer Crime, https://www.semanticscholar.org/paper/Digital-Evidence-and-Computer-Crime-Casey/8c28fbef0af2d0b0dfb772c82a8059e9094eb4c3, *D B Parker*, Fighting Computer Crime, 1983, NY., *I. Αγγελή*, Διαδίκτυο και ποινικό δίκαιο, ΠοινΧρον 2000, σελ. 678, υπό αρ. 7.

[60] Βλ. *J. R. Norgaard, H.J. Walbert, R. A. Hardy*, Shadow Markets and Hierarchies: Comparing and Modeling Networks in the Dark Net, https://s3.amazonaws.com/academia.edu.documents/51205101/Shadow_Markets_and_Hierarchies_-_Comparing_and_Modeling_Networks_in_the_Dark_Net_Norgaard.pdf?response-content-disposition=inline%3B%20filename%3DShadow_Markets_and_Hierarchies_Comparing.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=ASIATUSBJ6BAFRPY66IU%2F20200404%2Fus-east-1%... -Amz-Signature=e0c846e73557dbca224d0b2f7329500a1922654e686745abc90046b3436c8c2a.

τις αντοχές του μέσου ανθρωπίνου μυαλού, ρυθμό αύξηση των πληροφοριακών πόρων και των δεδομένων που παράγονται παγκοσμίως και είναι προσβάσιμες, τουλάχιστον τεχνικά σε πληθώρα ανθρώπων.

Εξ άλλου όπως σε όλο τον χώρο του δικαίου και ειδικά του ποινικού η ανθρώπινη, κυρίως όμως η εγκληματική, συμπεριφορά είναι εκείνη που δείχνει το νέο δρόμο στον οποίον για να καταλήξει η δίωξη πρέπει να προβεί στην αναγκαία ιχνηλάτηση, που εδώ πλέον αφορά ένα ψηφιακό περιβάλλον και τα δεδομένα του.

iv. Η κοινωνιολογική βάση της ηλεκτρονικής εγκληματικότητας.

Θα ήταν αντικείμενο μιας χωριστής μελέτης από μόνη της η αναφορά στην *κοινωνιολογική* βάση των προβληματισμών αναφορικά με την ηλεκτρονική εγκληματικότητα. Φυσικά η μελέτη αυτή δεν διεκδικεί έδαφος από τον τομέα αυτόν. Είναι όμως μια σημαντική παράμετρος για την κατανόηση του αντικειμένου αυτής της μελέτης το πώς εμφυτεύεται η ψηφιακή δράση μέσα στην εγκληματικότητα στην γενική της διάσταση.

Μια παράμετρος που συμπληρώνει το προφίλ του ηλεκτρονικού εγκλήματος είναι και αυτή των επιπτώσεων που έχει επιφέρει και σαφώς θα επιφέρει στο μέλλον μέσα στην κοινότητα. Είναι τέτοια η έκταση του κινδύνου στην έκθεση από την προβολή ατομικών εννόμων αγαθών από την δραστηριότητα που σχετίζεται με το ηλεκτρονικό έγκλημα, η οποία επιβάλλει την ιδιαίτερη προσοχή της επιστημονικής κοινότητας που σχετίζεται με το έγκλημα και την πάταξή του, αλλά και όλων των δομών εκείνων, από παρόχους ηλεκτρονικών υπηρεσιών και των ανεξαρτήτων αρχών, που τους ελέγχουν και τους αξιολογούν, μέχρι τις αρχές πρόληψης και καταστολής του εγκλήματος.

Η, πολλάκις αναφερθείσα, αλματώδης τεχνολογική ανάπτυξη σε συνδυασμό με την ολοένα αυξανόμενη προσφορά προϊόντων τεχνολογιών πληροφορικής και επικοινωνιών [Information and Communication Technologies (ICT)], η οποία προσφορά βρίσκει ιδιαίτερα μεγάλη ανταπόκριση στο αγοραστικό κοινό της κοινότητας, είναι ο ένας παράγοντας, που σε συνδυασμό με τον ψηφιακό αναλφαβητισμό (digital illiteracy), δημιουργεί συνθήκες ευχερούς ανάπτυξης της εγκληματικής δράσης και μάλιστα σε όλα τα επίπεδα.

Δεν είναι λίγες οι περιπτώσεις κατά τις οποίες άτομα με οικονομική δυνατότητα να αποκτούν πανάκριβες υπολογιστικές μηχανές και ιδιαίτερα smartphones, την στιγμή που οι λειτουργίες κι υπηρεσίες που αυτά παρέχουν στον κάτοχο είναι γνωστικά απλησίαστες από τον χειριστή της συσκευής. Η καταναλωτική μανία όμως, ως κοινωνικό μόρφωμα και

κοινωνιολογική παθολογία, αποτρέπει από τον αγοραστή από την σκέψη του κατά πόσο έχει ανάγκη την αναβαθμισμένη συσκευή αφήνοντάς τον στον αγώνα κοινωνικού ανταγωνισμού μέσα από την κατοχή υλικών αγαθών, δημιουργώντας μια επίπλαστη συνθήκη ευημερίας και κοινωνικής καταξίωσης. Ένα απλό κινητό (όχι smartphone) στα χέρια ενός καταξιωμένου δικηγόρου, μάλλον δεν είναι «εικόνα» συμβατή. Αντίθετα το smartphone τελευταίας τεχνολογίας και μεγάλης οικονομικής αξίας είναι ενδεδειγμένη πρακτική. Τώρα το κατά πόσο μπορεί να χειριστεί το smartphone πέρα από τις συνήθεις δραστηριότητες τηλεφωνικής επικοινωνίας, αποστολής SMS, φωτογράφισης και αποστολής μέσω εφαρμογής ηλεκτρονικής επικοινωνίας είναι κάτι άλλο (κάτι φυσικά που θα μπορούσε να κάνει και με ένα πολύ «συμβατικότερο» smartphone).

Αλλά και πρακτική γνώση των λειτουργιών του να έχει και πάλι ο *ψηφιακός αναλφαβητισμός* δεν του επιτρέπει ορθολογική χρήση. Συνήθη είναι τα μηνύματα, με τη μορφή κοινωνικής ενημέρωσης από την αρμόδια αστυνομική δομή για την μη διαχείριση πληροφοριών που εκθέτουν την ιδιωτικότητα των χρηστών. Το πάθος του χρήστη να αναδείξει ανά πάσα ώρα και στιγμή το που βρίσκεται δίνει σαφή, ακριβή και έγκαιρη πληροφόρηση στον δράστη να επιχειρήσει στον χώρο από τον οποίον απουσιάζει το θύμα. Ποιος έδωσε την πληροφορία; Το ίδιο το θύμα με ανάρτηση μέσω των εφαρμογών κοινωνικής δικτύωσης. Ποια άλλη ασφαλέστερη πληροφόρηση μπορούσε να αναμένει ο δράστης;

Και παραπέρα πόσοι χρήστες ηλεκτρονικών υπηρεσιών επικοινωνίας έχουν ασχοληθεί σοβαρά με πρακτικές επιλογές ασφάλειας; Από τα πιο απλά της μη κοινοποίησης πληροφόρησης αναφορικά με την κίνηση του ιδίου, μέχρι την συγκέντρωση σειράς αυστηρών προσωπικών στοιχείων, σε μια συσκευή ενός smartphone, ιδιαίτερα αν παρέχεται επαρκής αποθηκευτικός χώρος. Στοιχεία όπως κωδικοί πρόσβασης σε τραπεζικούς λογαριασμούς και μάλιστα όχι με υποτυπώδη έστω κρυπτογράφηση (διότι υπάρχει ο κίνδυνος να ξεχάσουν την λογική δομή της), προγραμματισμός ενεργειών και σημειώσεις σημαντικών γεγονότων, αρχεία με στοιχεία ή απεικονίσεις πιστωτικών ή χρεωστικών καρτών, προσωπικοί αριθμοί φορολογικού μητρώου (ΑΦΜ) ή μητρώου κοινωνικής ασφάλισης (ΑΜΚΑ), κλειδάριθμοι TAXISnet (για την Ελλάδα), δελτίου αστυνομικής ταυτότητας κλπ, δίνουν περισσότερα από όσα στοιχεία χρειάζεται ένας δράστης ηλεκτρονικού εγκλήματος για μια ηλεκτρονική απάτη λ.χ., επιτρέποντάς του με μόνη την κλοπή του smartphone να έχει, στην περίπτωση ενός οικογενειάρχη για παράδειγμα,

πρόσβαση στο χαρτοφυλάκιό του, αλλά ακόμη και εικόνα αναφορικά με κοντινά και σημαίνοντα γι αυτόν πρόσωπα, όπως είναι τα παιδιά του.

Η κοινωνική διάσταση της τάσης για έκθεση της προσωπικής στιγμής αυξάνει από μόνη της το έδαφος και τις ευκαιρίες για προσβολή εννόμων αγαθών μέσα από την εγκληματική δράση. Αυτή η «αρωγή» από το ίδιο το θύμα, δεν μπορεί να αξιολογηθεί εκτός ψηφιακού περιβάλλοντος, ακόμη και στις περιπτώσεις που η εγκληματική δράση είναι εκείνη της εκβίασης, αφού βέβαια ο δράστης έχει στα χέρια του τέτοια στοιχεία τα οποία δύσκολα θα μπορούσε να παραβλέψει το θύμα και μην λάβει σοβαρά υπόψη του την απειλή. Πόσο εύκολα θα μπορούσε να παραβλέψει μια απειλή ο Χ επιχειρηματίας όταν αποστέλλεται ως συνοδευτική ενός μηνύματος μια φωτογραφία του παιδιού του από το προαύλιο του σχολείου του;

Μήπως τελικά η ψηφιακή εγκληματικότητα είναι παραμετροποίηση του τρόπου κοινωνικής συμπεριφοράς και απότοκος του καταναλωτικού προφίλ του μέσου ανθρώπου στην κοινότητα;

3. ΤΑ ΨΗΦΙΑΚΑ ΠΕΙΣΤΗΡΙΑ

i. Μια πρώτη εννοιολογική προσέγγιση. Ψηφιακά Πειστήρια, Ψηφιακή Εγκληματολογία και Ψηφιακή Απόδειξη.

Μια πρώτη αναφορά στα *ψηφιακά πειστήρια* τα εντάσσει, κατ' αναγκαία λογική συνθήκη, στα αντικείμενα του ψηφιακού κόσμου. Ενός κόσμου, που κατακλύζει πλέον ολοένα και περισσότερο την ανθρώπινη δραστηριότητα σε όλες τις δομές και τα επίπεδά της (ατομικό – κοινωνικό, εθνικό – διεθνές κλπ). Ενός κόσμου, που καταφέρνει και παραμένει καινοτόμος και παρωχημένος ταυτόχρονα μέσα από μια φιλοσοφική προσέγγιση. Παρωχημένος καθόσον αυτό που ήταν καινοτόμο το 2010 λίγο καιρό μετά ήταν ήδη ξεπερασμένο και σε σύγκριση με το σήμερα, η τεχνολογική απόσταση είναι τέτοια που το καθιστά κυριολεκτικά παρωχημένο.

Κατά την παραδεδεγμένη εννοιολογική προσδιοριστική θέση, τα ψηφιακά πειστήρια είναι τα αντικείμενα εκείνα τα λειτουργούν ως υλικές συσκευές που μπορούν να φιλοξενήσουν και να αποθηκεύσουν σε ψηφιακή μορφή δεδομένα. Τέτοια δεδομένα είναι διάφορα αρχεία κειμένου, εικόνας, ήχου, εικόνας και ήχου σε μορφότυπο .doc, .docx. exe. .pdf, .mp3, .mp4 κλπ. Τα ψηφιακά στοιχεία, που είναι συσχετισμένα με μια εγκληματική συμπεριφορά μπορούν να δώσουν ποικίλα δεδομένα ανάλογα με το μορφότυπο του φορέα που τα φιλοξενεί αλλά και την δικτύωση του φορέα αυτού ενδεχόμενα με άλλες ηλεκτρονικές συσκευές.

Την διαχείριση των ερευνών αναφορικά με τα ψηφιακά πειστήρια, με την έννοια της πρωτοβουλίας στις ενέργειες βάσει των διεθνώς αναγνωρισμένων πρωτοκόλλων, έχει ειδική εξειδικευμένη μονάδα ανθρωπίνου δυναμικού, που κινείται στα πλαίσια ειδικού τομέα πραγματογνωμοσύνης. Όταν αφορά δε τη σχετική έρευνα στην εξιχνίαση ηλεκτρονικών εγκλημάτων τότε βρισκόμαστε στον χώρο της *Ψηφιακής Εγκληματολογίας* (Digital Forensics) ή αλλιώς Ηλεκτρονικής Εγκληματολογίας[61] (αναφερόμενη και ως ψηφιακή εγκληματολογική επιστήμη). Πρόκειται για αναπτυσσόμενο κλάδο της εγκληματολογίας, που περιλαμβάνει τον εντοπισμό και εξασφάλιση της ακεραιότητας των πειστηρίων, την ανάκτηση και διερεύνηση ψηφιακού υλικού, το οποίο εντοπίζεται σε ψηφιακές συσκευές συνήθως εμπλεκόμενες σε ηλεκτρονικά εγκλήματα, και την κατάρτιση και υποβολή σχετικών εκθέσεων με νομικά

[61] Βλ. https://www.el.wikipedia.org/wiki/Ψηφιακή_εγκληματολογία

αποδεκτό τρόπο. Σε ανώτερα εξειδικευμένα επίπεδα επιστημοσύνης, η ψηφιακή εγκληματολογία χωρίζεται σε διάφορους κλάδους, ανάλογα με τον τύπο των συσκευών, των μέσων ή των αντικειμένων, σε εγκληματολογία Υπολογιστών, εγκληματολογία Κινητών Συσκευών, εγκληματολογία Δικτύων, εγκληματολογία Ανάλυσης Δεδομένων, εγκληματολογία Βάσεων Δεδομένων.

Κοντά στις προσεγγίσεις αυτές είναι και η αναφορά στον ορισμό *ψηφιακή απόδειξη*[62], που αναφέρεται στην πληροφορία ή το δεδομένο, που προκύπτει από την αποδεικτική αξιοποίηση ενός ψηφιακού πειστηρίου, μέσα από το πρωτόκολλο διαχείρισής του ως αποδεικτικό στοιχείο. Ιδιαίτερα δε χαρακτηριστικά της ψηφιακής απόδειξης είναι η λανθάνουσα μορφή της (όπως λ.χ. ένα αποτύπωμα ή στοιχείο DNA), η ταχύτατη διασυνοριακή διάδοσή τους[63], το ευμετάβλητο και ευπαθές στην υπόστασή τους και η υπερευαισθησία στον χρονικό εντοπισμό τους (πτητικότητα ψηφιακών δεδομένων).

Συνωδά προσεγγίζουμε και τον εννοιολογικό καθορισμό του *αναλυτή*[64] των ψηφιακών πειστηρίων, ως τον ειδικά εκπαιδευμένο επαγγελματία, του οποίου έργο είναι η συλλογή, αναγνώριση και ανάλυση των αποδείξεων από ψηφιακά πειστήρια από συσκευές που μπορούν να φιλοξενήσουν και να αποθηκεύσουν σε ψηφιακή μορφή δεδομένα. Ο ερευνητής αυτός συγκεντρώνει τις ιδιότητες να κατανοεί τα ψηφιακά πειστήρια και τον τρόπο λειτουργίας τους, να διακρίνει μια μέθοδο ως νόμιμη, παράνομη, ηθική ή ανήθικη αναφορικά με τη συγκέντρωση δεδομένων και πληροφοριών, να γνωρίζει το νόμο και τα πλαίσια που καθορίζουν την διαδικασία της ψηφιακής πραγματογνωμοσύνης, να γνωρίζει την πιθανότητα κακόβουλης επίθεσης αλλά και πώς να την προλαμβάνει. Να γνωρίζει περαιτέρω τις αρμόδιες αρχές, την χρήση των ψηφιακών πειστηρίων στον δικαιϊκό χώρο καθώς επίσης να γνωρίζει και να καθορίζει πλαίσια για τις διαδικασίες και υποδείξεις για την χρήση των εργαλείων που χρησιμοποιεί. Τέλος να είναι σε θέση να μπορεί να αναλύει αλλά και να παρουσιάζει με τρόπο κατανοητό την εργασία του με την σύνταξη έκθεσης πραγματογνωμοσύνης αλλά και δια ζώσης, όταν και όπου παρασχεθεί ανάγκη δίνοντας απαντήσεις και επεξηγήσεις σε ερωτήματα που ανακύπτουν.

Τα ψηφιακά πειστήρια λοιπόν είναι τα στοιχεία εκείνα, που αποτελούν την βάση, το ερευνητικό αντικείμενο, για την διεξαγωγή ειδικής πραγματογνωμοσύνης, την οποία

[62] Βλ. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, «Electronic Crime Scene Investigation, A Guide for First Responders, Second Edition», σελ. xi.
[63] Βλ. *Δ. Κιούπης*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, σε Θ. Δαλακούρα, Το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 42.
[64] Βλ. *Γ. Μπουρμάς*, Η νομιμότητα των ερευνών σε ηλεκτρονικά δίκτυα και δεδομένα στις περιπτώσεις εγκλημάτων στον κυβερνοχώρο, ΠοινΔικ 2019, 563 επ.

συναντούμε κυρίως ως ανακριτική πράξη κατά την διερεύνηση των συνθηκών τέλεσης (τρόπος, τόπος, χρόνος, αποδείξεις) και την ανάδειξη ή υπόδειξη του προσώπου, που σχετίζεται με την διάπραξη του υπό έρευνα ηλεκτρονικού εγκλήματος ή μιας σχετικής αδικοπρακτικής συμπεριφοράς, όταν η αναφορά γίνεται στον χώρο του αστικού δικαίου. Περισσότερο εξειδικευμένα για τον χώρο της ποινικής δικαιοσύνης, τα ψηφιακά στοιχεία είναι πληροφορίες και δεδομένα αξίας σε μια έρευνα που αποθηκεύονται, λαμβάνονται ή μεταδίδονται από μια ηλεκτρονική συσκευή και σχετίζονται με την διάπραξη εγκληματικής συμπεριφοράς[65].

Η ειδική πραγματογνωμοσύνη, που προαναφέρεται, είναι μια παραγωγική διαδικασία, που στηρίζεται στη χρήσης της ειδικής επιστημονικής γνώσης για την αναγνώριση, συλλογή, την ανάκτηση, τη διερεύνηση υλικού που βρίσκεται σε ψηφιακές συσκευές, συχνά σε σχέση με το ηλεκτρονικό έγκλημα[66], την ανάλυση και την υποβολή αποδεικτικών στοιχείων στα δικαστήρια[67]. Αυτή η εννοιολογική προσέγγιση περιβάλλει τον όρο «πειστήρια» κατά την αντίστοιχη λεκτική απόδοση του διεθνώς κρατούντος όρου «Forensics». Οι πραγματογνώμονες ασχολούνται κυρίως με την ανάκτηση και την ανάλυση λανθάνουσας απόδειξης. Οι λανθάνουσες ενδείξεις, όπως αναφέρθηκε και παραπάνω, μπορούν να λάβουν πολλές μορφές, από τα δακτυλικά αποτυπώματα που απομένουν σε ένα παράθυρο, στο DNA από στοιχεία που ανακτώνται από λεκέδες αίματος, στα αρχεία σε έναν σκληρό δίσκο και στη διαδρομή αναζήτησης στο διαδίκτυο ή στο περιβάλλον του συστήματος υπολογιστή.

Οι έρευνες ψηφιακής εγκληματολογίας έχουν ποικίλες εφαρμογές. Η πιο διαδεδομένη αλλά και αντιληπτή από το μέσο άνθρωπο είναι η υποστήριξη ή αντίκρουση μιας υπόθεσης ενώπιον ποινικών ή πολιτικών δικαστηρίων[68]. Η αναφορά στην έννοια της ποινικής υπόθεσης αντιστοιχεί στην έννοια του ποινικού φαινομένου, όπως αυτό διαμορφώνεται μέσα από κανόνες αυστηρής εφαρμογής από το Κώδικα Ποινικής Δικονομίας (στο εξής ΚΠοινΔ). Η αξία των ευρημάτων και πορισμάτων μέσα από την διαδικασία ψηφιακής ανάλυσης έχει την χρησιμότητά της και στον χώρο του αστικού δικαίου, όπου η διαχείριση έχει να κάνει με εκείνους που ασχολούνται κυρίως με ζητήματα, τα οποία αφορούν στην προστασία των

[65] Βλ. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, «Electronic Crime Scene Investigation, A Guide for First Responders, Second Edition», από τους *M. B. Mukasey, J. L. Sedgwick, D. W. Hagyhttps*://www.ncjrs.gov/pdffiles1/nij/219941.pdf

[66] Βλ. *B. Carrier*, «Defining digital forensic examination and analysis tools», International Journal of Digital Evidence 1, 2003, σελ. 2 επ. σε http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.14.9813&rep=rep1&type=pdf

[67] Βλ. United States - Computer Emergency Readiness Team [US-CERT], Computer Forensics, sel. 1 https://www.us-cert.gov/sites/default/files/publications/forensics.pdf

[68] Βλ. *C. Brown*, «Computer Evidence: Collection & Preservation.» Hingham, Thomson/Delmar, 2006

δικαιωμάτων προστασίας προσωπικών δεδομένων και της διανοητικής ιδιοκτησίας, της βιομηχανικής ευρεσιτεχνίας και εν γένει της περιουσίας των ιδιωτών, χωρίς όμως να αποκλείεται και η περίπτωση που αφορά σε συμβατικές διαφορές μεταξύ εμπορικών οντοτήτων, όπου μπορεί να εμπλέκεται μια μορφή ψηφιακής αδικοπραξίας. Το αντικείμενο όμως της αστικής πτυχής της αξιοποίησης των πορισμάτων μια ψηφιακής πραγματογνωμοσύνης εκφεύγει της παρούσας μελέτης.

Όπως αναφέρθηκε και στην εισαγωγική αναφορά, έχει επικρατήσει στην επιστημονική κοινότητα μια σειρά εννοιολογικού κατακερματισμού του τομέα της ψηφιακής έρευνας σε επί μέρους κι εξειδικευμένους τομείς, που σχετίζονται με τον τύπο του ψηφιακού περιβάλλοντος στο οποίο εμπλέκονται και λειτουργούν.

Έτσι προκύπτει η πραγματογνωμοσύνη των ηλεκτρονικών υπολογιστών, των δικτύων και ειδικότερα της ασφάλειας στην επικοινωνία, στην ανάλυση δεδομένων και πληροφοριακών συστημάτων[69] και σε εκείνη που αναφέρεται στην χρήση και τα δεδομένα των κινητών ηλεκτρονικών συσκευών. Πολύ πρώιμα στην παρούσα μελέτη, μπορούμε σχηματικά να αναφέρουμε ότι η τυπική δομή της ψηφιακής πραγματογνωμοσύνης περιλαμβάνει τον εντοπισμό, την ανάκτηση, εξαγωγή, ανάλυση και ερμηνεία των ψηφιακών στοιχείων της έρευνας[70] και την σύνταξη και υποστήριξη (όπου και όταν το απαιτήσουν οι συνθήκες) μιας έκθεσης αναφορικά με τα συλλεγέντα στοιχεία[71]. Πέρα από το στοιχείο του εντοπισμού και της ανάδειξης αποδεικτικών στοιχείων ενός εγκλήματος, η ψηφιακή εγκληματολογία μπορεί να συνδέσει συγκεκριμένα δεδομένα της έρευνας σε συγκεκριμένους υπόπτους, να επιβεβαιώσει αλλοιώσεις ή μέσα από συσχέτιση των δεδομένων που προέκυψαν από την έρευνα να προσδιορίσει την πρόθεση του δράστη στον οποίον αποδίδεται η συγκεκριμένη κατηγορία.

ii. Ο διφυής χαρακτήρας των ψηφιακών πειστηρίων κατά την αξιοποίησή τους.

[69] Βλ. *J. Brunty*, «Validation of Forensic Toolsand Software, «A Quick Guide for the Digital Forensic Examiner», 2011, https://www.researchgate.net/profile/Josh_Brunty/publication/320808735_Validation_of_Forensic_Tools_and_Software_A_Quick_Guide_for_the_Digital_Forensic_Examiner/links/5e2f0643a 6fdcc3096941501/Validation-of-Forensic-Tools-and-Software-A-Quick-Guide-for-the-Digital-Forensic-Examiner.pdf

[70] Βλ. *Β. Κάτος*, Ψηφιακά Πειστήρια, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 64, *A. Huseinović, S. Mrdović*, «Comparison of Computer Forensics Investigation Models for Cloud Environment», http://people.etf.unsa.ba/~smrdovic/publications/MIPRO2018_Huseinovic_Mrdovic.pdf

[71] Βλ. *M. Reith, C. Carr, G. Gunsch*, An examination of digital forensic models. International Journal of Digital Evidence, (2002), https://pdfs.semanticscholar.org/c73f/47d8385f452dfd25bbaab754874b65594ccd.pdf https://el.wikipedia.org/wiki/Ψηφιακή_Εγκληματολογία

Επειδή η ειδική πραγματογνωμοσύνη αναφορικά με την εγκληματική δράση στον τομέα των ηλεκτρονικών υπολογιστών και του διαδικτύου είναι ύλη εργασίας, που απαντάται σε όλες τις κοινωνικές δομές, έστω και με διαφορετικά επίπεδα χρήσης, κρίσιμο στοιχείο αναδεικνύεται το εάν και κατά πόσο μπορούμε να κάνουμε λόγο για κοινές δομές όταν ο λόγος αφορά για επιστημονική ανακριτική εργασία σε διαφορετικά δικαιϊκά συστήματα.

Εδώ θα πρέπει να γίνει μια πρώτη διάκριση και αυτή αφορά το μεν το τεχνοκρατικό μέρος της έρευνας, το δε αφορά στην δικαιϊκή πλαισίωση και νομιμοποίηση της έρευνας. Κατ' αρχήν η τεχνοκρατική αναζήτηση δεν μπορεί να γνωρίζει όρια και περιορισμούς. Φραγμοί στην τεχνολογία μπορούν να τεθούν μόνο από δικαιϊκούς κανόνες και από ηθικές ενστάσεις, στο μέτρο που οι τελευταίες απηχούν φωνές σημαντικού κέντρου αποφάσεων. Λ.χ. μια πυρηνική κεφαλή, συναρμοσμένη σε σχηματισμό που μπορεί να βάλει, ως όπλο καταστροφής, σαφώς και είναι ένα τεχνολογικό επίτευγμα. Καίτοι όμως η σχετική ένσταση για την χρήση του απηχεί τον λόγο της συντριπτικής πλειοψηφίας των ανθρώπων του πλανήτη, την τελική απόφαση για έγκριση ή τερματισμό της παραγωγικής διαδικασίας του συγκεκριμένου όπλου, θα την έχει προνομιακά μια μειοψηφία που είναι το εκτελεστικό κέντρο αποφάσεων, συνήθως και ο χρηματοδότης ή ο κυβερνητικός σχηματισμός που διαχειρίζεται την κατάσταση. Το τεχνολογικό επίτευγμα, αποκομμένο από το λειτουργικό του αποτέλεσμα παραμένει τεχνικά εντυπωσιακό και ηθικά αποτροπιαστικό.

Στα ίδια πλαίσια το γεγονός ότι το αντικείμενο ηλεκτρονικός υπολογιστής είναι ένα και το αυτό τεχνικό μέγεθος, ακόμη και στις δομές του διαδικτύου των πραγμάτων, της υπολογιστικής νέφους, της μηχανικής μάθησης αλλά και της τεχνητής νοημοσύνης, προφανώς η *τεχνοκρατική γλώσσα,* η οποία χρησιμοποιείται για την ανάλυση, κατανόηση της λειτουργίας του και τον τεχνολογικό κατακερματισμό του, είναι ενιαία αλλά και μοναδική. Ο σκληρός δίσκος για παράδειγμα, ο τρόπος λειτουργίας των στρωμάτων επικοινωνίας στην μεταφορά πακέτων, είναι ο ίδιος σε κάθε περίπτωση, όπου και αν απαντάται η σχετική λειτουργία. Όταν λέμε ίδιος, αναφερόμαστε σαφώς στην τεχνική δομή, λειτουργικότητα και κανόνες χρήσης, που προβλέπονται από τον κατασκευαστή. *Η ψηφιακή γλώσσα είναι μια διεθνής γλώσσα.* Ο Χ ηλεκτρονικός υπολογιστής είτε συνδεθεί είτε λειτουργεί εκτός δικτύωσης στην χώρα Α επιτελεί τις ίδιες λειτουργίες και με την ίδια λειτουργική προσέγγιση που θα λειτουργήσει στην χώρα Β. Παραπέρα η έννοια και η τεχνολογική δομή της ασύρματης ή της ενσύρματης δικτύωσης παραμένει μια, με διαφοροποιήσεις ανάλογα με την τεχνική δομή, που όμως λειτουργεί με τον ίδιο τρόπο όταν είναι του αυτού τεχνολογικού επιπέδου.

Έτσι λοιπόν το πρόβλημα της εφαρμογής διαφορετικών δικαιικών συστημάτων σχετικά με το αξιόποινο συμπεριφορών στον ψηφιακό χώρο αλλά και την διαχείριση των ψηφιακών στοιχείων σε μια ποινική δίκη, ισορροπείται κατά κάποιον τρόπο από το γεγονός της *κοινής ψηφιακής γλώσσας*, η οποία επιτρέπει αναπαραγωγή μεθοδολογίας αλλά και επεξηγηματικές αναφορές, μέσα από την διακρατική συνεργασία των αρμοδίων και σχετιζομένων με το ηλεκτρονικό έγκλημα υπηρεσιών, σε σταθερό και τεχνολογικά ασφαλές έδαφος.

Η αποδοχή κοινών κανόνων[72] στην διαχείριση των δεδομένων, που προκύπτουν από την διενέργεια της ειδικής πραγματογνωμοσύνης, είναι ένα πρώτο βήμα αναφορικά με τον καθορισμό προϋποθέσεων χρήσης ενός πειστηρίου από ένα δικαιικό σύστημα όπου λαμβάνει χώρα η τεχνική του διαχείριση, σε ένα άλλο δικαιικό σύστημα όπου τελικά θα λάβει χώρα η δικαστική του αξιοποίηση. Επί του παρόντος τέτοια δικαιική ταύτιση δεν προκύπτει από το συγκριτικό δίκαιο. Δεν υπάρχει τέτοια αναφορά στην επιλογή των δικαιικών κανόνων που πλαισιώνουν την όλη ανακριτική διαδικασία.

Εκείνο το οποίο όμως σε κάθε περίπτωση πρέπει να αποτελεί κοινό τόπο είναι η παραδοχή ότι τα ψηφιακά πειστήρια, ως βάση για την εξαγωγή δεδομένων που θα λειτουργήσουν ως αποδεικτικά στοιχεία, έχουν ευρύτερο πεδίο, μπορεί να είναι περισσότερο προσωπικά, είναι μεταβλητά και η διαχείρισή τους απαιτεί διαφορετική κατάρτιση και ειδικά εργαλεία σε σύγκριση με την παραδοσιακή δομή των ερευνών σε φυσικά αποδεικτικά στοιχεία.

iii. Η ερευνητική πρόκληση.

Οι σημαντικές αλλαγές στο τοπίο της τεχνολογίας των πληροφοριών κατά την τελευταία ιδίως δεκαετία, έχουν καταστήσει τη συλλογή και ανάλυση των ψηφιακών στοιχείων όλο και πιο σημαντικό εργαλείο αναφορικά με την ενίσχυση του αποδεικτικού υλικού ή την κατάστρωση της υπερασπιστικής στρατηγικής στις περιπτώσεις των ηλεκτρονικών εγκλημάτων και την σχετική προετοιμασία αλλά και διεκπεραίωση δικαστικών υποθέσεων. Καθώς η τεχνολογία έχει γίνει πιο ευέλικτη, με φορητές προτάσεις τόσο ως προς τις υπολογιστικές μηχανές όσο και ως προς τη δικτύωση, αλλά και ισχυρή από

[72] Βλ. κατωτέρω υπό 10. Πρωτόκολλο Έρευνας και Διαχείρισης των Ψηφιακών Πειστηρίων και των Ψηφιακών Δεδομένων, σελ. 173 επ.

πλευράς τεχνολογικών δυνατοτήτων, που παρέχονται προς τους χρήστες, μεγαλύτερες ποσότητες από πληροφορίες δημιουργούνται, αποθηκεύονται και προσπελάζονται.

Οι σύγχρονες συσκευές μπορούν να χρησιμεύσουν ως τεράστιο αποθετήριο προσωπικών πληροφοριών ακόμα και σε περιπτώσεις φορητών προτάσεων, που μεταφέρονται εύκολα σε μια τσέπη και έχουν πρόσβαση με ένα μόνο χέρι ή ακόμα και φωνητική καθοδήγηση - εντολή. Υπάρχει ένα σαφές πλεονέκτημα από την διαχείριση πολλών πόρων πληροφόρησης για την εξιχνίαση μια εγκληματικής δράσης και ενδεχόμενα για την αιτιολόγηση καταδικαστικών αποφάσεων και γενικά για την εφαρμογή κι επιβολή του νόμου. Την ίδια όμως στιγμή είναι απαραίτητη η προσεκτική διαχείριση της δυνατότητας αυτής από εκείνους, που θεσμικά εμπλέκονται στην διαχείριση των αποδεικτικών αυτών στοιχείων, των οποίων η προσοχή πρέπει να εστιάσει στην διατήρηση της νομιμότητας αναφορικά με την άντληση των ψηφιακών δεδομένων αλλά και στην διατήρηση ακέραιου του περιβάλλοντος προστασίας των προσωπικών δεδομένων, όπου με τις ενέργειές τους ελλοχεύει κίνδυνος προσβολής του σκληρού πυρήνα κάποιας ατομικής ελευθερίας.

Το ενδιαφέρον και η προσοχή εστιάζεται στην εξισορρόπηση ανάμεσα στην ανάκτηση και συνεπώς στο παραδεκτό της χρήσης και αξιοποίησης των ψηφιακών στοιχείων με ταυτόχρονο έμπρακτο ενδιαφέρον και ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής[73], ατομικών ελευθεριών και συναφών δικαιωμάτων, ακόμη και στην περίπτωση που αναφερόμαστε στο πρόσωπο του ιδίου του κατηγορουμένου, πολύ δε περισσότερο όταν η αναφορά σχετίζεται με αμέτοχα τρίτα πρόσωπα.

Η χρησιμοποίηση και δικαστική εκμετάλλευση ψηφιακών στοιχείων είναι ένα σχετικά νέο εργαλείο για το δίκαιο, σχεδόν σε όλα τα δικαιικά συστήματα των αναπτυγμένων κοινωνιών, ωστόσο η εφαρμογή του νόμου μέσα από την τα διατακτικά των δικαστικών αποφάσεων βασίζεται ολοένα και περισσότερο στα ψηφιακά στοιχεία για σημαντικές πληροφορίες σχετικά με την εξεύρεση της ουσιαστικής αλήθειας και την αξιολόγηση των ισχυρισμών τόσο του δράστη όσο και του θύματος. Λόγω της αποδεικτικής ευκρίνειας και συναφούς αποδεικτικής ασφάλειας, που προκύπτει από την χρήση των ψηφιακών πειστηρίων, όπου αυτά προσφέρονται, αντιλαμβάνεται κανείς πόσο δυσκολότερες είναι οι περιπτώσεις δικαστικής διερεύνησης ή ανακριτικής διαχείρισης μιας ποινικής υπόθεσης, όταν απουσιάζουν αυτά τα στοιχεία.

[73] Βλ. *S. E. Goodison, R. C. Davis, and Br. A. Jackson*, Digital Evidence and the U.S. Criminal Justice System, Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

Παρακάτω παρατίθενται σε χωριστή ενότητα[74] ενδεικτικές αναφορές σε περιπτώσεις όπου η εκάστοτε υπόθεση, που απασχόλησε την δικαστηριακή πρακτική σε περιβάλλον ποινικής δίκης, αιτιολογήθηκε ή εξιχνιάστηκε μέσα από την αξιοποίηση των δεδομένων, τα οποία προέκυψαν από την ψηφιακή εξέταση που διενεργήθηκε. Υποθέσεις, από το αποδεικτικό υλικό των οποίων αν αφαιρεθεί το προϊόν της ψηφιακής πραγματογνωμοσύνης, ενδεχομένως δεν έχουν τίποτε, που να απομένει ως αποδεικτό υπόλοιπο, ικανό ώστε να οδηγήσει σε αιτιολογημένη κρίση τον δικαστή και σε αρκετές περιπτώσεις η υπόθεση να μην φτάσει ποτέ να αξιολογηθεί από την δικαιοσύνη ή την τοπική αρμόδια αστυνομική αρχή.

[74] Βλ κατωτέρω υπό 5. Επισκόπηση Δικαστικής Εφαρμογής και Αποδεικτικής Αξιοποίησης των Ψηφιακών Δεδομένων, σελ. 53 επ.

4. Η ΣΗΜΑΣΙΑ ΤΩΝ ΨΗΦΙΑΚΩΝ ΠΕΙΣΤΗΡΙΩΝ ΣΤΗΝ ΑΝΑΚΡΙΤΙΚΗ ΕΡΕΥΝΑ

i. Η Ανακριτική Διαδικασία ως στάδιο της ποινικής διαδικασίας.

Θα ήταν λογικά ασύνδετη μια αναφορά στην σημασία των ψηφιακών πειστηρίων στην ανακριτική έρευνα και στα στοιχεία που μπορούν να αντληθούν από την εξέτασή τους, χωρίς να ενταχθεί η όλη ερευνητική διαδικασία, που αποτελεί το κύριο αντικείμενο της μελέτης αυτής, στην σπονδυλωτή διάταξη ύλης, την οποία προβλέπει για την διαχείριση μιας ποινικής υπόθεσης ο Κώδικας Ποινικής Δικονομίας (Κ.Ποιν.Δ.).

Πολύ λακωνικά, αναφέρουμε ότι η ανάκριση εντάσσεται λειτουργικά στο στάδιο της προδικασίας, που είναι το στάδιο, το οποίο προηγείται της κύριας διαδικασίας, που είναι η μορφή της ποινικής δίκης, η οποία ως προσλαμβάνουσα παράσταση είναι η κρατούσα στην συνείδηση του μέσου ανθρώπου απεικόνιση της δικαστικής αξιολόγησης και διαχείρισης μιας ποινικής υπόθεσης, που συνήθως καταλήγει να κρίνεται ενώπιον ακροατηρίου.

Πρόκειται για διαδικασία, η οποία εντάσσεται στη, μετά την άσκηση της ποινικής δίωξης δικονομική, διάρθρωση του Κ.Ποιν.Δ.[75], που αφορά την προδικασία, δηλαδή την προετοιμασία του φακέλου πριν την εισαγωγή του στο στάδιο της κυρίας διαδικασίας, πολύ δε απλοϊκά, πριν την έναρξη της ποινικής δίκης στο ακροατήριο. Αποτελείται από τρία επί μέρους τμήματα, την προκαταρκτική εξέταση (αρ. 243 Κ.Ποιν.Δ.), την προανάκριση (αρ. 245 Κ.Ποιν.Δ.) και την κύρια ανάκριση (αρ. 246 Κ.Ποιν.Δ.). Βασικός σκοπός όλων αυτών των διαδικαστικών σταδίων, που δεν είναι απαραίτητο ότι η υπόθεση θα διέλθει από όλα τους, είναι η έρευνα της υπόθεσης. Με άλλα λόγια η συγκέντρωση υλικού σχετικού με την κατηγορία, προκειμένου στην συνέχεια να γίνει η σχετική αξιολόγηση για την αξιοποίησή του, με προσανατολισμό πάντοτε την εξεύρεση της ουσιαστικής αλήθειας[76] και όχι με αναγκαστική προσέγγιση εκείνη της στήριξης της κατηγορίας.

Ο αυστηρός χαρακτήρας των διατάξεων του Κ.Ποιν.Δ. επιβάλλει πρώτα από όλα την διαφύλαξη του κύρους της ίδιας ποινικής δικαιοσύνης. Αυτό επιτυγχάνεται (όχι πάντοτε απόλυτα) με την λειτουργία μηχανισμών προστασίας του όλου νομικού οικοδομήματος από

[75] Βλ. αρ. 239 επ. Κ.Ποιν.Δ., στο Γ΄ βιβλίο.

[76] Βλ. αρ. 239 § 2 Κ.Ποιν.Δ., *Β. Αδάμπας, Μ. Παπαχρήστου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, τομ. Α, Νομική Βιβλιοθήκη 2018, σελ. 1437 επ., *Θ. Δαλακούρας*, Περί του σκοπού της ποινικής δίκης, ΠοινΛογ, 2007, 1195, *Αδ. Παπαδαμάκης*, Προκαταρκτική εξέταση – προανάκριση: Μορφές και όρια της ερυενητικής δραστηριότητας, ΠοινΔικ 2008, 338 επ.

κακόβουλες διαχειρίσεις, όπως η λειτουργική του έκπτωση μέσα από την επιλογή της υποβολής μιας μήνυσης ή μιας έγκλησης από κάποιον, στηριζόμενη όμως επί αβασίμων κατηγοριών, προκειμένου να επιτευχθούν στόχοι και προσδοκίες που έχουν την βάση τους στις προσωπικές διαθέσεις, αντιπαλότητες και σκοπιμότητες του καταγγέλλοντος κατά του κατηγορουμένου.

Όλο το πνεύμα λοιπόν της προδικαστικής έρευνας κινείται στα πλαίσια της αναζήτησης της αλήθειας με σεβασμό στα δικαιώματα και τις ατομικές ελευθερίες των εμπλεκομένων προσώπων. Είναι αυτό που σε άλλο σημείο αυτής της καταγραφής παρουσιάσθηκε με την διαφοροποίηση της θέσης δράστη – διωκτικής αρχής, όπου ο πρώτος έχει το πλεονέκτημα της πρωτοβουλίας στις κινήσεις και τους προσανατολισμούς, χωρίς κανένα νομικό φραγμό (εξ άλλου η δράση του έχει την βάση της στην προσβολή νομικών κανόνων), ενώ η δεύτερη είναι υποχρεωμένη για να απαιτήσει την εφαρμογή του νόμου, να είναι η ίδια πάντα σύννομη και συνεπής.

Κατά την περιεκτική και κατατοπιστική αναφορά στο άρθρο 239 Κ.Ποιν.Δ., σκοπός της ανάκρισης, στη γενική της θεώρηση ως προδικασία, είναι η συλλογή των αναγκαίων αποδεικτικών στοιχείων (ουσιωδών κυρίως, κατά τον επιμερισμό ύλης σε μια ποινική δικογραφία, σύμφωνα με την πρακτική που ακολουθείται σε πολλές Εισαγγελίες) προκειμένου να βεβαιωθεί, με διαφορετικό βαθμό πιθανολόγησης ανά ερευνητικό στάδιο, η τέλεση αξιόποινης πράξης και να αποφασιστεί[77] αν τελικά η υπόθεση θα πρέπει να εισαχθεί προς εκδίκαση ενώπιον του αρμοδίου δικαστικού σχηματισμού. Το ερευνητικό πεδίο καθορίζεται από την υπό δίωξη πράξη και όχι από τα πρόσωπα που καταρχήν εμπλέκονται καθόσον, χαρακτηριστικό της ποινικής δίωξης είναι η in rem άσκησή της, κάτι που με την σειρά του (νομικά) σημαίνει ότι εφόσον προκύψει σχετικό υλικό, τότε η δίωξη στρέφεται κατά οποιουδήποτε υπόπτου.

ii. Τα δικονομικά χαρακτηριστικά – Αρχές της Ανακριτικής Διαδικασίας.

Η ανακριτική διαδικασία εξ ορισμού καθορίζεται και πλαισιώνεται από κανόνες που χαρακτηρίζουν τον τρόπο λειτουργίας των ανακριτικών υπαλλήλων καθώς και το προϊόν της εξαγωγικής διαδικασίας. Οι κανόνες αυτοί στηρίζονται σε θεσμικές αρχές, οι οποίες και δίνουν συγκεκριμένα χαρακτηριστικά στην όλη διαδικασία.

[77] Από την Εισαγγελική Αρχή ή από το αρμόδιο Δικαστικό Συμβούλιο, ή από σύμφωνη γνώμη του Εισαγγελέα Εφετών και του Προέδρου Εφετών (στις ειδικά προβλεπόμενες περιπτώσεις συγκεκριμένων διώξεων σε περιπτώσεις κακουργημάτων)

Εξέχουσα θέση έχει η αρχή της αυτεπάγγελτης συγκέντρωσης του αποδεικτικού υλικού, σύμφωνα με την οποία τα όργανα που είναι επιφορτισμένα με το ανακριτικό έργο, δηλαδή οι ανακριτικοί (και άλλοτε προανακριτικοί) υπάλληλοι, ενεργούν κι επιχειρούν αναλαμβάνοντας πρωτοβουλία για την συγκέντρωση υλικού που σχετίζεται με την υπό έρευνα αξιόποινη δράση, χωρίς να δεσμεύονται από τις θέσεις και διαθέσεις των εμπλεκομένων προσώπων, ούτε να αναμένουν πρωτοβουλίες των ενδιαφερομένων προσώπων.

Στα χαρακτηριστικά της ανακριτικής διαδικασίας θα πρέπει να εντάξουμε και την αυστηρή προσήλωση στο ερευνητικό έργο χωρίς προσανατολισμούς και προσδοκίες είτε στήριξης της κατηγορίας είτε αποδόμησής της. Το έργο της διαδικασίας αυτής ολοκληρώνεται όταν έχουν εξαντληθεί, μέσα από την έρευνα, όλες οι πιθανές εκδοχές σχετικά με τον εντοπισμό της αλήθειας αναφορικά με την τέλεση της πράξης. Και όλα αυτά σε επίπεδο ενδείξεων ενοχής, διότι η απόδειξη της ενοχής απασχολεί τον Δικαστή, που θα κληθεί να κρίνει στο ακροατήριο[78].

Σημαντική εδώ είναι η αρχή της μυστικότητας της ανακριτικής διαδικασίας. Σε αντίθεση με την κυρία διαδικασία στην ανακριτική έρευνα και γενικότερα στο στάδιο της προδικασίας κρατεί η μυστικότητα των ενεργειών των εμπλεκόμενων λειτουργών. Αυτή η μυστικότητα καταρχήν αφορά στην απουσία δομών δημοσιότητας κατά την ρητή αναφορά του άρθρου 241 εδ. α΄ Κ.Ποιν.Δ. Με τον τρόπο αυτόν προστατεύεται κατ' αρχήν η έρευνα και η αποτελεσματικότητα της διαδικασίας ως σύνολο καθώς η δημόσια έκθεση των ενεργειών των αρμοδίων υπαλλήλων, ίσως θα έφερνε προσκόμματα μέσα από ενέργειες, που θα αλλοίωναν την γενική εικόνα και τα πειστήρια πριν την επέμβαση των ανακριτικών υπαλλήλων. Από την άλλη προστατεύεται και η προσωπικότητα του κατηγορουμένου, αλλά και σε ορισμένες περιπτώσεις και του καταγγέλλοντος – θύματος (ιδίως στα εγκλήματα όπου μετέχει ανήλικος ή αφορούν σε προσβολή της γενετήσιας ελευθερίας)[79]. Εννοείται ότι η αρχή της μυστικότητας κάμπτεται αναφορικά με την άσκηση δικαιωμάτων του κατηγορουμένου αλλά και του παρισταμένου προς υποστήριξη της κατηγορίας, μέσα από την αναγνώριση στον καθένα από αυτούς δικαιωμάτων, που στόχο έχουν την πληροφόρησή τους αναφορικά με την πορεία των ανακριτικών ενεργειών και των αποτελεσμάτων τους.

[78] Βλ. *Χ. Σεβαστίδης*, Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, 2015 τ. ΙΙΙ, σελ. 2798.
[79] Βλ. *Αργ. Καρράς*, Ποινικό Δικονομικό Δίκαιο, εκδ. ε΄ 2017, σελ. 371 επ., *Ν. Ανδρουλάκης*, Κώδικας Ποινικής Δικονομίας, 2015, σελ. 304

Η αρχή της αναλογικότητας και του σκοπού, είναι εξ ίσου σημαντική παράμετρος στην έρευνα, καθόσον η λειτουργική της παρουσία στον χώρο της ανάκρισης σχετίζεται με την προστατευτική εφαρμογή θεμελιωδών αρχών και κανόνων που προστατεύουν τα ατομικά δικαιώματα και τις σχετικές ελευθερίες του ατόμου, ως απόρροια της συνταγματικής αρχής του σεβασμού της ανθρώπινης αξιοπρέπειας. Σύμφωνα με την αρχή της αναλογικότητας, οι ενέργειες που εντάσσονται στην ανακριτική δραστηριότητα πρέπει να αποτελούν την προσφορότερη και αποτελεσματικότερη για τον επιδιωκόμενο *σκοπό* πρόταση, να λαμβάνουν χώρα μόνο στο μέτρο του *αναγκαίου* για την επίτευξη του σκοπού αυτού και να φροντίζει τον σκληρό πυρήνα των ατομικών δικαιωμάτων των θιγομένων προσώπων, στο μέτρο που τέτοιες ενέργειες ξεπερνούν το αναγκαίο μέτρο, ήτοι αποτελούν την όχι λιγότερο επαχθή επιλογή[80].

Στην ανακριτική διαδικασία επιτρέπεται κατ' αρχήν η χρήση κάθε αποδεικτικού μέσου, κατά τη ρητή αναφορά στο άρθρο 178 § 1 Κ.Ποιν.Δ. Η αναφορά σε ειδικότερες κατηγορίες αποδεικτικών μέσων (λ.χ. έγγραφα, μάρτυρες, πραγματογνωμοσύνη) έχει σαφώς ενδεικτικό χαρακτήρα, σύμφωνα με την βούληση του ιστορικού νομοθέτη[81], ο οποίος εκφράστηκε πανομοιότυπα με τη διατύπωση που κρατούσε κατά το προϊσχύσαν νομοθετικό καθεστώς. Πλέον η αποδεικτική απαγόρευση περιορίζεται στα αποδεικτικά εκείνα μέσα που αποκτήθηκαν με αξιόποινη πράξη ή προέκυψαν μέσω αξιοποίνων πράξεων.

iii. Η έκθεση ως δομικό στοιχείο στο σχηματισμό της ποινικής δικογραφίας.

Περαιτέρω στο στάδιο της ανάκρισης κρατεί ο έγγραφος τύπος. Ο έγγραφος τύπος διατηρεί ένα δικό του ιδιαίτερο πεδίο, το οποίο θα μας απασχολήσει στη συνέχεια ιδιαίτερα αναφορικά με την *ειδική έκθεση* του αρ. 265 § 3 Κ.Ποιν.Δ[82].

Στο εισαγωγικό σημείο, στο οποίο βρισκόμαστε αυτή τη στιγμή, θέση έχει η αναφορά σχετικά με τη δικονομική δομή της (έγγραφης) *έκθεσης* στο φαινόμενο της ποινικής δίκης και ειδικότερα στη σύνθεση της ποινικής δικογραφίας στην τεχνική της δομή.

---

[80] Βλ. *Χ. Σεβαστίδης*, Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, 2015 τ. ΙΙΙ, σελ. 2796 επ., *Β. Αδάμπας, Μ. Παπαχρήστου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, τομ. Α, Νομική Βιβλιοθήκη 2018, σελ. 1437 επ.,

[81] Βλ. 178 § 1 Κ.Ποιν.Δ., όπως αυτός (ο Κ.ΠοινΔ.) προέκυψε από το Ν 4620/2019 (ΦΕΚ Α 96/11.06.2019), που είναι ο νέος Κ.Ποιν.Δ., όπως αυτός τροποποιήθηκε με το Ν 4637/2019 (ΦΕΚ Α 180/18.11.2019).

[82] Βλ. 8. Η Κατάσχεση των Ψηφιακών Δεδομένων (Κατ' άρθρο 265 Κ.Ποιν.Δ., *viii. Η ειδική έκθεση της § 3*, σελ. 124 επ.

Η έκθεση από μόνη της ως εννοιολογικό περιεχόμενο δεν σημαίνει τίποτε διαφορετικό από την *παρουσίαση* ενός στοιχείου. Αυτό μπορεί να είναι μια ιδέα, μια διήγηση, μια καταγραφή, ένα στοιχείο πάντως, το οποίο μπορεί να αποδοθεί λεκτικά, ήτοι να περιγραφεί ορισμένα χωρίς να καταλείπεται αμφιβολία.

Δεν διαφέρει σε κάτι η εννοιολογική προσέγγιση του όρου στο πεδίο του Κ.Ποιν.Δ. Εδώ αποτελεί δικονομικό τεχνικό όρο, που αφορά στην έγγραφη κατάδειξη ενός εξελικτικού της ποινικής διαδικασίας γεγονότος. Πρόκειται για διαδικαστική πράξη, η οποία καθορίζεται αυστηρά ως προς τις προϋποθέσεις και της έννομες συνέπειές της, με περαιτέρω σκοπό την εξέλιξη ή την περάτωση ενός διαδικαστικού σταδίου[83] εννόμων συνεπειών. Αφορά σε δομικό στοιχείο της ποινικής δικογραφίας, με το οποίο εξασφαλίζεται η ακρίβεια των στοιχείων που αναδεικνύονται από την έρευνα ή η συντέλεση ή μη της δικονομικής εξέλιξης της ποινικής δίκης. Εξασφαλίζει τον αποκλεισμό εμπλουτισμού της ποινικής δικογραφίας με στοιχεία που δεν πληρούν τις προϋποθέσεις του νόμου, ή την άτακτη χρονικά είσοδό τους στην δικογραφία, με κύριο σκοπό την εξασφάλιση της προστασίας θεμελιωδών υπερασπιστικών δικαιωμάτων του κατηγορουμένου. Η σημασία της για την εξέλιξη της ποινικής δίκης είναι τόσο σημαντική που ο νομοθέτης επιφύλαξε σημαντικές συνέπειες σε περίπτωση που διαπιστωθεί πλημμέλεια στην σύνταξή της[84].

Ως υλική υπόσταση η έκθεση είναι πρώτα από όλα έγγραφο. Δεν προβλέπεται μια ψηφιακή δομή της και αυτό ως λογικό κενό θα μας απασχολήσει κατωτέρω[85]. Περαιτέρω συντάκτης του εγγράφου αυτού πρέπει να είναι δημόσιος υπάλληλος ο οποίος εκπληρώνει[86] καθήκοντα στην ποινική διαδικασία για να βεβαιώσει πράξεις, που ενήργησε ο ίδιος ή άλλος αρμόδιος δημόσιος υπάλληλος με τον οποίο συμπράττει ή δηλώσεις τρίτων προσώπων που απευθύνονται σε αυτούς. Συνεπώς έγγραφο δημοσίου υπαλλήλου, ο οποίος δεν έχει σχέση με την ποινική διαδικασία, δεν είναι έκθεση[87]. Στοιχεία της έκθεσης είναι η αναγραφή του τόπου και το χρόνου σύνταξής της.

---

[83] Βλ. *Αθ. Κονταξής*, Κώδικας Ποινικής Δικονομίας, Συνδυασμός θεωρίας και πράξης, α΄ τομ., Δ΄ εκδ., 2006, σελ. 1040.
[84] Βλ. *Θ. Δαλακούρας*, Ο νέος Κώδικας Ποινικής Δικονομίας, συνοπτική ερμηνεία κατ' άρθρο του Ν 4620/2019 (με ενημέρωση μέχρι το Ν4640/2019), 2019, Νομική Βιβλιοθήκη, σελ. 135.
[85] 8. Η Κατάσχεση των Ψηφιακών Δεδομένων (Κατ' άρθρο 265 Κ.Ποιν.Δ., viii. Η ειδική έκθεση της § 3, σελ. 124 επ.
[86] Βλ. *Θ. Δαλακούρας*, Ο νέος Κώδικας Ποινικής Δικονομίας, συνοπτική ερμηνεία κατ' άρθρο του Ν 4620/2019 (με ενημέρωση μέχρι το Ν4640/2019), 2019, Νομική Βιβλιοθήκη, σελ. 133.
[87] Βλ. *Μ. Γεωργιάδου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, τομ. Α, Νομική Βιβλιοθήκη 2018, σελ. 895 επ.,

Η αναγραφή, και μάλιστα απόλυτα ακριβής, του χρόνου σύνταξης της έκθεσης είναι μια άλλη σημαντική παράμετρος. Έχει μεγάλη σημασία και για τον λόγο αυτόν η έκθεση διαλαμβάνει (αρ. 151 Κ.Ποιν.Δ.) τόσο το χρονικό σημείο έναρξης της σύνταξής της όσο και λήξης της. Αυτό που φαίνεται κατ αρχήν ως υπερβολικό (λ.χ. θα μπορούσε να υποστηρίξει κανείς ότι η χρονοσήμανση με μόνη την αναγραφή της ημεροχρονολογίας θα ήταν αρκετή) ουσιαστικά είναι απόλυτα επιβεβλημένο. Η αμεσότητα[88] στην σύνταξη της έκθεσης είναι αναγκαία για την πιστότερη απόδοση του γεγονότος που καταγράφεται και βεβαιώνεται με αυτήν. Έτσι η απόδοση της ακριβούς χρονολογίας σύνταξης αποδεικνύει την χρονική εγγύτητα στην καταγραφή του γεγονότος, το οποίο βεβαιώνει, ώστε να αποθαρρύνει αντιρρήσεις και ενστάσεις σχετικά με την πιστότητα της καταγραφής, ή σχετικά με τη λογική ένταξή της στο χρόνο[89].

Η σημασία της για την ασφάλεια των καταγραφών, οι οποίες διαλαμβάνονται σε μια ποινική δικογραφία είναι τόσο μεγάλη κάτι που τελολογικά αναδεικνύεται μέσα από τις συνέπειες που επιφυλάσσει ο Κ.Ποιν.Δ. στις περιπτώσεις εκείνες, που δεν πληρούνται οι προϋποθέσεις για το παραδεκτό αυτής. Οτιδήποτε λοιπόν δεν διαλαμβάνεται σε έγκυρη και δικονομικά παραδεκτή έκθεση, αποκλείεται να χρησιμοποιηθεί ή να σηματοδοτήσει εξελικτικό στάδιο στην περαιτέρω πρόοδο της διαδικασίας, άλλως δημιουργεί ακυρότητα. Σημαντικά στοιχεία της η αναγραφή των στοιχείων των προσώπων που συμπράττουν (με τη μεγαλύτερη δυνατή λεπτομέρεια), η περιγραφή των όσων διαλαμβάνει με την μεγαλύτερη πιστότητα απόδοσης του γεγονότος (λ.χ. μαρτυρικής κατάθεσης, αυτοψίας, κατάσχεσης αντικειμένων), η υπογραφή της από τα πρόσωπα που μνημονεύονται ότι συνέπραξαν ή δηλώσεις ή πράξεις τους που διαλαμβάνονται σε αυτήν. Η αποδεικτική της δε ισχύς είναι απόλυτη, όπως όλων των δημοσίων εγγράφων, προσβαλλομένη μόνο για πλαστότητα, που πρέπει να επικαλεστεί και να αποδείξει εκείνος, που προβάλλει τον σχετικό ισχυρισμό.

Στο σημείο αυτό επιβάλλεται διευκρινιστικά να αναφερθεί ότι η απόλυτη αποδεικτική ισχύς μιας εκθέσεως έχει να κάνει με τα όσα βεβαιώνει ο ανακριτικός υπάλληλος, ενώ για το διανοητικό περιεχόμενο, που περιλαμβάνεται σε αυτήν αναφορικά με τις δηλώσεις τρίτων, οι οποίες βεβαιώνεται ότι ειπώθηκαν ή εγχειρίστηκαν σε αυτόν, χωρεί αντίθετη απόδειξη. Βεβαιώνεται δηλαδή το ότι εμφανίστηκε ενώπιον του ανακριτικού υπαλλήλου ο

[88] Βλ. *Αργ. Καρράς*, Ποινικό Δικονομικό Δίκαιο, εκδ. ε΄ 2017, ερμηνεία αρ. 149.

[89] Βλ. για την καλύτερη κατανόηση του σημείου αυτού, δίδεται ως παράδειγμα περίπτωση κατά την οποία η σύλληψη του κατηγορουμένου φέρεται κατά την σχετική έκθεση λ.χ. την 2-4-2020 και ώρα 19:20, ενώ η λήψη απολογίας (όχι ανωμοτί κατάθεσης) του φέρεται την 2-4-2020 και ώρα 17:10, δηλαδή σχήμα πρωθύστερο. Σφάλμα στην καταγραφή διορθώσιμο; Ή μήπως ακυρότητα ή και πλαστότητα της έκθεσης (αρ. 152 Κ.Ποιν.Δ.). Δεν νομίζω ότι η απάντηση είναι ιδιαίτερα εύκολη.

συγκεκριμένος μάρτυρας σε ημέρα και ώρα που καταγράφεται στην έκθεση και η αποδεικτική ισχύς της καλύπτει αυτό το γεγονός. Για τα όσα όμως ενήργησε ή κατέθεσε ο μάρτυρας ενώπιον του ανακριτικού υπαλλήλου, χωρεί ανταπόδειξη. Αναφορικά όμως με τα βεβαιωθέντα από τον ανακριτικό υπάλληλο που τη συντάσσει και σχετικά λ.χ. με τη βεβαίωση γεγονότος διενέργειας αυτοψίας, κατάσχεσης κλπ, δεν χωρεί ανταπόδειξη[90] παρά μόνο προσβολή για πλαστότητα, όπως προαναφέρθηκε.

Τελευταία αλλά εξ ίσου σημαντική σε σχέση με τα όσα αναφέρθηκαν ανωτέρω σχετικά με την έκθεση και τον ρόλο της στην ποινική διαδικασία, έρχεται η ερευνητική πρόκληση σχετικά με την απάντηση στο ερώτημα που τίθεται αναφορικά με το εάν και κατά πόσο είναι δυνατή η ένταξη στα άρθρα 148 επ. του Κ.Ποιν.Δ. μιας *ψηφιακής εκδοχής* της έκθεσης. Όπως θα δούμε παρακάτω, μέσα στο τεχνικό οπλοστάσιο του πραγματογνώμονα που επιχειρεί σε έναν χώρο για την αναγνώριση πειστηρίων και την συλλογή αποδεικτικού υλικού, υπάρχει πάντοτε μια μηχανή ψηφιακής απεικόνισης[91]. Το ζήτημα θα μας απασχολήσει στο ειδικότερο κεφάλαιο σχετικά με την *ειδική έκθεση* αναφορικά με τα ψηφιακά πειστήρια και στο σημείο εκείνο θα γίνει η περιγραφή της ειδικότερης προβληματικής και η αναφορά της λειτουργικής ανάγκης που καλείται (και κυρίως δύναται) να καλύψει τεχνικά αυτή η πρόταση για ψηφιακή απόδοση (καταγραφή) του ερευνητικού σταδίου.

iv. Ανακριτική Διαδικασία και τα ψηφιακά πειστήρια ως στοιχείο απόδειξης στην ποινική δίκη.

Η αναφορά σε ψηφιακά πειστήρια, όταν κινούμαστε στον χώρο της ανακριτικής έρευνας σχετικά με την εξιχνίαση εγκληματικής δράσης, είναι ταυτόσημη με το ζήτημα της απόδειξης. Μια παράμετρος της ποινικής δίκης με σημαντικό βάρος, που συνδέεται με τον ιδιαίτερα διαδεδομένο (στα σχετικά δικόγραφα) αναιρετικό λόγο της ειδικής κι εμπεριστατωμένης αιτιολογίας σε συμμόρφωση του δικαστή με την δεσμευτική επιταγή του άρθρου 94 Συντ όσο και με το σημαντικό και άξιο προσοχής στοιχείο της αιτιολόγησης των διατάξεων εισαγγελέα και δικαστή κατά το άρθρο 139 Κ.Ποιν.Δ.

[90] Βλ. *Μ. Γεωργιάδου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, τομ. Α, Νομική Βιβλιοθήκη 2018, σελ. 904 επ., *Αθ. Κονταξής*, Κώδικας Ποινικής Δικονομίας, Συνδυασμός θεωρίας και πράξης, α΄ τομ., Δ΄ εκδ., 2006, σελ. 1083.

[91] Βλ. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, «Electronic Crime Scene Investigation, A Guide for First Responders, Chapter 2. Investigative tools and equipment, Second Edition», σελ. 13 επ.

Η έννοια της απόδειξης στην ποινική δίκη κατέχει εξέχουσα θέση, τούτο είναι και λογικό και συνεπές προς όλο το πνεύμα του Κ.Ποιν.Δ., το οποίο έχει ως κεντρικό άξονα το τεκμήριο αθωότητας του κατηγορουμένου, επιβάλλοντας την απόδειξη της κατηγορίας και όχι της αθωότητας του κατηγορουμένου. Η διάταξη του άρθρου 265 στην δομή του ισχύοντος Κ.Ποιν.Δ. ήρθε να καλύψει λογικές ανάγκες και συμβατικές όσο και θεσμικές δεσμεύσεις και υποχρεώσεις της χώρας[92], που θα μας απασχολήσουν σε ειδικότερη αναφορά στην κατάλληλη θέση και αφορούν στην θεσμική κατοχύρωση της χρησιμοποίησης των ψηφιακών πειστηρίων στην ποινική δίκη. Με την διάταξη αυτήν δόθηκε λύση σε ζητήματα ψηφιακών αποδείξεων, των οποίων η δικονομική διαχείριση, δεν μπορούσε να καλυφθεί από τις υπάρχουσες δομές της (παραδοσιακής) κατάσχεσης πειστηρίων, η οποία ενδεχόμενα μπορούσε να καλύψει τους υλικούς φορείς αλλά όχι τα σχετικά δεδομένα, από το οποία εκπορευόταν ουσιαστικά και η απόδειξη του ενδιαφέροντος γεγονότος.

Μάλιστα για την απόδειξη στην βάση στοιχείων των νέων τεχνολογικών πληροφορικής κι επικοινωνιών, διατυπώθηκε και η άποψη ότι θα έπρεπε να αποτελέσουν χωριστό κεφάλαιο[93] στον τομέα των αποδείξεων στον Κ.Ποιν.Δ. και αυτό περισσότερο για την διασφάλιση των δικαιωμάτων του κατηγορουμένου, καθόσον ήδη η γενική ρήτρα του άρθρου 178 § 1 (αλλά και 177 § 1) Κ.Ποιν.Δ. επιτρέπει στον Δικαστή την αναζήτηση απόδειξης οπουδήποτε, τηρουμένων των νομίμων διαδικασιών και προϋποθέσεων παραδεκτού αναφορικά με την προέλευση και την συλλογή της απόδειξης.

Προηγήθηκε η αναφορά στην σημερινή τεχνοκρατούμενη πραγματικότητα, στην οποία καλείται πλέον να κινηθεί η ανακριτική πράξη μέσα σε ένα ψηφιακό περιβάλλον, όπου συναντούμε νέες εγκληματικές συμπεριφορές, σχετιζόμενες αποκλειστικά με το διαδίκτυο και της υπολογιστικές μηχανές. Ένα περιβάλλον όπου ακόμη και παραδοσιακές μορφές εγκληματικής δράσης, όπως η απάτη, η πλαστογραφία, η δυσφήμιση έχουν αναβαθμιστεί πρακτικά με εκφάνσεις ψηφιακής εκδοχής τέλεσής τους.

Στα νέα αυτά δεδομένα ανταποκρινόμενος ο ποινικός νόμος δεν μπορούσε να αφήσει αναξιοποίητη την πληροφορία από τα ψηφιακά πειστήρια και τα εξ αυτών προερχόμενα δεδομένα. Παρουσιάζονται υπό τον υπέρτιτλο «Επισκόπηση Δικαστικής Εφαρμογής και

[92] Βλ. *Θ. Δαλακούρας*, Ο νέος Κώδικας Ποινικής Δικονομίας, συνοπτική ερμηνεία κατ' άρθρο του Ν 4620/2019 (με ενημέρωση μέχρι το Ν4640/2019), 2019, Νομική Βιβλιοθήκη, σελ. 209.
[93] Βλ. *Αλ. Καργόπουλος*, Ανακριτικές πράξεις επί ψηφιακών δεδομένων: Δικαιικοί άξονες και προβληματισμοί, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 203.

Αποδεικτικής Χρήσης των Ψηφιακών Δεδομένων»[94] περιπτώσεις κατά τις οποίες την αδυναμία σύνδεσης των γεγονότων μεταξύ τους, την αδυναμία σύνδεσης δράσης του υπόπτου και εγκληματικού αποτελέσματος ή της αποκάλυψης της ταυτότητας του δράστη τους, τις ανατρέπει η σύγχρονη ψηφιακή εγκληματολογία, με παγκοσμίως αναγνωρισμένες τεχνικές μεθόδους, με μεθοδολογία και δεσμευτικά πρωτόκολλα ενεργειών αξιοποιώντας στο έπακρο τις τεχνολογίες αιχμής στον τομέα της πληροφορικής και των επικοινωνιών.

Αναδεικνύεται συνεπώς ιδιαίτερα σημαντική η ανακριτική αξιοποίηση των ψηφιακών πειστηρίων, σε μέτρο τέτοιο που πραγματικά να αναρωτιέται κανείς εάν είναι νοητή σήμερα οποιαδήποτε τέλεση σοβαρού πλημμελήματος ή κακουργήματος χωρίς να αφήσει ένα ψηφιακό ίχνος, ακόμη και αν αυτό έχει να κάνει με μια απλή διαδικτυακή αναζήτηση ή με την χρήση τεχνολογιών ηλεκτρονικών επικοινωνιών, ή με την επίκληση από μέρους των διαδίκων, που εμπλέκονται στην υπόθεση, κάποιου ψηφιακού δεδομένου ή έστω ενός ίχνους γεωεντοπισμού. Γίνεται αντιληπτό ότι στην αναγκαιότητα άντλησης πληροφορίας και χρησιμοποίησής της μέσα από τα ψηφιακά δεδομένα αναφερόμαστε ακόμη και για αποδεικτικά στοιχεία, τα οποία λειτουργούν στο περιβάλλον της εγκληματικής δράσης και επιτρέπουν την σύνδεσή του είτε με άλλα δεδομένα είτε με στοιχεία που ενισχύουν ή καταρρίπτουν ισχυρισμούς των εμπλεκομένων διαδίκων ή ακόμη επιβεβαιώνουν ή διαψεύδουν τις βασικές θέσεις επί των πραγματικών περιστατικών της αρχής που επίσταται των διαδικασιών της δίωξης.

Οι αποδεικτικές ανάγκες αυτές, οι οποίες είναι συνυφασμένες και με τις αντίστοιχες απαιτήσεις για ασφάλεια στην κοινότητα επιτάσσουν την αξιοποίηση πληροφοριών από τα ψηφιακά πειστήρια και την αξιολόγηση των δεδομένων που πηγάζουν από αυτά. Ο κανόνας δε που θέλει τα εξαγόμενα αποτελέσματα να είναι και ασφαλή, επιτρέπουν την αποτελεσματικότερη υποστήριξη ισχυρισμών, παρέχουν ασφαλέστερο ως προς την αποδεικτική ισχύ αποτέλεσμα, κάτι που με την σειρά του άγει σε ισχυρά αιτιολογημένη δικαστική κρίση, στοιχείο ιδιαίτερα σημαντικό στην αναζήτηση κρίσεων στο περιβάλλον του ποινικού δικαίου.

Οι προαναφερόμενες σκέψεις ισχύουν πολύ περισσότερο, για να μην πούμε σε απόλυτο βαθμό, στις περιπτώσεις έρευνας ενός κυβερνοεγκλήματος, το οποίο παράγεται και υφίσταται μόνο στον ψηφιακό κόσμο και στον κόσμο της δικτύωσης και των ηλεκτρονικών

[94] Βλ. κατωτέρω υπό αρ. 5. Επισκόπηση Δικαστικής Εφαρμογής και Αποδεικτικής Χρήσης των Ψηφιακών Δεδομένων, σελ. 53 επ.

επικοινωνιών[95]. Η παραδοσιακή μορφή απόδειξης στα εγκλήματα αυτά χωρίς την αξιοποίηση των ψηφιακών δεδομένων δεν έχει να προσφέρει καμιά ουσιαστική βοήθεια. Μόνη η απόδειξη λ.χ. από υλικό DNA του κατηγορουμένου στον χώρο όπου κινήθηκε το κυνερβοέγκλημα, μπορεί να ικανοποιεί (και αυτό με ερωτηματικό) τις απαιτήσεις της ποινικής δίωξης στο στάδιο της προδικασίας και μάλλον μέχρι το σημείο εκείνο που συντηρεί τη νομιμοποιητική βάση για την διεξαγωγή των ερευνών, αλλά σε καμιά περίπτωση δεν αποτελεί από μόνο του, ικανό στοιχείο για την προσαγωγή σε δίκη του κατηγορουμένου, πολύ δε περισσότερο στην καταδίκη του.

Τουλάχιστον για τα εγκλήματα στο διαδίκτυο και στα εγκλήματα σχετικά με τα πληροφοριακά συστήματα και τα ψηφιακά δεδομένα, η αποδεικτική παρουσία των ψηφιακών πειστηρίων πρέπει να θεωρείται δεδομένη. Διαφορετική προσέγγιση για την εξιχνίασή τους λογικά είναι αδύνατη[96]. Χωρίς βέβαια αυτό το τελευταίο να μειώνει την αποδεικτική τους συνδρομή στον ανακριτή αξιόποινης πράξης όταν η έρευνα αφορά σε κοινό (παραδοσιακό) έγκλημα.

Αυτά τα (νέα) δεδομένα φυσικά δεν προέκυψαν εσχάτως. Το ηλεκτρονικό έγκλημα στις βασικές μορφές του απασχολεί εδώ και έτη την επιστήμη[97] και την πρακτική σε όλες τους τις πτυχές, αναγκαστικά λοιπόν και στο ζήτημα των αποδεικτικών δυσχερειών, ιδίως αναφορικά με την σύνδεσή του με το πρόσωπο του εγκληματικού ηγήτορα.

Τα σημαντικά αυτά στοιχεία, βάρυναν στις σχετικές επιλογές σε διεθνές όσο και εθνικό νομοθετικό επίπεδο και έτσι σήμερα το άρθρο 265 Κ.Ποιν.Δ. καλύπτει το σχετικό κενό στο προηγούμενο ποινικό δικονομικό δίκαιο.

---

[95] Βλ. *Αλ. Καργόπουλος*, Ανακριτικές πράξεις επί ψηφιακών δεδομένων: Δικαιικοί άξονες και προβληματισμοί, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 201.

[96] Βλ. *Αλ. Καργόπουλος*, Ανακριτικές πράξεις επί ψηφιακών δεδομένων: Δικαιικοί άξονες και προβληματισμοί, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 201.

[97] Βλ. ενδεικτικά *Δ. Κιούπης*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 41 επ., *Γ. Μπουρμάς*, Η νομιμότητα των ερευνών σε ηλεκτρονικά δίκτυα και δεδομένα στις περιπτώσεις εγκλημάτων στον κυβερνοχώρο, ΠοινΔνη 2019, σελ. 557, *Ι. Αγγελή*, Διαδίκτυο και ποινικό δίκαιο, ΠοινΧρον 2000, σελ. 676, *Θ. Δαλακούρας*, Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν 4411/2016), ο.π., σελ. 5, *Β. Κάτος*, Ψηφιακά Πειστήρια, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 65 επ.

5. ΕΠΙΣΚΟΠΗΣΗ ΔΙΚΑΣΤΙΚΗΣ ΕΦΑΡΜΟΓΗΣ και ΑΠΟΔΕΙΚΤΙΚΗΣ ΑΞΙΟΠΟΙΗΣΗΣ ΤΩΝ ΨΗΦΙΑΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η παραδοσιακή εξιχνίαση των εγκληματικών πράξεων σταθερά έχει μεταβεί σε άλλο επίπεδο καθαρά τεχνολογικής δομής. Οι παλαιότερες χρησιμοποιούμενες τεχνικές, φαντάζουν πλέον ανίσχυρες (τουλάχιστον από απόψεως ακρίβειας), στις περισσότερες των περιπτώσεων, στην εξυπηρέτηση των σκοπών της ανακριτικής και σαφώς δεν εξυπηρετούν στα πλαίσια της αποδεικτικής αξιοποίησης των ευρημάτων, που σήμερα, αναζητούνται και εντοπίζονται στα ηλεκτρονική/ψηφιακή διάσταση. Πλέον, οι φερόμενοι εγκληματίες κατηγορούνται και καταδικάζονται για εγκλήματα εξαιτίας του εκπληκτικά ισχυρού και όλο και πιο ευέλικτου προσωπικού υπολογιστή και της τεχνολογίας της πληροφορικής. Η αστυνομία και οι ανακριτικές και εν γένει διωκτικές αρχές βρίσκουν όλο και περισσότερους τρόπους για να αποδείξουν εγκληματική δραστηριότητα απλά αναλύοντας το περιεχόμενο των ψηφιοποιημένων πληροφοριών, που ανακτώνται από τον υπολογιστή του κατηγορούμενου.

Την χρησιμότητα των νέων μεθόδων, πρακτικών και τεχνικών αναδεικνύει πιο δραστικά (με την έννοια της ευκολότερης αντίληψης του σημείου αναφοράς) μια αναδρομή σε εγκληματικές συμπεριφορές, που αποδόθηκαν αρχικά ως κατηγορία και τελικά καταλογίστηκαν στον δράστη τους μέσα από την χρησιμοποίηση της ψηφιακής έρευνας και των ψηφιακών πειστηρίων. Οι περιληπτικές αναφορές που παρατίθενται κατωτέρω αφορούν κυρίως την ανάδειξη της τεχνικής εξιχνίασης που μερικές φορές ήταν καθόλα συμπωματική, χωρίς να γίνεται εμβάθυνση των περιπτώσεων και των σχετικών αξιολογήσεων της μεθοδολογίας που ακολουθήθηκε στο σημείο αυτό.

Τρεις περιπτώσεις που θα αποτελέσουν την εισαγωγή στην θεματική αυτήν, περιγράφουν τη σημασία των ψηφιακών αποδεικτικών στοιχείων για τον χώρο της ποινικής δικαιοσύνης. μια περίπτωση παρουσιάζει ένα παράδειγμα για το πώς το ψηφιακό δεδομένο μπορεί να αποτελέσει κεντρικό στοιχείο για το κλείσιμο των υποθέσεων και τη δίωξη, μια άλλη περίπτωση δείχνει πώς τα σφάλματα στην λήψη των ψηφιακών δεδομένων και εν γένει αποδείξεων μπορούν να έχουν σοβαρές συνέπειες και η τρίτη περίπτωση υπογραμμίζει τις προκλήσεις για τη σύγχρονη έρευνα όταν τα ψηφιακά αποδεικτικά στοιχεία είναι περιορισμένα ή δεν υπάρχουν.

Η πρώτη περίπτωση αφορά την υπόθεση της Casey Anthony[98], που το 2008 κατηγορήθηκε για το θάνατο της τρίχρονης κόρης της Caylee Marie Anthony, της οποίας η εξαφάνιση δηλώθηκε με καθυστέρηση 31 ημερών. Το ενδιαφέρον θέμα, αναφορικά με το αντικείμενο της μελέτης, που ανέκυψε είχε να κάνει με το γεγονός ότι αρχικά το πόρισμα από τον έλεγχο του ηλεκτρονικού υπολογιστή της κατηγορουμένης, ανέδειξε 84 αναζητήσεις του όρου «χλωροφόρμιο» στην πλατφόρμα αναζήτησης της google, στοιχείο, το οποίο στήριξε την κατηγορία καθόσον το θύμα φέρεται να αναισθητοποιήθηκε με την προαναφερόμενη χημική ουσία και μετά ακολούθησε ο θάνατός του. Η αρχική στήριξη της κατηγορίας όμως στο στοιχείο αυτό κατέπεσε όταν ο πραγματογνώμονας με νέα έκθεσή του ανέφερε ότι το ψηφιακό υλικό *δεν ήταν ορθά εξασφαλισμένο* κατά την έρευνα και ότι επανάληψη της έρευνας ανέδειξε μόνο 1 αναζήτηση του όρου «χλωροφόρμιο» στην google και εκείνη αναφορικά με την χρήση της ουσίας το στον 19ο αιώνα[99] κάτι που μπορούσε να υποστηρίξει ισχυρισμό αναζήτησης από απλή περιέργεια.

Σε άλλη περίπτωση το 2012 εξαφανίστηκε ο Christian Aguilar, ενώ ο τελευταίος μάρτυρας που τον είδε ήταν ο φίλος του Pedro Bravo. Η σωρός του Aguilar βρέθηκε 60 μίλια δυτικά από το τελευταίο σημείο που τους είδαν μαζί (περιοχή της Florida). Το ενδιαφέρον εδώ στοιχείο αφορούσε το στοιχείο που χρησιμοποιήθηκε κατά του Pedro Bravo και αφορούσε πόρισμα από την εξέταση του *κινητού* του, και ειδικότερα στην προσωρινή μνήμη της εφαρμογής Facebook, όπου βρέθηκε ένα screenshot από την υποδομή siri του κινητού του περίπου την ώρα της βεβαιωμένης εξαφάνισης του θύματος, όπου υπήρχε η καταγραφή «*I need to hide my roommate*». Επειδή το κινητό του κατηγορουμένου δεν διέθετε την λειτουργία siri ενεργή, η σχετική αναζήτηση έγινε μέσω της εφαρμογής Facebook προκειμένου να έχει πρόσβαση στην εφαρμογή siri. Η ανάλυση των δεδομένων θέσης και κίνησης του κατηγορουμένου απέδειξαν ότι αυτός κινήθηκε επίσης μακριά και δυτικά την ίδια ώρα της εξαφάνισης του θύματος. Ο Pedro Bravo το 2014 καταδικάστηκε[100] για ανθρωποκτονία. Για την ιστορία, αιτία της εγκληματικής δράσης εξελήφθη η σύναψη σχέσης του θύματος με την πρώην φιλενάδα του δράστη.

---

[98] Βλ https://www.crimemuseum.org/crime-library/forensic-investigation/forensic-analysis-of-the-casey-anthony-trial/

[99] Βλ. Alvarez, Lizette (July 18, 2011). "Software Designer Reports Error in Anthony Trial". nytimes.com/. Retrieved, July 18, 2011. https://en.wikipedia.org/wiki/Death_of_Caylee_Anthony#Opening_statements_and_witness_testimony, *S. E. Goodison, R. C. Davis, and Br. A. Jackson*, Digital Evidence and the U.S. Criminal Justice System, Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

[100] Βλ. https://www.miamiherald.com/news/local/community/miami-dade/article1980000.html

Την σημασία της αξιοποίησης ψηφιακών πειστηρίων και των εξ αυτών δεδομένων, αναδεικνύει με τον καλύτερο τρόπο η περίπτωση της δολοφονίας του Philip Welsh το 2014 στο Meryland[101]. Ο θανών ήταν οδηγός ταξί και λάτρης της *αποχής* από την χρήση των νέων τεχνολογιών, δεν διέθετε κινητό τηλέφωνο ούτε είχε λογαριασμούς σε μέσα κοινωνικής δικτύωσης, ούτε διέθετε ηλεκτρονικό υπολογιστή. Παρόλα αυτά διέθετε το σπίτι του σε συναδέλφους του για να αναπαυθούν όταν αυτός εργαζόταν. Ο θάνατός του διαπιστώθηκε την επόμενη μέρα και αφού προηγήθηκε σχετική αναζήτηση επειδή δεν είχε παρουσιαστεί στην εργασία του. Μέχρι σήμερα η υπόθεση είναι ανεξιχνίαστη και η σχετική θέση των ανακριτικών υπαλλήλων είναι ότι αυτό οφείλεται στην *έλλειψη* ψηφιακών πειστηρίων[102].

Παραπέρα και προς ενίσχυση των ανωτέρω, παρατίθενται περιπτώσεις για την ενίσχυση της ερευνητικής πρόκλησης, μέσα από την σχετική καταγραφή υποθέσεων που απασχόλησαν την δικαιοσύνη αλλά και την εν γένει ειδησιογραφία[103]:

1. Ένας πρώην καθηγητής του κολλεγίου Marist, ο James Kent, καταδικάστηκε για την κατοχή παιδικής πορνογραφίας και για την προαγωγή ανηλίκου στην πορνεία. Στις 5 Απριλίου 2007, ο Kent παραπονέθηκε ότι ο υπολογιστής γραφείου του δεν λειτουργούσε κανονικά και έτσι τον απέστειλε στο τμήμα τεχνικό τμήμα του κολλεγίου για να τον σαρώσει για έναν ιό. Οι αρμόδιοι τεχνικοί αντί να βρουν έναν ιό, βρήκαν ένα φάκελο που περιλάμβανε μεγάλο αριθμό φωτογραφιών μικρής ηλικίας κοριτσιών, που συμμετείχαν σε διάφορες σεξουαλικές πράξεις. Το τμήμα απέστειλε τον υπολογιστή στην αστυνομία, ο οποίος συνέλαβε αμέσως τον Kent, ο οποίος τελικά διώχθηκε ποινικά και καταδικάστηκε σε τρία χρόνια φυλάκισης[104].

2. Ο Άγγλος κληρικός Dominic Stone *κατέβασε* ψηφιακά εκατοντάδες πορνογραφικές εικόνες παιδιών, όσο εργαζόταν ως εφημέριος. Ενώ αρχικά δεν καταδικάστηκε σε κάποια ποινή στερητική της ελευθερίας, ωστόσο άμεσα με την εξιχνίαση των πράξεών του, διατάχθηκε να εγγραφεί ως σεξουαλικός δράστης για 10 χρόνια και δεν του επετράπη να

---

[101] Βλ. *S. E. Goodison, R. C. Davis, and Br. A. Jackson*, Digital Evidence and the U.S. Criminal Justice System, Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

[102] Βλ. https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2flocal%2fcrime%2fphilip-welshs-simple-life-hampers-search-for-his-killer%2f2014%2f05%2f05%2f1fd20a52-cff7-11e3-a6b1-45c4dffb85a6_story.html, *C. Johnston*, A county's only unsolved murder has a victim without a digital footprint, https://arstechnica.com/tech-policy/2014/05/a-countys-only-unsolved-murder-has-a-victim-without-a-digital-footprint/

[103] Σημειώνεται ότι η κατωτέρω παράθεση αφορά στο επιστημονικό ερέθισμα και μόνο και η αποφυγή εμβάθυνσης στην κάθε περίπτωση έχει να κάνει αποκλειστικά και μόνο με τη νοηματική ενότητα και την οικονομία της ύλης

[104] Βλ. https://www.brainz.org/15-criminal-cases-solved-digital-evidence

εργάζεται στο ιερατείο για το υπόλοιπο της ζωής του. Ο Stone προσπάθησε να υποστηρίξει ότι κάποιος άλλος μπορεί να έχει χρησιμοποιήσει τον υπολογιστή του για να κατεβάσει τις εικόνες χωρίς να το γνωρίζει, αλλά το μόνο άλλο άτομο που είχε πρόσβαση στον υπολογιστή ήταν η σύζυγός του. Περαιτέρω αποδείχθηκε ότι κατά τη στιγμή των λήψεων των ψηφιακών αρχείων ελάμβανε χώρα η διακονία του. Την κατάρριψη των ισχυρισμών του ανέδειξε η ερευνητική πράξη καθόσον οι ερευνητές μπορούσαν να ελέγξουν όχι μόνο τα αρχεία στον υπολογιστή αλλά επίσης να βεβαιώσουν πότε προστέθηκαν ή έτυχαν επεξεργασίας τα αρχεία. Τελικά ο ιερέας δικάστηκε το Νοέμβριο του 2010 για τις πράξεις αυτές, που αφορούσαν αρχείο με 600 περίπου απεικονίσεις[105] και καταδικάστηκε σε 16 φορές ποινής εννέα μηνών φυλάκισης[106].

3. Ο James M. Cameron εργάστηκε ως ο κορυφαίος εισαγγελέας ναρκωτικών στο γραφείο του Γενικού Εισαγγελέα του Maine, όταν μια μέρα εμφανίστηκαν ομοσπονδιακοί πράκτορες στο σπίτι του με εντάλματα έρευνας για τους τέσσερις υπολογιστές μέσα. Η Yahoo είχε αναφέρει την εύρεση παιδική πορνογραφίας στις φωτογραφίες ενός κατόχου λογαριασμού που αργότερα θα αναγνωριζόταν ως σύζυγος του Cameron. Βρήκαν επίσης 17 προφίλ χρηστών στο Yahoo που έστειλαν και έλαβαν παιδική πορνογραφία, όλα αυτά προέρχονταν από τους υπολογιστές στο σπίτι του Cameron. Σημαντικές από την ειδησιογραφία αλλά και τη σχετική νομολογία είναι οι ενστάσεις (8 στον αριθμό) που προέβαλε ο κατηγορούμενος (εισαγγελέας) αναφορικά με την καθ' ύλη και κατά τόπο αρμοδιότητα του δικαστή που εξέδωσε το ένταλμα έρευνας καθώς και για το θεσμικό περιεχόμενο και τις εντολές έρευνας στην περίπτωσή του, ενστάσεις που απορρίφθηκαν στο σύνολό τους[107].

4. Ο Urbain Morelli ήθελε να εγκαταστήσει ένα σύστημα Internet υψηλής ταχύτητας στο σπίτι του. Όταν ήρθε ο τεχνικός, παρατήρησε ότι υπήρχε ένα τρίποδο και μια web cam που ήταν εστιασμένη στην τρίχρονη κόρη του Morelli και ότι υπήρχαν και φάκελοι στον υπολογιστή του Morelli με την ονομασία «Lolita Porn». Ωστόσο, ο τεχνικός επέστρεψε την επόμενη μέρα για να διαπιστώσει ότι η κάμερα είχε μετακινηθεί σε λιγότερο ενοχοποιητική θέση. Ο τεχνικός ανέφερε το περιστατικό και έλαβε ένταλμα έρευνας για την αναζήτηση στο σπίτι του Morelli. Όπως αναμενόταν, βρέθηκε παιδική πορνογραφία στον υπολογιστή.

[105] Βλ. BBC, Convicted Marchington child porn vicar quits, https://www.bbc.com/news/uk-england-stoke-staffordshire-11706195
[106] Βλ. lichfieldlive, Dominic Stone, Diocese of Lichfield reassures worshippers after vicar is sentenced over child porn, https://lichfieldlive.co.uk/tag/dominic-stone/
[107] Βλ. No. CR-09-24-B-W United States District Court, D. Maine U.S. v. Cameron 652 F. Supp. 2d 74 (D. Me. 2009) Decided Sep 1, 2009, https://casetext.com/case/us-v-cameron-3.

Ωστόσο, ο Morelli προσέφυγε ενώπιον του Καναδικού Ανώτατου Δικαστηρίου στην υπόθεση, υποστηρίζοντας ότι δεν υπήρχε επαρκής αιτία για το ένταλμα έρευνας. Το Ανώτατο Δικαστήριο του Καναδά[108] με εφαρμογή διατάξεων του Συντάγματος, έκανε δεκτή την ένσταση έλλειψης αιτιολογίας αναφορικά με τη συλλογή των ψηφιακών πειστηρίων.

5. Ο Vernor Gumila, 41 ετών, προπονητής σε εφηβικές ομάδες, συνελήφθη για κατοχή παιδικής πορνογραφίας αφού οι αρχές έλαβαν ένταλμα για την έρευνα στον υπολογιστή του συγκατοίκου του. Ενώ η αστυνομία βρισκόταν στο σπίτι, ρώτησαν αν μπορούσαν επίσης να ψάξουν και στον υπολογιστή του Gumila. Ο Gumila έδωσε τη συναίνεσή του και, αφού βρέθηκαν φωτογραφίες παιδικής πορνογραφίας στον υπολογιστή του, συνελήφθη. Δεν είναι σαφές εάν η Gumila συμφώνησε με εμπιστοσύνη, ελπίζοντας ότι απλά δεν θα βρουν κάτι ενοχοποιητικό στον υπολογιστή του ή αν το έκανε με δισταγμό στα πλαίσια του να μην κινήσει σε βάρος του υποψίες. Πιθανότατα δεν ήταν σίγουρος για το αν ήταν νόμιμο για τις αρχές να ψάξουν στον υπολογιστή του. Δεν κατανόησε την έννοια της συγκατάθεσής του. Ο δικαστής αποφάνθηκε ότι υπήρξαν αποδεικτικά στοιχεία σχετικά με τα cookies ιστότοπων για επισκέψεις και ενέργειές του στο Internet αλλά και στον σκληρό δίσκο του υπολογιστή της Gumila έδειξαν ότι διαμοίραζε - αντί να βλέπει μόνο εικόνες - παιδική πορνογραφία. Σύμφωνα με την κατηγορούσα αρχή, βρέθηκαν 53 cookies και τα cookies κατέγραψαν περισσότερες από 80 επισκέψεις σε διάφορους υπόπτους ιστότοπους. Μια λίστα αγαπημένων αναζητήσεών του στο Internet οδηγούσαν σε ιστότοπους που περιείχαν ονόματα όπως «Lolita», «Lola», «Lolly» και «preteen» σε συνδυασμό με όρους sex acts. Επίσης, κατά την δικαστική κρίση ο Gumila είχε τη δυνατότητα να ανακτήσει τις εικόνες από προσωρινούς φακέλους Internet, η οποία ήταν καθοριστική για τον νομικό ορισμό της κατοχής. Ο υπερασπιστικός ισχυρισμός του ήταν ότι η συγκέντρωση του υλικού στον υπολογιστή του έγινε εν αγνοία του[109]. Η καταδίκη του τελεσιδίκησε[110] μετά από έφεση που άσκησε κατά της πρωτόδικης καταδίκης του.

6. Η λήψη μέσων και αρχείων από το διαδίκτυο έγινε αναμφισβήτητα πιο δημοφιλής με την άφιξη του Napster[111], όπου θα μπορούσε κάποιος να κατεβάσει εντελώς δωρεάν μουσική από οποιονδήποτε συνδεόταν με την υπηρεσία που ήταν πρόθυμος να μοιραστεί.

[108] Βλ. Urbain P. Morelli Appellant v. Her Majesty The Queen Respondent, 2010 SCC 8 File No.: 32741, 2009: February 18; 2010: March 19, https://scc-csc.lexum.com/scc-csc/scc-csc/en/7847/1/document.do

[109] Βλ. Susan Sarkauskas, man found guilty of owning child porn, https://www.dhbusinessledger.com/article/20100903/news/309039887

[110] Βλ. THE PEOPLE OF THE STATE OF ILLINOIS, Plaintiff-Appellee, v. Vernor Gumila, Defendant-Appellant. District & No. Second District Docket No. 2-11-0761 Filed December 6, 2012, https://courts.illinois.gov/opinions/appellatecourt/2012/2nddistrict/2110761.pdf

[111] Βλ. https://gr.napster.com/

Άλλα προγράμματα peer2peer (p2p) ακολούθησαν σύντομα, όπως το LimeWire και το Share Bear. Ο Nathaniel Solon χρησιμοποίησε αυτό το δίκτυο P2P για να κατεβάσει παράνομα μουσική, βιντεοπαιχνίδια και, αργότερα, παιδική πορνογραφία. Η δράση του αποκαλύφθηκε από το Internet Crime Against Children Agency[112], το οποίο διαπίστωσε ότι όχι μόνο κατεβάζει τέτοια αρχεία, αλλά και τα διαμοιράζει. Μετά την καταδίκη του σε 72 μήνες φυλάκισης[113] και τον εγκλεισμό του σε κατάστημα κράτησης, υπήρξε θύμα πολλών ξυλοδαρμών και μεταφέρθηκε σε απομόνωση για την προστασία του. Η καταδίκη του τελεσιδίκησε[114] μετά από έφεση που άσκησε κατά της πρωτόδικης καταδίκης του. Σημαντικό στοιχείο από πλευράς ψηφιακών πειστηρίων είναι το γεγονός ότι ο κατηγορούμενος αιτιολόγησε την αρχική του ομολογία στο γεγονός ότι δεν είχε τα οικονομικά μέσα να καλύψει την σχετική δαπάνη για μίσθωση υπηρεσιών ειδικού εμπειρογνώμονα για τον έλεγχο των ψηφιακών πειστηρίων που χρησιμοποιήθηκαν στην δίκη. Ο Δικαστής του παρείχε τη δυνατότητα αυτήν με την χορήγηση πίστωσης ποσού 20.000,00 $.

7. Ο Lyndon Humbracht, αποφάσισε ότι η αποστολή γυμνών φωτογραφιών παιδιών ως συνημμένο ηλεκτρονικού ταχυδρομείου ήταν μια καλή ιδέα. Αυτό οδήγησε τις αρχές να επισκεφθούν το σπίτι του, όπου αναγνώρισε ότι διαθέτει παιδική πορνογραφία. Οι ειδικοί ανακριτικοί υπάλληλοι με τεχνικές γνώσεις ερεύνησαν τον υπολογιστή του και βρήκαν «πολυάριθμες» εικόνες παιδικής πορνογραφίας και ταινίες σε δίσκους CD[115].

8. Ενώ ένας ανησυχητικός αριθμός περιπτώσεων σε εγκλήματα διαδικτυακά σχετίζονται με την παιδική πορνογραφία, υπάρχουν και περιπτώσεις αξιοποίησης στοιχείων από τον υπολογιστή του δράστη για καταδίκη σε περιπτώσεις άλλων εγκλημάτων. Τέσσερα χρόνια μετά το θάνατο της συζύγου του, ο Matt Baker[116] καταδικάστηκε για δολοφονία και καταδικάστηκε σε 65 χρόνια φυλάκισης. Η σύζυγός του είχε αυτοκτονήσει λόγω

---

[112] Βλ. https://www.icactaskforce.org, Το Πρόγραμμα Δράσης για τα Εγκλήματα κατά των Παιδιών στο Διαδίκτυο (Internet Crimes Against Children Task Force Program (ICAC) βοηθά τους κρατικούς και τοπικούς φορείς επιβολής του νόμου να αναπτύξουν αποτελεσματική αντίδραση στη σεξουαλική εκμετάλλευση παιδιών με τη χρήση τεχνολογίας και τα εγκλήματα κατά των παιδιών στο Internet. Η υποστήριξη αυτή περιλαμβάνει τα συστατικά στοιχεία της εγκληματολογίας και της έρευνας, την κατάρτιση και την τεχνική βοήθεια, τις υπηρεσίες των θυμάτων, την πρόληψη και την εκπαίδευση στην κοινότητα. Σχετική η νομοθετική πράξη «PROTECT Our Children Act 2008".

[113] Βλ. United States v. Solon, 596 F.3d 1206 (10th Cir. 2010), https://www.leagle.com/decision/infco20100217056

[114] Βλ. United States Court of Appeals,Tenth Circuit. UNITED STATES of America, Plaintiff-Appellee, v. Nathaniel SOLON, Defendant-Appellant. No. 09-8018., https://caselaw.findlaw.com/us-10th-circuit/1508118.html

[115] Βλ. Illinois Attorney General, Kane County Man Sentenced On Child Pornography Conviction, https://illinoisattorneygeneral.gov/about/index.html

[116] Βλ. http://www.nbcnews.com/id/34983893/ns/us_news-crime_and_courts/t/murdering-minister-sentenced-years/#.XnurDIgzZPY

υπερβολικής δόσης από υπνωτικά χάπια και είχε αφήσει ακόμη και ένα σημείωμα αυτοκτονίας. Αργότερα αποκαλύφθηκε, μετά από ανάλυση του υπολογιστή του Baker, ότι είχε γράψει «υπερβολική δόση σε υπνωτικά χάπια» σε μηχανή αναζήτησης και είχε επισκεφθεί διάφορες φαρμακευτικές ιστοσελίδες πριν από το θάνατο της συζύγου του. Οι αρχές ερεύνησαν τον υπολογιστή του και διαπίστωσαν ότι είχε επίσης επισκεφθεί αρκετούς ιστότοπους πορνογραφίας φετίχ, οι οποίοι χρησίμευσαν για τον προσδιορισμό του χαρακτήρα του στο δικαστήριο.

9. Ένας πρώην κυβερνήτης του αντιτορπιλικού των USS Benfold, ο οποίος αποστρατεύθηκε από το Πολεμικό Ναυτικό των ΗΠΑ το 2002, ο Χασάν Αμπού-Τζιχαάν, καταδικάστηκε σε 10 χρόνια φυλάκισης για διαρροή λεπτομερειών σχετικά με τις κινήσεις του αντιτορπιλικού σε έναν διαχειριστή ιστότοπου με έδρα το Λονδίνο που υποστήριζε επιθέσεις εναντίον Αμερικανών. Το 1997, ο Abu-Jihaad άλλαξε το όνομά του από τον Paul Raphael Hall σε Hassan Abu-Jihaad, ο οποίος μεταφράζεται σε Hassan «*Πατέρας της Τζιχάντ*». Η διαρροή δεν έγινε γνωστή μέχρι που ο Abu-Jihaad εγκατέλειψε το Πολεμικό Ναυτικό όταν μια έρευνα για τις εκδόσεις Azzam οδήγησε στην αναζήτηση ενός διαμερίσματος στο Λονδίνο, που συνδέεται με έναν από τους διοργανωτές της ιστοσελίδας και οι αρχές βρήκαν μια δισκέτα που περιέχει πληροφορίες του αμερικανικού ναυτικού[117]. Κατά της καταδίκης του και της ποινής του σε φυλάκιση δέκα ετών, άσκησε έφεση, αλλά η καταδίκη επικυρώθηκε από Τριμελή Επιτροπή, αφού διαπιστώθηκε ότι ο νόμος περί επιτήρησης της αλλοδαπής πληροφόρησης ήταν συνταγματικός και χρησιμοποιήθηκε σωστά για την απόκτηση των απαραίτητων αποδεικτικών στοιχείων για την καταδίκη[118].

10. Μερικές φορές ένας εγκληματίας μπορεί να χρησιμοποιήσει τον υπολογιστή του με έναν τρόπο που φαντάζει ύποπτος και αυτή η χρήση από μόνη της μπορεί να οδηγήσει σε καταδίκη. Σε ορισμένες περιπτώσεις, ο υπολογιστής μπορεί να οδηγήσει την αστυνομία σε σημαντικά αποδεικτικά στοιχεία. Αυτή είναι η περίπτωση του Krenar Lusha[119] του Ηνωμένου Βασιλείου. Ανακαλύφθηκε μετά από αναζήτηση στο φορητό υπολογιστή του ότι είχε κατεβάσει εκτεταμένες οδηγίες για την κατασκευή εκρηκτικών και αυτοκτονικών ζωνών. Αυτό οδήγησε τους αξιωματικούς να τον συλλάβουν και αφού έψαξαν το διαμέρισμά του, βρήκαν 71,8 λίτρα βενζίνης, νιτρικού καλίου και φυσιγγίων κυνηγετικών όπλων, μαζί με

[117] Βλ. District of Connecticut, U.S. V. Hassan Abu-Jihaad, 3:07CR57 (MRK) (District of Connecticut), https://www.justice.gov/usao-ct/us-v-hassan-abu-jihaad
[118] Βλ. https://en.wikipedia.org/wiki/Hassan_Abujihaad
[119] Βλ. The Telegraph, Albanian "terrorist" caught with bomb-making materials in his home, court hears https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/6591313/Albanian-terrorist-caught-with-bomb-making-materials-in-his-home-court-hears.html

4300 GB μνήμης που περιλάμβανε οδηγίες για τη χρήση των διαφόρων συστατικών κατασκευής βόμβων. Επίσης, λειτούργησαν ενοχοποιητικά για τον Lusha συνομιλίες του στο εξωτερικό (μέσω του MSN) όπου περιέγραφε τον εαυτό του ως τρομοκράτη, ότι ήταν καλός ελεύθερος σκοπευτής και ότι του άρεσε να σκοτώνει τους Εβραίους και τους Αμερικανούς. Αυτές οι συνομιλίες ανακτήθηκαν από τον υπολογιστή του. Η άντληση στοιχείων από την ψηφιακή έρευνα στήριξε όλη την δίωξη εναντίον του συγκεκριμένου κατηγορουμένου[120].

11. Ο νεαρότερος τρομοκράτης στο Ηνωμένο Βασίλειο που καταδικάστηκε για τρομοκρατία, ο Hammaad Munsi συνελήφθη μετά την επιστροφή του από ταξίδι στο Πακιστάν[121]. Η αστυνομία κατέσχεσε τις αποσκευές του και βρήκε ένα φορητό υπολογιστή μέσα στο οποίο περιείχε μια «εγκυκλοπαίδεια τρομοκρατικής διδασκαλίας», με πολλές πληροφορίες μεταξύ των οποίων ήταν λεπτομέρειες για το πώς να φτιαχτεί ένα πυροβόλο όπλο. Ο Hammaad Munsi επίσης έφερε σφαιρικά ρουλεμάν κατά τη στιγμή της σύλληψης, όπλο επιλογής για βομβιστές αυτοκτονίας. Αν και ήταν πολύ νέος, ήταν ενεργό μέλος μιας τρομοκρατικής οργάνωσης και όντας συχνός χρήστης του διαδικτύου, ήταν υπεύθυνος μιας ιστοσελίδας που δημοσίευε υλικό σχετικό με την τρομοκρατία[122]. Στην εποχή του υπολογιστή, δεν αποτελεί έκπληξη το γεγονός ότι κάποιος τόσο νέος μπορεί να εμπλακεί σε εγκλήματα που αποδεικνύονται από ψηφιακά πειστήρια.

12. Ένας μεγάλος σχεδιασμός τρομοκρατικού χτυπήματος σταμάτησε στην περίπτωση του Dihren Barot[123] το 2006, ο οποίος πρότεινε σειρά συντονισμένων επιθέσεων στο Ηνωμένο Βασίλειο. Το σχέδιο περιελάμβανε την έκρηξη μιας «dirty bomb»[124], επίθεση σε ένα τρένο και την τοποθέτηση επί τριών οχημάτων κυλίνδρων αερίου[125] και εκρηκτικών υλών πριν την τοποθέτησή τους σε πολυσύχναστους χώρους. Ήταν σε μεγάλο βαθμό η άντληση δεδομένων από τους υπολογιστές που χρησιμοποίησε ο Barot και οι συνεργάτες

[120] Βλ. https://www.inboundwriter.com/technology/computer-forensics-is-the-answer-to-digital-crimes/

[121] Βλ. The Gurdian, https://www.theguardian.com/world/2015/apr/07/brother-of-hassan-munshi-uk-youngest-convicted-terrorist-feared-joined-isis

[122] Βλ. BBCNews Computer terror teenager jailed, http://news.bbc.co.uk/2/hi/uk_news/england/london/7625041.stm

[123] Βλ. https://www.globalsecurity.org/security/profiles/dhiren_barot.htm, the Guardian, Man gets life sentence for terror plot, https://www.theguardian.com/world/2006/nov/07/terrorism.uk

[124] Βλ. Η «βρώμικη βόμβα» είναι ραδιενεργό όπλο που συνδυάζει ραδιενεργό υλικό με συμβατικά εκρηκτικά. Ο σκοπός του όπλου είναι να μολύνει την περιοχή γύρω από αμάχους. Δεν πρέπει να συγχέεται με την ατομική βόμβα και τα πυρηνικά όπλα. https://www.health.ny.gov/environmental/emergency/dirty_bombs.htm

[125] Βλ. Ένας «κύλινδρος αερίου» είναι ένα δοχείο πίεσης για αποθήκευση και συγκράτηση αερίων σε υψηλότερη ατμοσφαιρική πίεση. Οι φιάλες αερίου υψηλής πίεσης ονομάζονται επίσης φιάλες. Μέσα στον κύλινδρο, τα αποθηκευμένα περιεχόμενα μπορεί να βρίσκονται σε κατάσταση συμπιεσμένου αερίου, ατμού πάνω σε υγρό, υπερκρίσιμο υγρό ή διαλυμένα σε υλικό υποστρώματος, ανάλογα με τα φυσικά χαρακτηριστικά των περιεχομένων. Ένας τυπικός σχεδιασμός κυλίνδρου αερίου είναι επιμήκης, στέκεται όρθιος σε ένα πεπλατυσμένο άκρο πυθμένα, με τη βαλβίδα και προσαρμόζεται στην κορυφή για σύνδεση με τη συσκευή λήψης. https://www.sciencedirect.com/topics/engineering/gas-cylinder

του, που οδήγησαν στην καταδίκη τους, χρησιμοποιώντας στοιχεία από τα ψηφιακά πειστήρια. Συνολικά, κατασχέθηκαν και αναλύθηκαν πάνω από 300 υπολογιστές και χρησιμοποιώντας τα δεδομένα από αυτούς τους υπολογιστές σώθηκαν εκατοντάδες (αν όχι χιλιάδες) ζωές.

13. Περισσότερες από 250 δημοσιεύσεις στο Facebook αναφέρονται ως πηγή ψηφιακών πληροφοριών, που συγκεντρώθηκαν κατά τη διάρκεια εγκληματολογικών ερευνών στο δευτεροβάθμιο δικαστήριο της Ιντιάνα. Μια από τις καταγεγραμμένες περιπτώσεις μιλά για τον Larry Jo Thomas, ο οποίος παρουσιαζόταν εικονικά με το όνομα «Slaughtaboi Larro» στο Facebook. Δημοσίευσε μια φωτογραφία στον τοίχο του Facebook με ένα τουφέκι επίθεσης AR-15. Όταν έλαβε χώρα η έρευνα σχετικά με τη δολοφονία του Rito Llamas-Jaurez, ο Larry κατηγορήθηκε και τελικά κρίθηκε ένοχος τελεσίδικα[126], καθώς ο Llamas-Jaurez πυροβολήθηκε με πυρομαχικά τύπου AR-15. Οι ανακριτές βρήκαν επίσης ένα βραχιόλι κοντά στον τόπο του εγκλήματος, που ταίριαζε με εκείνο που φορούσε ο Larry Jo Thomas σε μία από τις φωτογραφίες στο Facebook.

14. Μια φοιτήτρια του πανεπιστημίου της Μάντσεστερ, η Mikayla Munn, το Μάρτιο του 2016 γέννησε στην μπανιέρα της, στο δωμάτιο του κοιτώνα της[127]. Αμέσως μετά τον τοκετό, έπνιξε το νεογέννητο αγοράκι της στη μπανιέρα, αλλά «αιτιολόγησε» την αξιόποινη πράξη της, δηλώνοντας ότι δεν γνώριζε την εγκυμοσύνη της και ότι οι πόνοι της γέννας ήταν αισθητοί όταν λούστηκε, ακολουθούμενοι από τον τοκετό. Κατά την διερεύνηση των ψηφιακών στοιχείων της, οι ερευνητές διαπίστωσαν ότι είχε πραγματοποιήσει αναζήτηση στη Google για «αμβλώσεις σε οικιακό περιβάλλον» και «τρόπους για την τομή του ομφάλιου λώρου ενός μωρού». Η Munn αποδέχθηκε τις κατηγορίες κηρύχθηκε ένοχη για παραμέληση σε ποινή φυλάκισης 12 ετών[128] και φυλακίστηκε για 9 έτη.

15. Ο Ross Compton από το Middletown του Οχάιο, καταδικάστηκε για λόγους επιβαρυντικής εμπρηστικής και ασφαλιστικής απάτης στο σπίτι του Court Donegal το 2016. Το περιστατικό του κόστισε 400.000 δολάρια σε ζημιά. Όταν ο Ross υπέβαλε πλαστά ιατρικά πιστοποιητικά που περιγράφουν την καρδιακή του ασθένεια, τα δεδομένα από τον βηματοδότη του χρησίμευσαν ως αποδεικτικά στοιχεία ενώπιον του δικαστηρίου. Τα

[126] Βλ. COURT OF APPEALS OF INDIANA, Larry J. Thomas, Appellant-Defendant v. State of Indiana, Appellee-Plaintiff, Court of Appeals Case No. 18A-CR-1714 Appeal from the Marion Superior Court, The Honorable Lisa F. Borges, Judge - Trial Court Cause No. 49G04-1603-MR-9636, https://www.in.gov/judiciary/opinions/pdf/03271902pdm.pdf.

[127] Βλ. https://www.indystar.com/story/news/crime/2018/07/25/mikayla-munn-sentenced-death-her-new-born-baby-dorm-manchester-university/832684002/

[128] Βλ. https://www.theindianalawyer.com/articles/47670-woman-gets-prison-in-death-of-baby-delivered-in-bathtub

δεδομένα που συλλέχθηκαν από το βηματοδότη περιλάμβαναν τον καρδιακό του ρυθμό, τη ζήτηση από τον ρυθμό και τους καρδιακούς ρυθμούς που βοήθησαν στην απόδειξη της παραποίησης στοιχείων και της ασφαλιστικής απάτης. Το Δικαστήριο απασχόλησε και η νομιμότητα ή μη της ψηφιακής έρευνας, από πλευράς ευαίσθητων προσωπικών δεδομένων που αφορούν στην υγεία σε συνδυασμό με τις συνταγματικές διατάξεις για την ελευθερία και την προστασία της προσωπικότητας. Η τελική κρίση ήταν υπέρ της παραδοχής της νομιμότητας αναφορικά με τη λήψη των δεδομένων[129].

16. Μετά τη ρωσική προσάρτηση της Κριμαίας τον Φεβρουάριο του 2014, οι διεθνείς εντάσεις εστίασαν σε ισχυρισμούς ότι τα ρωσικά στρατεύματα επιχειρούσαν σε άλλα μέρη της Ουκρανίας. Ρώσοι αξιωματούχοι επανειλημμένα αρνήθηκαν αυτούς τους ισχυρισμούς. Ξεκινώντας από τα τέλη Ιουνίου του 2014, ο Alexander Sotkin[130], λοχίας του Ρωσικού στρατού, δημοσίευσε μια μηνιαία διαδρομή selfies που λαμβάνονται από το κινητό του τηλέφωνο στον λογαριασμό του στο Instagram. Ο Τύπος επέλεξε την ιστορία όταν ανακαλύφθηκε ότι τα αρχεία jpeg που δημοσιεύθηκαν περιελάμβαναν γεωγραφικά μεταδεδομένα και ότι οι γεωγραφικές εικόνες και οι εικόνες έδειξαν ότι ο λοχίας μετακινήθηκε, ενόσω βρισκόταν σε ενεργή υπηρεσία, από στρατιωτική βάση στη Ρωσία στην ανατολική Ουκρανία και στη συνέχεια επέστρεψε στη βάση του.

Συμπερασματικά προκύπτει ότι τα γεωγραφικά μεταδεδομένα, όπως αυτά που είναι ενσωματωμένα στις εικόνες του Sotkin, είναι μια μορφή μεταδεδομένων εντοπισμού. Οι γεωγραφικές λέξεις που δημιουργούνται από τα smartphones τείνουν να είναι πολύ ακριβείς και σχετίζονται με άλλους τύπους μεταδεδομένων αρχείων, όπως ημερομηνίες και χρονικά σήματα. Ο συνδυασμός των ανωτέρω και αναφορές που δείχνουν ότι οι χρήστες smartphone παίρνουν πάνω από 150 εικόνες ανά μήνα δίνουν μια σημαντική ποσότητα πληροφορίας που επιτρέπουν την άντληση απαντήσεων σε ερωτήματα του τύπου ποιοι; Τί; Πότε; Αλλά και λεπτομέρειες κατά τη διάρκεια μιας έρευνας. Γεωγραφικά μεταδεδομένα και άλλοι τύποι δεδομένων τοποθεσίας μπορούν επίσης να ενσωματωθούν σε άλλους τύπους αρχείων, όπως αρχεία βίντεο και μηνύματα SMS. Άλλα δεδομένα τοποθεσίας κινητού τηλεφώνου μπορούν να αντληθούν από τις διαδρομές που αποθηκεύονται σε εφαρμογές χαρτογράφησης, συνδέσεις Wi-Fi, πύργους κυψελών στο ιστορικό κλήσεων και εφαρμογές.

[129] Βλ. https://www.journal-news.com/news/crime--law/using-pacemaker-data-stealing-personal-information-judge-middletown-arson-case-says/BAGH5WM0iCxOTwTPfM3P7J/

[130] Βλ. https://www.theguardian.com/commentisfree/2014/aug/01/russian-soldier-alexander-sotkin-instagram-ukraine-selfies

17. Η Connie Dabate[131] δολοφονήθηκε στο σπίτι της το 2015. Σύμφωνα με το ένταλμα σύλληψής του, ο σύζυγός της Richard έδωσε αντιφατική και μη πειστική εξήγηση των γεγονότων της ημέρας, ισχυριζόμενος ότι επέστρεψε στο σπίτι μετά από ειδοποίηση συναγερμού και πως όταν μπήκε στο σπίτι του, ακινητοποιήθηκε και βασανίστηκε από έναν εισβολέα. Είπε στην αστυνομία ότι ο εισβολέας πυροβόλησε στη συνέχεια και σκότωσε τη Connie όταν επέστρεψε στο σπίτι από το γυμναστήριο. Στηριζόμενη σε αποδεικτικά στοιχεία που συλλέχθηκαν από το Fitbit[132] της Connie, η αστυνομία μπόρεσε να αποδείξει ότι ήταν στο σπίτι την ώρα που ο Richard δήλωσε ότι ήταν στο γυμναστήριο. Σύμφωνα με τα στοιχεία του Fitbit, η Connie σταμάτησε να κινείται ένα λεπτό πριν από την λήξη του συναγερμού.

Πορισματικά προκύπτει ότι φορητές συσκευές όπως το Fitbits παρακολουθούν την τοποθεσία κίνησης του κατόχου μέσω GPS και δραστηριότητες όπως η απόσταση που διανύθηκε, τα βήματα που ελήφθησαν, ο χρόνος ύπνου και ο καρδιακός ρυθμός. Οι συσκευές έχουν ρυθμιστεί ώστε να συγχρονίζουν δεδομένα σε εφαρμογές σε smartphones και προσωπικούς υπολογιστές ή σε νέους ιστότοπους σύννεφων ή κοινωνικών μέσων. Η συλλογή αποδείξεων μπορεί να γίνει από οποιαδήποτε από αυτές τις πηγές χρησιμοποιώντας τυποποιημένα εργαλεία και τεχνικές ψηφιακής πραγματογνωμοσύνης.

18. Η περίπτωση του Howze v. Western Express, Inc.[133] περιστράφηκε γύρω από τους τραυματισμούς που προκλήθηκαν όταν ένας ελκυστήρας-ρυμουλκούμενο ανάγκασε μια μοτοσυκλέτα να εκτραπεί από το δρόμο. Το εν λόγω όχημα δεν μπορούσε να προσδιοριστεί οριστικά από μάρτυρα, παρόλο που ο μάρτυρας υπενθύμισε ότι το λογότυπο του ρυμουλκούμενου έγραφε «Western Express». Τα φορτηγά του εναγόμενου («Western Express») ήταν εξοπλισμένα με ιχνηλάτες ώστε να είναι ευχερής ο έλεγχος της κίνησης των οχημάτων της εταιρίας ως περιουσιακών στοιχείων της. Κατά τη συνήθη πρακτική της εταιρίας, τα δεδομένα από τους ιχνηλάτες συλλέγονταν και διατηρούνταν σε μια κεντρική βάση δεδομένων. Ο εναγόμενος ισχυρίστηκε ότι η αναζήτηση της βάσης δεδομένων απεδείκνυε ότι δεν είχε φορτηγά στον εν λόγω δρόμο τη νύχτα του ατυχήματος. Για να αντιμετωπίσει αυτόν τον ισχυρισμό, ο ενάγων ανέφερε την εξαμηνιαία πολιτική διατήρησης στοιχείων GPS του Western Express και αμφισβήτησε την εγκυρότητα της έρευνας του εναγομένου, η οποία διεξήχθη 27 μήνες μετά το ατύχημα. Ο δικαστής αποφάσισε ότι υπήρχε ζήτημα ουσιαστικού γεγονότος το οποίο έπρεπε να επιλυθεί από κριτική επιτροπή. Κρίσιμη

[131] Βλ. https://www.cbsnews.com/news/slain-womans-fitbit-data-cited-murder-case-husband/
[132] Βλ. https://www.fitbit.com/eu/home, πρόκειται για «έξυπνο ρολόι» που υποβοηθά στην άσκηση με την καθοδήγηση του χρήστη, διαθέτοντας γεωεντοπισμό και δεδομένα κίνησης και άθλησης.
[133] Βλ. Υπόθεση Howze v. Western Express, Inc., 101 Fed. R. Evid. Serv. 107, WL 4180898 (N.D. Ala., 2016.

για την δικαστική διαχείριση της υπόθεσης αυτής αναδείχθηκε η υπηρεσία λήψης δεδομένων.

Οι συσκευές εντοπισμού περιουσιακών στοιχείων επωφελούνται από το GPS, το Wi-Fi και την τεχνολογία Bluetooth για να επιτρέπουν στις οντότητες να παρακολουθούν τα κινούμενα περιουσιακά στοιχεία τους. Μπορούν να συλλέξουν βασικά δεδομένα τοποθεσίας ή ενδέχεται να έχουν επεκτείνει λειτουργίες που λαμβάνουν άλλες πληροφορίες, όπως διαγνωστικά, μηνύματα, καιρικές συνθήκες ή δεδομένα συμμόρφωσης. Χρησιμοποιούνται για την παρακολούθηση κινητών στοιχείων υψηλής αξίας (π.χ. οχημάτων στόλου, εξοπλισμού κατασκευών, ιατρικών συσκευών) και αρχίζουν να εμφανίζονται στην αυξανόμενη ποικιλία συσκευών καταναλωτών IoT[134]. Η υπόθεση Howze καταδεικνύει ότι η αποδεικτική ισχύς των δεδομένων από τα στοιχεία γεωεντοπισμού και τα σχετικά μεταδεδομένα είναι εξαιρετικά αποδεκτά στην δικαστηριακή πρακτική. Είναι επίσης ιδιαίτερα χρήσιμες οι πληροφορίες, που προσφέρουν στους ερευνητές που εργάζονται για μια οντότητα οργανισμό που κατέχει ή χρησιμοποιεί το επίμαχο περιουσιακό στοιχείο. Όπως και στην υπόθεση Howze, η βάση δεδομένων του πελάτη μπορεί να αναζητηθεί ή τα δεδομένα μπορούν να εξάγονται σε μια καλύτερη πλατφόρμα για να καταστούν κατανοητά και να διαφυλαχθούν πληροφορίες που απαντούν σε κρίσιμα ερωτήματα αναφορικά με τις ζητούμενες απαντήσεις και ειδικότερα αναφορικά με το Ποιός; Πότε; Πού; Ο πραγματογνώμονας στην περίπτωση αυτήν μπορεί να αποφύγει την εξέταση στο ίδιο το αντικείμενο, που συγκεντρώνει το ενδιαφέρον, αντλώντας στοιχεία από τη βάση δεδομένων ή την σχετική εφαρμογή. Στην περίπτωση αυτήν τα δομημένα δεδομένα θα πρέπει να συλλέγονται και να παρέχονται νωρίς στην έρευνα για να αποφεύγονται περιπτώσεις κατά τις οποίες αυτά καταστρέφονται λ.χ. σε περίπτωση μιας τακτικής προγραμματισμένης εκκαθάρισης της βάσης δεδομένων. Τα ζητήματα ασφάλειας φυσικά στην διαχείριση των δομημένων δεδομένων θα πρέπει να τύχουν ιδιαίτερης προσοχής. Στην περίπτωση μάλιστα που προκύπτει ένας μεγάλος όγκος δεδομένων ή πολυπλοκότητα των σχετικών ερωτημάτων που πρέπει να απαντηθούν, τότε είναι απαραίτητη η συμμετοχή ειδικού είτε ως τεχνικού συμβούλου είτε ως πραγματογνώμονα, που κατανοεί δομημένα δεδομένα.

[134] Βλ. *Chr. Stergiou, K. Psannis, B.-G. Kimb, Br. Gupta*, Secure integration of IoT and Cloud Computing, https://www.researchgate.net/profile/Kostas_Psannis/publication/311065854_Secure_Integration_of_Internet-of-Things_and_Cloud_Computing/links/5a44ca35aca272d2945c4b1b/Secure-Integration-of-Internet-of-Things-and-Cloud-Computing.pdf

6. ΣΥΝΟΠΤΙΚΕΣ ΑΝΑΦΟΡΕΣ ΣΤΗΝ ΔΙΚΟΝΟΜΙΚΗ ΔΙΑΡΘΩΣΗ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΑΝΑΚΡΙΤΙΚΗ ΕΡΕΥΝΑ

Για την ευχερέστερη παρακολούθηση των θέσεων και των αναφορών που καταγράφονται προοδευτικά στις επόμενες ενότητες, κατά την ειδικότερη προσέγγιση του αντικειμένου της μελέτης αυτής, κατά προσωπική εκτίμηση, ενδείκνυται μια σχηματική και καταγραφική όμως, αναφορά στον τρόπο με τον οποίον ο Κ.Ποιν.Δ. ρυθμίζει τις ερευνητικές πράξεις στο στάδιο της προδικασίας, αλλά και σε εκείνες τις διατάξεις που αναφέρονται στα πρόσωπα που λειτουργικά εμπλέκονται στις ανακριτικές έρευνες, οι αναφερόμενοι ως ανακριτικοί υπάλληλοι. Η αναφορά είναι απλά καταγραφική διότι ο τομέας της προδικασίας στον Κ.Ποιν.Δ. τόσο γενικά όσο και ειδικότερα οι ερευνητικές διαδικασίες και πρακτικές από μόνες τους είναι τομέας που απαιτεί εμβάθυνση, η οποία εκφεύγει των ορίων της παρούσας αναζήτησης. Κατά την επιλογή λοιπόν του Κ.Ποιν.Δ. οι ανακριτικοί υπάλληλοι διαχωρίζονται σε γενικούς και ειδικούς.

i. Η παραγγελία για την ποινική έρευνα.

Η αρμοδιότητα για την επιχείρηση ερευνών σχετικά με την εξιχνίαση, προετοιμασία – συγκέντρωση αποδεικτικού υλικού μέχρι την τελική παραπομπή σε δίκη κατηγορουμένου, ή το, με οποιονδήποτε άλλο προβλεπόμενο τρόπο, πέρας της ποινικής δίωξης, ανήκει στον Εισαγγελέα Πλημμελειοδικών[135] (αρμοδιότητα που βγήκε ενισχυμένη μέσα από την πρόσφατη αναθεώρηση του Κ.Ποιν.Δ.[136]). Έγινε αναφορά σε επιχείρηση ερευνών και όχι σε ποινική δίωξη καθόσον στην πρώτη εντάσσουμε όλες τις ερευνητικές δράσεις, οι οποίες αποβλέπουν στην αξιολόγηση κατά πρώτον και στην αξιοποίηση, κατά δεύτερον λόγο, των πληροφοριών που παρουσιάζονται στον αρμόδιο Εισαγγελέα[137]. Αντίθετα με την άσκηση της ποινικής δίωξης έχουμε ενεργοποίηση του φαινομένου της ποινικής δίκης που σε κάθε περίπτωση θα καταλήξει με δικαιοδοτική κρίση αξιολόγησης του υλικού, όχι κατ' ανάγκη σε περιβάλλον δικαστικού σχηματισμού.

---

[135] Σύμφωνα με το άρθρο 27 § 1 Κ.Ποιν.Δ. Περαιτέρω όμως βάσει της ιεραρχικής δομής της Εισαγγελικής Αρχής και σύμφωνα με το άρθρο 28 § 1 Κ.Ποιν.Δ. σε εγκλήματα εξαιρετικής σημασίας το αρμόδιο Συμβούλιο Εφετών μπορεί να διατάξει τον Εισαγγελέα Εφετών να προβεί εκείνος στην άσκηση ποινικής δίωξης.

[136] Βλ. Ν 4620/2019, ΦΕΚ Α 96/11.06.2019, όπως ισχύει.

[137] Βλ. *Θ. Δαλακούρας*, Η λειτουργική αρμοδιότητα του Εισαγγελέα Πλημμελειοδικών υπό το φως των ρυθμίσεων του Ν 3160/2003, (Άσκηση ποινικής δίωξης – Αποχή από την ποινική δίωξη – Αρχειοθέτηση της υπόθεσης), ΠοινΧρον 2004, 585 επ.,

Η άσκηση της ποινικής δίωξης για την προσωπική (πολλές φορές και για την περιουσιακή και οικονομική επίσης) κατάσταση του κατηγορουμένου, συνεπάγεται ιδιαίτερα σημαντικές συνέπειες, όπως είναι η στέρηση της προσωπικής ελευθερίας, συνθήκη για την οποία επέδειξε ενδιαφέρον ο συντακτικός νομοθέτης με την διάταξη του άρθρου 7 Συντ να αποκλείει την αναδρομική δημιουργία αξιοποίνου. Έτσι η άσκηση και η γενικότερη διαχείρισή της, ασκείται στο όνομα της Ελληνικής Πολιτείας, η οποία είναι και ο μοναδικός και αποκλειστικός φορέας εξουσίας[138]. Σημειώνεται ότι η άσκηση της ποινικής δίωξης γίνεται αποκλειστικά από τον Εισαγγελικό λειτουργό, που είναι επιφορτισμένος με το έργο αυτό. Πρόκειται για ιδιαίτερα σημαντική πτυχή του ποινικού δικονομικού μας συστήματος, ώστε η κίνηση της ποινικής δίωξης από οποιονδήποτε άλλον να καθιστά την διαδικασία άκυρη στην βάση της ρήτρας των απολύτων ακυροτήτων[139] του άρθρου 171 παρ. 1 περ. β΄ Κ.Ποιν.Δ.

Επιπρόσθετα, η άσκηση της ποινικής δίωξης είναι αποδεσμευμένη από την ύπαρξη κάποιου προσώπου ως υπαιτίου καθόσον η κίνησή της αναφέρεται σε αξιόποινη πράξη, ήτοι ασκείται in rem και όχι in personam (δεν συνδέεται υποχρεωτικά με την ύπαρξη προσώπου υποδεικνυομένου ως δράστη)[140]. Περαιτέρω διαφοροποιήσεις αναφορικά με το είδος του εγκλήματος, έχουμε στις περιπτώσεις της αυτεπάγγελτης δίωξης και σε εκείνην της κατ' έγκληση, δηλαδή στις περιπτώσεις που η πρωτοβουλία για την ενημέρωση του Εισαγγελέα που θα διατάξει την δίωξη έχει επιφυλαχθεί υπέρ του θύματος[141].

Πριν την άσκηση όμως της ποινικής δίωξης σαφώς και δεν αποκλείονται οι σχετικές ποινικές έρευνες για την αποδεικτική ενίσχυση και γενικότερα για την αξιοποίηση πληροφοριών αναφορικά με διάπραξη αξιόποινης πράξης. Στα πλαίσια αυτής του ερευνητικού σταδίου, ο Εισαγγελέας Πλημμελειοδικών διατάσσει προκαταρκτική εξέταση ή προανάκριση[142]. Τόσο στις δύο αυτές περιπτώσεις, όπως και στην περίπτωση της ανάκρισης,

---

[138] Βλ. *Β. Αδάμπας, Μ. Παπαχρήστου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 160 επ., *Αργ. Καρράς*, Ποινικό Δικονομικό Δίκαιο, 2017, σελ. 249.

[139] Βλ. *Θ. Δαλακούρας*, Οι ακυρότητες στο ποινικοδικονομιό μας σύστημα, σε Θ. Δαλακούρα, Το ηλεκτρονικό έγκλημα, Νομική Βιβλιοθήκη 2019, σελ. 28 επ.,

[140] Βλ. *Β. Αδάμπας, Μ. Παπαχρήστου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 163 με τις εκεί παραπομπές.

[141] Αφορά σε σχετικά ήπιες αξιόποινες συμπεριφορές που δεν έχουν επικινδυνότητα για το κοινό και ενδέχεται η δίωξή τους να μην είναι επιθυμητή από το ίδιο το θύμα εν όψει δημοσιοποίησης στοιχείων, την οποία δεν επιθυμεί.

[142] Βλ. *Π. Παπανδρέου*, Η Προκαταρκτική εξέταση, ΠοινΔικ 2006, 191, με τις εκεί παραπομπές στη νομολογία και τη θεωρία, *της ιδίας*, Η ποινική δίκωξη, ΠοινΔικ 2006, 439, *της ιδίας*, Η περάτωση της προανάκρισης, ΠοινΔικ 2006, 1287, *Β. Αδάμπας, Μ. Παπαχρήστου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 198 επ. με τις εκεί παραπομπές

η παραγγελία του Εισαγγελέα Πλημμελειοδικών είναι καθοριστική για τα επιτρεπτά πλαίσια της έρευνας.

Αποδέκτης της παραγγελίας του Εισαγγελέα Πλημμελειοδικών είναι κάποιος ανακριτικός υπάλληλος, από τον κύκλο των προσώπων που καθορίζονται στο άρθρο 31 Κ.Ποιν.Δ. με σαφή αναφορά/παραπομπή της διάταξης σε ειδικότερα νομοθετήματα.

ii. Οι ανακριτικοί υπάλληλοι.

Σύμφωνα με την διάταξη του άρθρου 31 Κ.Ποιν.Δ., η αυτεπάγγελτη προανάκριση και η προκαταρκτική εξέταση διενεργούνται ύστερα από παραγγελία του εισαγγελέα πλημμελειοδικών και υπό τη διεύθυνσή του από: α) τους πταισματοδίκες και όπου δεν υφίσταται ειδικό πταισματοδικείο από τους ειρηνοδίκες, β) τους αρμόδιους βαθμοφόρους της Ελληνικής Αστυνομίας και του Λιμενικού Σώματος, που ορίζονται στους αντίστοιχους οργανισμούς ως γενικοί ανακριτικοί υπάλληλοι, και γ) δημοσίους υπαλλήλους, όπου αυτό προβλέπεται σε ειδικούς νόμους, που ορίζονται ως ειδικοί ανακριτικοί υπάλληλοι. Στις περιπτώσεις που ορίζει ο νόμος και ειδικότερα στα άρθρα 245 παρ. 2 Κ.Ποιν.Δ. (προανάκριση) και 250 παρ. 2 Κ.Ποιν.Δ. (ανάκριση) αυτεπάγγελτη προανάκριση ενεργεί ο ανακριτικός υπάλληλος ή ο ανακριτής, αντίστοιχα, χωρίς παραγγελία από τον Εισαγγελικό λειτουργό. Πρόκειται για τις περιπτώσεις όπου από την καθυστέρηση, που συνεπάγεται η υποβολή έκθεσης για αξιολόγηση από τον Εισαγγελέα, ενδέχεται να υποστεί αλλοίωση ή απώλεια σημαντικό αποδεικτικό υλικό.

Ο καθορισμός των γενικών ανακριτικών υπαλλήλων στον χώρο του Αστυνομικού ή του Λιμενικού Σώματος, ρυθμίζεται από τους εσωτερικούς οργανισμούς τους και αναφέρεται κατά κύριο λόγο στους αξιωματικούς των σωμάτων αυτών[143]. Όλοι οι ανωτέρω υποχρεούνται να εκτελούν αμελλητί τις παραγγελίες των δικαστικών και των εισαγγελικών αρχών σύμφωνα με τις διατάξεις του κώδικα οργανισμού των δικαστηρίων και κατάστασης δικαστικών λειτουργών.

Έργο των ανακριτικών υπαλλήλων είναι η άμεση, κατά το δυνατόν, επέμβαση κι διασφάλιση του αποδεικτικού υλικού, που αφορά στην τέλεση της υπό έρευνας αξιόποινης συμπεριφοράς. Στα πλαίσια των δράσεών τους αυτών οι ανακριτικοί υπάλληλοι συγκεντρώνουν πληροφορίες για το έγκλημα και τους υπαιτίους, μεταβαίνουν επί τόπου, διεξάγουν κάθε είδους νομιμοποιούμενη έρευνα, εξετάζουν μάρτυρες, διασφαλίζοντας ότι

[143] Βλ. αρ. 13 παρ. 4 και 23 παρ. 1 Ν 1481/1981, αρ. 1 παρ. 3 Ν 2226/1994.

δεν υπάρχει αλλοίωση των μαρτυρικών τους καταθέσεων (λ.χ. με τον διαχωρισμό τους και την ταυτόχρονη, εφόσον είναι δυνατόν, εξέτασή τους από διαφορετικούς υπαλλήλους), γενικότερα δε ενεργούν οτιδήποτε είναι αναγκαίο για την διατήρηση των αποδείξεων και την εξιχνίαση της ερευνώμενης εγκληματικής συμπεριφοράς[144].

Περαιτέρω ειδικότερα πεδία αναφορικά με εγκληματικές πράξεις, οι οποίες μπορούν να λάβουν μορφή τέλεσης πάντα μέσα από τον ψηφιακό κόσμο, αποτελώντας μια ακόμη εκδοχή ηλεκτρονικής εγκληματικότητας, διαμορφώνουν τον κύκλο των ειδικών ανακριτικών υπαλλήλων, οι οποίοι είναι δημόσιοι υπάλληλοι, που λειτουργούν σε δομές κρατικών υπηρεσιών[145] ή ανεξαρτήτων αρχών[146], όπως είναι οι οικονομικές δομές και τα τελωνεία και ορίζονται από τα εσωτερικά λειτουργικά τους διατάγματα και οργανογράμματα, ως ανακριτικοί υπάλληλοι.

Ως τέτοιοι ειδικοί ανακριτικοί υπάλληλοι αναφέρονται ενδεικτικά[147] οι λιμενικοί αξιωματικοί, οι υπάλληλοι κι επιθεωρητές των Οικονομικών Υπηρεσιών, οι δασικοί υπάλληλοι, οι θηροφύλακες, οι αξιωματικοί της πυροσβεστικής υπηρεσίας.

Μια σημαντική επισήμανση έχει να κάνει με τα όρια αρμοδιοτήτων των υπαλλήλων της ΕΛΑΣ, οι οποίοι κατ' άρθρα 31 και 239 επ. Κ.Ποιν.Δ. επιχειρούν πάντοτε κατασταλτικά, ήτοι μετά από την σχετική νομιμοποιητική διαδικασία της εισαγγελικής παραγγελίας και σύμφωνα με τα αυστηρά πλαίσια δράσης που ορίζει ο Κώδικας. Από την άλλη στα ίδια πρόσωπα, συμπυκνώνεται και η δράση που επιφυλάσσει ο Ν 4249/2014[148]. Σύμφωνα με το αρ. 11 § 3 Ν 4249/2014, όπως ισχύει, η αρμοδιότητα της αστυνομίας περί δημόσιας ασφάλειας περιλαμβάνει ιδίως α. τη δίωξη των εγκλημάτων κατά της ζωής, της προσωπικής ελευθερίας, της ιδιοκτησίας και λοιπών περιουσιακών δικαιωμάτων, β. τη δίωξη του οικονομικού και του *ηλεκτρονικού εγκλήματος*, γ. τον έλεγχο και τη δίωξη της παράνομης διακίνησης ναρκωτικών, δ. τη δίωξη του λαθρεμπορίου και της αρχαιοκαπηλίας, ε. τη μέριμνα για την προστασία των ανηλίκων και την εφαρμογή των διατάξεων για τα ήθη, στ.

---

[144] Βλ. *Π. Παναγιωτόπουλος*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 1536, *Θ. Δαλακούρας*, Η συγκέντρωση του αποδεικτικού υλικού, ΠοινΧρον 2011, 247.

[145] Βλ. *Ν. Λίβος*, Η διεξαγωγή διοικητικών και ανακριτικών ερευνών από το Σώμα Δίωξης Οικονομικού Εγκλήματος (ΣΔΟΕ), σε Ι. Φωτόπουλου, Φορολογικές Κυρώσεις, 2002, 119.

[146] Βλ. *Γρ. Τσόλιας*, Οι ελεγκτικές αρμοδιότητες της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Μια πρώτη προσέγγιση), ΔiΜΕΕ 2005, 539. *Ν. Λίβος*, «Πολύ κακό για το τίποτα»; Οι ανακριτικές αρμοδιότητες της Αρχής Καταπολέμησης της Νομιμοποίησης Εσόδων από Εγκληματικές Δραστηριότητες, ΠοινΧρον 2006, 380.

[147] Βλ. *Π. Καίσαρης, Σπ. Παππάς*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 156 με τις εκεί παραπομπές στα ειδικότερα νομοθετήματα, που καθορίζουν τις αρμοδιότητές τους ως ανακριτικών υπαλλήλων.

[148] Βλ. Ν 4249/2014 «Αναδιοργάνωση ΕΛΑΣ, Πυροσβεστικού, Γ.Γ.Π.Π., αναβάθμιση Υπηρεσιών Υπ.Δημ.Τάξης».

τον έλεγχο της τήρησης των διατάξεων που αφορούν τα υπομνήματα και την προστασία του εθνικού νομίσματος και συναλλάγματος, ζ. την επιτήρηση των τόπων όπου συχνάζουν οι ύποπτοι διάπραξης εγκλημάτων και τον έλεγχο των προσώπων αυτών, η. την αναζήτηση εξαφανισθέντων προσώπων και απολεσθέντων και κλεμμένων αντικειμένων, θ. την αναζήτηση και σύλληψη των διωκόμενων προσώπων. Ο νόμος κάνει αναφορά σε δίωξη αλλά η ανάγνωση της διάταξης στο πνεύμα και το περίγραμμα αρμοδιοτήτων της Αστυνομικής Διεύθυνσης στην οποία υπάγεται το τμήμα ασφαλείας, που είναι η εξασφάλιση της δημόσιας ειρήνης και ευταξίας, της απρόσκοπτης κοινωνικής διαβίωσης των πολιτών, η πρόληψη και καταστολή του εγκλήματος και την προστασία του Κράτους. Πρόκειται λοιπόν για την διοικητική δράση των γενικών ανακριτικών υπαλλήλων, με σαφώς προληπτικό προσανατολισμό, τουλάχιστον κατά ένα μεγάλο μέρος των ενεργειών τους.

Μάλιστα η Ελληνική Αστυνομία, για την εκπλήρωση της αποστολής της: α. χρησιμοποιεί επιστημονικές και τεχνικές μεθόδους διαλεύκανσης των εγκλημάτων και διαθέτει εγκληματολογικά εργαστήρια, τα οποία παρέχουν τις υπηρεσίες τους και σε άλλες αρχές, β. διαθέτει και χρησιμοποιεί τα αναγκαία επίγεια, εναέρια και πλωτά μεταφορικά και άλλα μέσα και υλικοτεχνικό εξοπλισμό, γ. μπορεί να συνάπτει μνημόνια συνεργασίας με φορείς και οργανισμούς άλλων Υπουργείων και Οργανισμούς Τοπικής Αυτοδιοίκησης για θέματα γενικής αστυνόμευσης και εξυπηρέτησης των πολιτών, κοινής αρμοδιότητας, τα οποία εγκρίνονται με απόφαση των Υπουργών Εσωτερικών και Δημόσιας Τάξης και Προστασίας του Πολίτη και του κατά περίπτωση συναρμόδιου Υπουργού, δ. συνεργάζεται με τις αντίστοιχες αρχές και Υπηρεσίες των άλλων χωρών και συμμετέχει στο Διεθνή Οργανισμό Εγκληματολογικής Αστυνομίας (Δ.Ο.Ε.Α. - INTERPOL), στην Ευρωπαϊκή Αστυνομική Υπηρεσία (EUROPOL), στον Ευρωπαϊκό Οργανισμό για τη διαχείριση της επιχειρησιακής συνεργασίας στα εξωτερικά σύνορα των κρατών - μελών της Ε.Ε. (FRONTEX), σε Διεθνείς και Περιφερειακούς Οργανισμούς, καθώς και στα όργανα της Ευρωπαϊκής Ένωσης που χειρίζονται θέματα αστυνομικής φύσης.

iii. Η αστυνομική έρευνα.

Από την ανακριτική έρευνα που επιχειρούν οι αστυνομικοί ως (προ-)ανακριτικοί υπάλληλοι κατ' αρ. 31 Κ.Ποιν.Δ. πρέπει να διακρίνουμε την *αστυνομική έρευνα*, η οποία εντάσσεται στο πλέγμα των διοικητικών αρμοδιοτήτων των σωμάτων ασφαλείας. Πρόκειται για έρευνες που επιχειρούνται στην βάση της κρίσης του επικεφαλής ομάδας αστυνομικών ή

και σε περίπτωση μεμονωμένου υπαλλήλου, που εκτιμά ότι υπάρχει συνθήκη που αφορά προπαρασκευή ή τέλεση αξιόποινης πράξης, ή αναφέρεται σε πρόσωπο ή ομάδα προσώπων που κρίνονται ύποπτοι. Τα σχετικά κριτήρια και τα πλαίσια επιτρεπτής έρευνας από τους αστυνομικούς υπαλλήλους, ενεργούντες στα πλαίσια των αρμοδιοτήτων του και όχι ως ανακριτικοί υπάλληλοι, καθορίζονται από τα άρθρα 93 και ειδικότερα 96 επ. ΠΔ 141/1991[149].

Η σχετική αστυνομική έρευνα μπορεί να περιλαμβάνει έρευνα σε κατοικία που επιτρέπεται μόνο με τη ρητή συναίνεση του ενοίκου της, σωματικές έρευνες σε μεταφορικά μέσα και μεταφερόμενα αντικείμενα και έρευνες σε ιδιωτικούς χώρους μη προσιτούς στο κοινό που δεν υπάγονται στην έννοια της κατοικίας, οι οποίες γίνονται όταν υπάρχει σοβαρή υπόνοια τελέσεως αξιοποίνου πράξεως ή απόλυτη ανάγκη, έρευνες σε χώρους δημοσίους ή ιδιωτικούς αλλά ελεύθερα προσιτούς στο κοινό, οι οποίες γίνονται ελεύθερα. Μέριμνα λαμβάνεται προκειμένου κατά τις έρευνες να μην θίγεται η προσωπικότητα ούτε να ενοχλείται αδικαιολόγητα το πρόσωπο που υποβάλλεται σε σωματική έρευνα ή ο ιδιοκτήτης του χώρου ή αντικειμένου που ερευνάται, στο μέτρο που αυτό είναι δυνατό[150].

iv. Η ένταξη της ανακριτικής έρευνας στην ποινική δίκη. Η Εισαγγελική παραγγελία.

Από την σχετική σπονδυλωτή διάρθρωση αναφορικά με την εξέλιξη του ποινικού φαινομένου, μπορούμε να δώσουμε μια σχηματική δομή της πορείας από την αξιοποίηση των πληροφοριών για διάπραξη αξιόποινης πράξης ηλεκτρονικού εγκλήματος μέχρι την αμετάκλητη περάτωση της ποινικής δίωξης.

Οι αρμόδιοι αστυνομικοί υπάλληλοι της δίωξης ηλεκτρονικού εγκλήματος θεσμικά είναι δέκτες των σχετικών καταγγελιών τρίτων, αλλά και οι ίδιοι έχουν την δυνατότητα αναζήτησης αξιόποινων συμπεριφορών στον παγκόσμιο ιστό. Η διακίνηση υλικού παιδικής πορνογραφίας, ιδίως με τη μορφή του διαμοιρασμού σχετικών αρχείων με διάταξη peer2peer, η διασπορά ηλεκτρονικών μηνυμάτων με σκοπό το hacking, το cracking ή το phishing, αλλά και ενδεχόμενη διαρροή – διαχείριση υλικού που αφορά τρομοκρατία, μόλις εντοπιστούν από τους ανακριτικούς υπαλλήλους, πρέπει να υποβληθούν για αξιολόγηση από τον αρμόδιο Εισαγγελικό λειτουργό.

[149] Βλ. ΠΔ 141/1991, Αρμοδιότητες οργάνων Υπ. Δημοσίας Τάξης, Θέματα Οργάνωσης Υπηρεσιών κλπ., ΒΔ Νόμος

[150] Βλ. για σχετικούς προβληματισμούς αναφορικά με την θεμιτή άσκηση της αστυνομικής έρευνας *Ελ. Συμεωνίδου - Καστανίδου* Αστυνομική Βία: Νομικό πλαίσιο και προβλήματα εφαρμογής, ΝοΒ 2006, σελ. 1641.

Εδώ τίθεται ένα σημαντικό ζήτημα αναφορικά με την δυνατότητα του εκάστοτε εισαγγελικού λειτουργού, ο οποίος ενδέχεται (για να μην μιλήσουμε με ανεπίτρεπτη επιστημονικά βεβαιότητα) να μην διαθέτει τις ειδικές γνώσεις[151] ώστε να αξιολογήσει ανάλογα το υποβληθέν υλικό αλλά και τον τρόπο κτήσης του.

Ο Εισαγγελέας Πλημμελειοδικών (σε μια πολύ απλοϊκή, για την κατανόηση της διαδικασίας, προσέγγιση, καθόσον περαιτέρω εμβάθυνση εκφεύγει των πλαισίων της μελέτης αυτής) θα ενεργήσει δίδοντας την σχετική παραγγελία του, η οποία είναι κατεξοχήν μια έγγραφη εντολή, χωρίς να αποκλείεται από το νόμο και μια πρώτη προφορική εντολή προς αποφυγή απώλειας αποδεικτικού υλικού από την καθυστέρηση που συνεπάγεται η τήρηση της έγγραφης διαδικασίας με την καταχώρηση της υπόθεσης και τον σχηματισμό σχετικής καταγραφής στα τηρούμενα σχετικά αρχεία της εισαγγελίας.

ν. Παραγγελία για έρευνα (προκαταρκτική εξέταση, προανάκριση ή ανάκριση).

Η εντολή που θα διαλαμβάνει η παραγγελία, έχει να κάνει με την αποδεικτική συνοχή που αναδεικνύει το εισφερθέν υλικό, η φερομένη ως τελεσθείσα αξιόποινη συμπεριφορά και η ποινική της διαβάθμιση (πλημμέλημα ή κακούργημα) καθώς και η ενδεχόμενη δομική της πολυπλοκότητα, η οποία μπορεί να αναδείξει ακόμη και μια δομή εγκληματικής οργάνωσης. Η διαφορετικότητα στην επικινδυνότητα της εγκληματικής πράξης, βάσει όλων των ανωτέρω παραμέτρων, που πολύ πρόχειρα και συνοπτικά καταγράφηκαν ανωτέρω, δίνει τη βάση για τη μορφή που θα λάβει η παραγγελία.

Η αυξημένη αποδεικτική συνοχή και ενδεχόμενη άμεση απόδοση της πράξης σε ύποπτο, εφόσον κινείται στα πλαίσια κακουργηματικής πράξης, είναι βέβαιο ότι δικαιολογεί τον σχηματισμό κακουργηματικής δικογραφίας, με άσκηση ποινικής δίωξης και παραγγελία ανάκρισης, με σαφή πλέον απόδοση κατηγορίας και σύνταξη κατηγορητηρίου από τον παραγγέλλοντα εισαγγελικό λειτουργό, που την διαβιβάζει στον ανακριτή.

Αναλογική η προσέγγιση με εκπτώσεις στις διαβαθμίσεις ανά κατηγορία, όπως προαναφέρθηκαν, οδηγεί στην παραγγελία για προανάκριση[152] ή προκαταρκτική εξέταση[153].

[151] Βλ. *Ν. Δαγκλής*, Η αποδεικτική και διαγνωστική ελευθερία του ποινικού δικαστή σε ζητήματα που απαιτούν ειδικές γνώσεις: Εγγύηση ή ανάχωμα στην διερεύνηση του ηλεκτρονικού εγκλήματος σε Θ. Δαλακούρα, Το ηλεκτρονικό έγκλημα, Νομική Βιβλιοθήκη 2019, σελ. 188 επ., *Ι. Αγγελής*, Ηλεκτρονικό έγκλημα και απονομή της ποινικής δικαιοσύνης, ΠοινΔικ 2005, σελ. 1062 επ.
[152] Βλ. *Π. Παπανδρέου,* Η περάτωση της προανάκρισης, ΠοινΔικ 2006, 1287,
[153] Βλ. *Σ. Δασκαλόπουλος*, Η προκαταρκτική εξέταση και η άσκηση ποινικής δίωξης κατά το Ν 3160/2003, ΠοινΧρον 2003, 1027 επ.

Σαφώς όλες οι δράσεις αυτές και οι συνυφασμένες με τις σχετικές αρμοδιότητες διαδικασίες, είναι τμήματα της προδικασίας, που σε αντίθεση με την κυρία διαδικασία, διέπεται από την αρχή της έγγραφης διαδικασίας και της μυστικότητας (αρ. 241 εδ. α΄ Κ.Ποιν.Δ.), όπως σχολιάζεται και σε άλλο σημείο (ενταγμένο στην σχετική εκείνη συλλογιστική)[154] της μελέτης αυτής.

vi. Το αντικείμενο της ανακριτικής έρευνας. Σκοπός - Μέσα.

Σε μια λιγόλογη κι ελλειπτικά διατυπωμένη διάταξη[155], ο νομοθέτης δίνει τις παραμέτρους του ερευνητικού πεδίου της ανάκρισης, ως διαδικαστικό τμήμα της προδικασίας. Και φυσικά στην βασική ορολογική παραδοχή η έννοια της ανάκρισης περιλαμβάνει με την ευρεία έννοιά της όλο το φάσμα των παραγγελιών, δηλαδή κι εκείνη της προακαταρκτικής εξέτασης (αρ. 243 επ. Κ.Ποιν.Δ.) όσο και της προανάκρισης (αρ. 245 επ. Κ.Ποιν.Δ.) αλλά και της (κυρίας) ανάκρισης, με την στενή/τεχνική έννοια (αρ. 246 επ. Κ.Ποιν.Δ.).

Σύμφωνα με την διάταξη του άρθρου 239 Κ.Ποιν.Δ. η ανάκριση δεν περιορίζεται στο εύρος της έρευνας, η οποία καταλαμβάνει από πλευράς ενεργειών *καθετί* που μπορεί να βοηθήσει την *εξακρίβωση της αλήθειας*. Ο νομοθέτης επέλεξε μια ευρεία, ως προς τα μέσα έρευνας, τα οποία μπορεί να επιλέξει για την ικανοποίηση του σκοπού ο ανακριτικός υπάλληλος. Το πολυσχιδές της εγκληματικής δράσης και ευρηματικότητα των δραστών, σαφώς θα εγκλώβιζε την έρευνα σε στεγανά, τα οποία θα την καθιστούσαν δυσλειτουργική στην περίπτωση κατά την οποία, κάποια ερευνητική ενέργεια θα βρισκόταν εκτός του ορισμένου πεδίου. Σε όλες αυτές τις σκέψεις να προστεθεί και το στοιχείο της διαρκούς προόδου της τεχνολογίας (σε όλους τους τομείς και όχι αποκλειστικά στον τομέα της πληροφορικής και των επικοινωνιών), που επιβάλλουν μερικές φορές καινοτόμες μεθόδους

[154] Βλ. ανωτέρω υπό 4. Η σημασία των ψηφιακών πειστηρίων στην ανακριτική ερεύνα, *ii. Τα δικονομικά χαρακτηριστικά – Αρχές της Ανακριτικής Διαδικασίας*, σελ. 44 επ.

[155] Βλ. αρ. 239 Κ.Ποιν.Δ. στο οποίο ορίζεται ότι «- *Σκοπός της ανάκρισης. 1. Σκοπός της κύριας ανάκρισης είναι η συλλογή των αναγκαίων αποδεικτικών στοιχείων για να βεβαιωθεί η τέλεση εγκλήματος και να αποφασιστεί αν πρέπει να εισαχθεί κάποιος σε δίκη γι' αυτό. 2. Κατά την κύρια ανάκριση γίνεται καθετί που μπορεί να βοηθήσει την εξακρίβωση της αλήθειας, εξετάζεται και βεβαιώνεται αυτεπαγγέλτως όχι μόνο η ενοχή, αλλά και η αθωότητα του κατηγορουμένου, καθώς και κάθε στοιχείο που αφορά την προσωπικότητά του και επηρεάζει την επιμέτρηση της ποινής. Αν ο κατηγορούμενος είναι ανήλικος, γίνεται ειδική έρευνα για την υγιεινή, την ηθική και τη διανοητική του κατάσταση, για την προηγούμενη ζωή του, για τις οικογενειακές συνθήκες και γενικά για το περιβάλλον του. Γι' αυτό το σκοπό όποιος ενεργεί την ανάκριση μπορεί να αναθέσει τη συλλογή των απαιτούμενων πληροφοριών σε έναν από τους επιμελητές που υπηρετούν στις κατά τόπους Υπηρεσίες Επιμελητών Ανηλίκων. Η σχετική έκθεση των επιμελητών τίθεται στη δικογραφία, λαμβάνει δε γνώση αυτής και ο κατηγορούμενος.*»

για την προσπέλαση σε χώρους, που ίσως σε διαφορετική περίπτωση αποτελούσαν στεγανά για την επιβολή της δικαιοσύνης.

Ο δε ερευνητικός στόχος του συγκεκριμένου διαδικαστικού σταδίου είναι η συλλογή των αναγκαίων αποδεικτικών στοιχείων για να βεβαιωθεί η τέλεση εγκλήματος και να αποφασιστεί αν πρέπει να εισαχθεί κάποιος σε δίκη γι' αυτό. Με άλλα λόγια η αποδεικτική ενίσχυση της κατηγορίας που θα δικαιολογήσει (θεμελιώσει) δίωξη για αξιόποινη πράξη, η οποία θα προσάγει κατηγορούμενο σε δίκη. Σημαντικός όμως εδώ είναι ο προσανατολισμός στην αρχή της εξεύρεσης της αλήθειας (*ουσιαστικής* αλήθειας). Στα πλαίσια αυτά εξετάζεται και βεβαιώνεται αυτεπαγγέλτως, ακόμη και αν δεν το αιτηθεί ο κατηγορούμενος, όχι μόνο η ενοχή, αλλά και η αθωότητά του, καθώς και κάθε στοιχείο που αφορά την προσωπικότητά του και επηρεάζει την επιμέτρηση της ποινής. Η όλη διατύπωση της διάταξης δίνει μια εικόνα πλήρους προπαρασκευής ενός υλικού, το οποίο θα αποτελέσει την λεγόμενη δικογραφία, που θα κριθεί, μέσα από την ζωντανή διαδικασία στο ακροατήριο, από τον δικαστή. Συνεπώς ο όποιος ενδεχόμενος εμπλουτισμός της δικογραφίας στο στάδιο της κυρίας δίκης, προς την κατεύθυνση της καταδίκης του κατηγορουμένου ή της απαλλαγής του, έχει να κάνει είτε με την προσκόμιση νέων στοιχείων, είτε με την διαφορετική ανάγνωση του υλικού που ήδη συγκεντρώθηκε και σχημάτισε την δικογραφία.

Εύγλωττα λοιπόν έχει υποστηριχθεί ότι *η ανάκριση τότε μόνο έχει εκπληρώσει ουσιαστικά το δικονομικό της προορισμό, όταν η υπόθεση έχει διερευνηθεί προς όλες τις κατευθύνσεις και τις πτυχές της με την αξιολόγηση πάντων των στοιχείων, φθάνοντας, κατά τον τρόπο αυτόν, σε απροσμάχητο στατικό στάδιο*[156]. Βέβαια το απροσμάχητο στατικό στάδιο αναφέρεται στην μη μεταβολή της ερευνητικής κατεύθυνσης, μετά από την αξιολόγηση όλου του αποδεικτικού υλικού. Αναφέρεται με άλλα λόγια στην αδυναμία μεταβολής των υποδείξεων, που αποδεικτικά προέκυψαν στο ερευνητικό αυτό στάδιο. Σε καμιά περίπτωση η θέση αυτή δεν έχει και την αξιολογική προσέγγιση της απόδειξης τέλεσης της εγκληματικής συμπεριφοράς για την οποία η έρευνα, διότι αυτό είναι έργο του Δικαστηρίου και αφορά στην απόδειξη της ενοχής του κατηγορουμένου[157]. Αυτό δεν είναι έργο της ανάκρισης, με όποια μορφή κι επίπεδο και αν γίνεται η έρευνα. *Η Ανάκριση ως αποτέλεσμα της ερευνητικής πορείας του σταδίου της προδικασίας μπορεί να κατηγορεί όχι να καταδικάζει.*

[156] Βλ. *Β. Αδάμπας, Μ. Παπαχρήστου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 1437, με παραπομπή στην ΣυμβΠλημΒολ 178/2000, ΠοινΧρον 2000, 459.
[157] Βλ. *Χ. Σεβαστίδης*, Κώδικας Ποινικής Δικονομίας (ερμηνεία κατ' άρθρο) τομ ΙΙΙ, 2015, σελ. 2798,

vii. Μερικές ακόμη σημαντικές παράμετροι.

Έχει αναφερθεί και σε άλλο των αναζητήσεών μου, ότι το πνεύμα που επικρατεί στην προδικασία, το οποίο χαράσσει την πορεία και δίνει τον χαρακτήρα της, είναι εκείνο που αναδεικνύεται από τον συνδυασμό της έγγραφης διαδικασίας (σε αντίθεση με την διαδικασία στο ακροατήριο) και της μυστικότητας. Ρητά η διάταξη του άρθρου 241 εδ. α΄ Κ.Ποιν.Δ, ορίζει ότι «*Η ανάκριση γίνεται πάντοτε εγγράφως και χωρίς δημοσιότητα……*». Όπως έχει εύσχημα και περιεκτικά αναφερθεί, πρόκειται για αρχές που επηρεάζουν σε επίπεδο ερμηνείας και εφαρμογής τη διεξαγωγή της γενικότερης ανακριτικής διαδικασίας[158].

αα. Η *αρχή της έγγραφης διαδικασίας* διέρχεται των στοιχείων της εκθέσεως, που είναι η διαδικαστική βάση κάθε πράξης που επιχειρείται στο στάδιο της προδικασίας και στην οποία αναφερθήκαμε λεπτομερώς ανωτέρω[159]. Ουσιαστικά είναι η έγγραφη απόδοση δράσεων και πράξεων, άρα γεγονότων, που λαμβάνουν χώρα στο στάδιο αυτό, επί των οποίων η σχετική βεβαίωση με τη σύμπραξη δικαστικού γραμματέα ή δύο ανακριτικών υπαλλήλων, ως εγγύηση της πιστότητας της αναφοράς γεγονότος (λ.χ. κατ' οίκον έρευνας, μαρτυρικής κατάθεσης κλπ), η οποία εμπεριέχεται στην έκθεση. Σκοπός που εξυπηρετείται με την διαδικαστική αυτήν πρακτική είναι η αξιοποίηση του αποδεικτικού υλικού από τις δικαστικές δομές (Εισαγγελέας, Δικαστικό Συμβούλιο, Δικαστήριο), που θα το αξιολογήσουν συσχετιζόμενο το υλικό αυτό με την δίωξη. Και όλα αυτά χωρίς την αμφισβήτηση αναφορικά με το εάν εμφιλοχώρησαν αλλοιώσεις σε αυτό που αποδίδει ως γεγονός η έκθεση[160].

ββ. Σημαντικό λειτουργικό ρόλο διαδραματίζει περαιτέρω η *αρχή της μυστικότητας* της διαδικασίας. Πρόκειται για την θεσμική δομή της διενέργειας όλων των ερευνητικών διεργασιών χωρίς δημοσιότητα. Πρόκειται ουσιαστικά για την αρχή της μυστικότητας με την ευρεία έννοια, άλλως για την αρχή της εξωτερικής μυστικότητας[161], σύμφωνα με οποία αποκλείεται η δυνατότητα παράστασης κοινού. Η εγγυητική λειτουργία της προστασίας από το ενδεχόμενο προσβολής των δικαιωμάτων του κατηγορουμένου, εξασφαλίζεται με την ύπαρξη του θεσμού των δικονομικών ακυροτήτων, με τις οποίες θα εξαφανιστεί πρακτικά κάθε ενέργεια που προσέβαλε δικαιώματά του. Με αυτήν επιτυγχάνεται η προστασία της

[158] Βλ. *Θ. Δαλακούρας*, Ο Νέος Κώδικας Ποινικής Δικονομίας, Συνοπτική ερμηνεία κατ' άρθρο Ν 4620/2019, Νομική Βιβλιοθήκη 2019, σελ.184.
[159] Βλ. ανωτέρω υπό 4. Η Σημασία των Ψηφιακών Πειστηρίων στην Ανακριτική Έρευνα, *ii. Τα δικονομικά χαρακτηριστικά – Αρχές της Ανακριτικής Διαδικασίας*, σελ. 44 επ.
[160] Βλ. *Β. Αδάμπας, Μ. Παπαχρήστου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 1444, σύμφωνα με τους οποίους η έγγραφη διαδικασία είναι απόρροια της άλλης αρχής που διέπει την προδικασία, ήτοι εκείνης της μυστικότητας.
[161] Βλ. *Θ. Δαλακούρας*, Οι ειδικές ανακριτικές πράξεις του αρθρ. 6 Ν 2928/2001, ΠοινΧρον 2001, σελ. 1022.

προσωπικότητας των εμπλεκομένων προσώπων, τόσο του κατηγορουμένου, βάσει της αρχής του τεκμηρίου της αθωότητας, ώστε να αποφευχθεί ο κοινωνικός στιγματισμός του, όσο όμως και του καταγγέλλοντος ή θύματος, ιδίως σε περιπτώσεις εγκλημάτων κατά της γενετήσιας ελευθερίας, όπου η στάση του κοινού πολλές φορές μεταλλάσσει τους ηθικούς ρόλους.

Σε αντίθεση με την εξωτερική δημοσιότητα, το δικαίωμα πληροφόρησης των διαδίκων της δίκης, μέσα από τις κατοχυρώσεις δικαιωμάτων κατά το στάδιο της προδικασίας, κατά τα οριζόμενα στα άρθρα 89 επ. Κ.Ποιν.Δ., παρέχει δικαίωμα για διαρκή και έγκαιρη ενημέρωση των διαδίκων στο στάδιο της προδικασίας (*εσωτερική δημοσιότητα*)[162]. Ειδικότερα ο κατηγορούμενος διατηρεί σειρά δικαιωμάτων (αρ. 89 έως και 106 Κ.Ποιν.Δ.), η προσβολή των οποίων συνιστά την απόλυτη ακυρότητα του αρ. 171 παρ. 1 δ΄ Κ.Ποιν.Δ.[163] με τις δραστικές συνέπειες της ακύρωσης όλων των διαδικαστικών πράξεων που ακολούθησαν (στηρίχθηκαν) στην άκυρη πράξη.

γγ. Σημαντική θέση στην ερευνητική αυτήν βάση, κατέχει η αρχή της *αναλογικότητας*, όπως πλέον έχει και ρητά θεσμοθετηθεί με την ισχύουσα διατύπωση του άρθρου 251 § 2 Κ.Ποιν.Δ[164].

Πρόκειται για αρχή του δικαίου, που έχει τη βάση της στο άρθρο 25 § 1 Συντ. με πλείστες όσες αναφορές σε νομοθετήματα αλλά και στη νομολογία όλων των κλάδων του δικαίου. Το περιεχόμενό της, στην πιο έσχατη δομή του διατυπωμένο δίδεται με τις ακόλουθες διάδοχες σκέψεις αποδίδει ως δικαιικό περιεχόμενο στο άρθρο 25 παρ. 1 Συντ, σύμφωνα με το οποίο οι κρατικές επιλογές, όπως αυτές εκφράζονται και μέσα από τις αποφάσεις και δράσεις των οργάνων της διοίκησης αλλά και της δικαστικής εξουσίας, πρέπει *να σέβονται την αρχή της αναλογικότητας*. Οι επιλογές των οργάνων αυτών και των εξουσιών που εκφράζονται μέσα από αυτές, πρέπει να ορίζονται γενικώς, κατά τρόπο αντικειμενικό και να δικαιολογούνται από αποχρώντες λόγους δημοσίου ή κοινωνικού συμφέροντος, να τελούν δε σε συνάφεια προς το αντικείμενο και τον χαρακτήρα της ρυθμιζόμενης δραστηριότητας. Ενόψει της αρχής της αναλογικότητας, οι επιβαλλόμενοι από τον νόμο περιορισμοί (όπως λ.χ. η στέρηση της ιδιοκτησίας στην περίπτωση της κατάσχεσης που μας απασχολεί εδώ) πρέπει να είναι πρόσφοροι και αναγκαίοι για την επίτευξη του

[162] Βλ. *Αδ. Παπαδαμάκης*, Προκαταρκτική εξέταση – προανάκριση: Μορφές και όρια της ερευνητικής δραστηριότητας, ΠοινΔικ 2008, 340, *Αργ. Καρράς*, Ποινικό Δικονομικό Δίκαιο, εκδ. ε΄, 2017, 369, *Β. Αδάμπας, Μ. Παπαχρήστου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 1445.
[163] Βλ. *Θ. Δαλακούρας*, Οι Ακυρότητες στο ποινικοδικονομικό μας σύστημα, σε Θ. Δαλακούρα, Ηλεκτρονικό έγκλημα, νομική βιβλιοθήκη 2019, 23 επ. και ειδικότερα 33 επ.
[164] Όπως διαμορφώθηκε η διάταξη αυτή με το αρ. 8 § 12 Ν 4637/2019.

επιδιωκόμενου από τον νομοθέτη σκοπού δημοσίου ή κοινωνικού συμφέροντος και να μην είναι δυσανάλογοι σε σχέση με αυτόν. Εκείνος που επιχειρεί πρέπει να διαθέτει (αλλά να είναι έτοιμος και να το τεκμηριώσει αν παραστεί ανάγκη) ευρύ περιθώριο εκτίμησης ως προς την καταλληλότητα και αναγκαιότητα ενός μέτρου και, συνεπώς, ο ενδεχόμενος δικαστικός έλεγχος της τήρησης της αρχής της αναλογικότητας περιορίζεται στην κρίση εάν η θεσπιζόμενη ρύθμιση ή διοικητική επιλογή ή ερευνητική δράση είτε είναι προδήλως απρόσφορη είτε υπερβαίνει προδήλως το απαραίτητο για την πραγματοποίηση του επιδιωκόμενου σκοπού μέτρο. Προκειμένου δε ο δικαστής να είναι σε θέση να ελέγξει τα ανωτέρω, ήτοι το εάν η ερευνητική δράση αποβλέπει στην ικανοποίηση συνταγματικώς θεμιτού σκοπού, πρέπει να προκύπτει ή να συνάγεται από την ίδια τη ρύθμιση, ερμηνευόμενη σύμφωνα με τους κανόνες της λογικής και τα διδάγματα της κοινής πείρας και σε συνδυασμό με τη λοιπή νομοθεσία που διέπει την επιλογή κι επιβολή του ανακριτικού μέτρου να προκύπτει η προαναφερόμενη συμμόρφωση και συμβατότητα[165].

Την αποτύπωση των αρχών αυτών την διαπιστώνουμε και στην τεχνική δομή της διάταξης του άρθρου 265 §§ 5 και 6 Κ.Ποιν.Δ., όπου υπάρχει αυστηρός περιορισμός στην πρόσβαση, αναπαραγωγή και αντιγραφή του ψηφιακού αντιγράφου (digital copy), το οποίο θα συσχετιστεί στην ποινική δικογραφία καθώς και άλλη ψηφιακή απόδοση της έρευνας, που τυχόν θα συνοδεύει την πραγματογνωμοσύνη που θα συνταχθεί από τον ερευνητή – αναλυτή στο τμήμα ψηφιακών πειστηρίων, που θα αναλύσει τα κατασχεθέντα πειστήρια.

[165] Βλ. ΣτΕ (σχηματισμός Ολομέλειας) 201/2020, σκέψη 13η, ΒΔ Νόμος (όμοιες και οι ΟλΣτΕ 202 έως 207/2020), με τις εκεί παραπομπές σε όμοια μείζονα σκέψη αναφορικά με την ερμηνεία της αρχής της αναλογικότητας παλαιότερων αποφάσεών του ιδίου σχηματισμού.

7. ΤΑ ΨΗΦΙΑΚΑ ΔΕΔΟΜΕΝΑ

Αφού προηγήθηκε η ανάπτυξη σχετικά με την θεωρητική βάση της αναζήτησης αλλά και την σημασία, που έχουν για την ανακριτική έρευνα, τα ψηφιακά δεδομένα, τα οποία εντοπίζονται εξαγόμενα από τις ηλεκτρονικές εργασίες κι επικοινωνίες, φτάνουμε στο σημείο της παρουσίασης του ορισμού τους και των χαρακτηριστικών τους, ως μια προσπάθεια κατανόησης των ιδιαιτεροτήτων τους, που θα επιτρέψει στην συνέχεια στις ειδικότερες προσεγγίσεις των ζητημάτων, τα οποία αναφύονται όταν γίνεται λόγος για την ανακριτική έρευνα, που αναφέρεται σε αυτά.

Α) ο γενικός νομικός ορισμός για τα ψηφιακά δεδομένα.

Ο Ποινικός Κώδικας (Π.Κ.) στα πλαίσια της συμμόρφωσης της χώρας μας, ουσιαστικά μέσα από τις επιταγές της Σύμβασης της Βουδαπέστης για το κυβερνοέγκλημα και τεχνικά μέσα από τις διατάξεις του Ν 4411/2016, ορίζει στο άρθρο 13 περ. θ΄ ότι τα «*Ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία*.». Ο ορισμός αυτός διατηρήθηκε και στην πρόσφατη θεμελιώδη τροποποίηση του Π.Κ. με το Ν 4619/2019. Ο ορισμός αυτός κρατεί ως τεχνικός – νομικός όρος στον χώρο του ποινικού δικαίου με την έννοια της διατήρησης αυτού του περιεχομένου στις αναφορές μας στον δικαιικό χώρο και όχι με την τεχνοκρατική διάσταση του όρου «τεχνικός».

Από τον ορισμό αυτόν διαμορφώνεται μια εικόνα για τα αποδιδόμενα χαρακτηριστικά, τόσο από άποψη νομική όσο και από άποψη τεχνολογική, τα οποία με την σειρά τους είναι στοιχεία, που θα καθορίσουν τον τρόπο με τον οποίον γίνεται η επιστημονική και τεχνική προσέγγισή τους στο περιβάλλον της ανακριτικής έρευνας με σκοπό την άντλησή τους και η αξιοποίησή τους στην ποινική δίκη. Στο σημείο αυτό πρέπει να τονιστεί το γεγονός ότι καίτοι τα ψηφιακά δεδομένα φέρονται άρρηκτα συνδεμένα με το ηλεκτρονικό έγκλημα, στην διάσταση που δίδεται ανωτέρω[166] αλλά και στις περισσότερες

[166] Βλ. ανωτέρω υπό 2. Γενικές Αναφορές στο Ηλεκτρονικό Έγκλημα, *i. Εννοιολογικός προσδιορισμός του ηλεκτρονικού εγκλήματος*, σελ. 22 επ.

θέσεις των μελετητών[167], είναι σαφές ότι η σημασία τους για την εξιχνίαση μιας αξιόποινης συμπεριφοράς αγγίζει και τις περιπτώσεις των παραδοσιακών εγκλημάτων. Έτσι, λ.χ. ο εντοπισμός ενός δεδομένου ψηφιακής μορφής (λ.χ. μιας φωτογραφίας που βεβαιώνεται ότι δεν έχει αλλοιωθεί ως δεδομένο) μπορεί να οδηγήσει στην σύνδεση ενός ατόμου με την ερευνώμενη πράξη, ή από την άλλη να οδηγήσει στην απαλλαγή του. Ένα αρχείο εικόνας ήχου από ένα κινητό τηλέφωνο κατά την ώρα τέλεσης μιας εγκληματικής πράξης μπορεί να αναδείξει ότι λ.χ. ο καταγγελλόμενος βιασμός δεν είναι σε καμιά περίπτωση βιασμός τόσο στην ουσιαστική όσο και στην νομοτεχνική του διάσταση[168]. Ή να δώσει προσδιοριστικά στοιχεία, βάσει χρήσης ηλεκτρονικών συσκευών, συνήθων ηλεκτρονικής επικοινωνίας, σε τόπο και χρόνο που αποξενώνουν τον φερόμενο ως δράστη από το εγκληματικό προσκήνιο.

Πρόκειται λοιπόν κατ' αρχήν για άυλα στοιχεία. Δεν έχουν απτή υλική μορφή και για τον λόγο αυτόν υπήρχαν οι πολλές θεωρητικές ενστάσεις για τον τρόπο διαχείρισής τους με το παλαιό (προ του ισχύοντος Κ.Ποιν.Δ.) δικονομικό καθεστώς, όπου ουσιαστικά ακολουθούσαν την τύχη των υλικών φορέων τους, των ψηφιακών πειστηρίων, κάτι το οποίο μπορεί να λειτούργησε ως λύση ανάγκης, χωρίς όμως αυτό να σημαίνει ότι ήταν νομικά ορθό και απαλλαγμένο από θεωρητικές ενστάσεις και πρακτικούς προβληματισμούς. Το γεγονός ότι έχουμε να κάνουμε με άυλο στοιχείο σαφώς και απαιτεί σημαντική προσοχή καθόσον επιβάλλει διαχειριστικές μεθόδους και προσεγγίσεις διαφορετικές από τις συνήθεις παραδοσιακές πρακτικές στα πλαίσια της ανακριτικής έρευνας. Και τούτο σε δύο επίπεδα. Τόσο στο επίπεδο το αμιγώς ερευνητικό όσο και στο επίπεδο της διαχείρισης της συνθήκης αναφορικά με την άσκηση των δικαιωμάτων του κατηγορουμένου βασικά αλλά και των διαδίκων ως σύνολο κατ' επέκταση.

Είμαστε ακόμη μακριά από τις αναφορές στο πρωτόκολλο διαχείρισης των ψηφιακών δεδομένων από την εντοπισμό τους μέχρι την αξιοποίησή τους. Επιβάλλεται όμως, για την καλύτερη κατανόησή τους, η κατηγοριοποίησή τους, προκειμένου να αναδειχθούν ιδιαιτερότητες, που ενδεχόμενα απαιτούν ιδιαίτερη προσοχή από τον ερευνητή.

---

[167] Βλ. ενδεικτικά από τις προηγούμενες παραπομπές, *Β. Κάτος*, Ψηφιακά Πειστήρια, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, σελ. 65, *Δ. Κιούπη*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, σελ. 41 επ, *Θ. Δαλακούρας*, Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν 4411/2016), ο.π., σελ. 5, *Γ. Μπουρμά*, Η νομιμότητα των ερευνών σε ηλεκτρονικά δίκτυα και δεδομένα στις περιπτώσεις εγκλημάτων στον κυβερνοχώρο, ΠοινΔνη 2019, σελ. 557, *Ι. Αγγελή*, Διαδίκτυο και ποινικό δίκαιο, ΠοινΧρον 2000, σελ. 676, *R. Anderson, Chr. Barton, R. Boehme, R. Clayton, M. J.G. van Eeten, M. Levi, T. Moore, St. Savage*, Measuring the Cost of Cybercrime, 2012, http://www.med.a51.nl/sites/default/files/pdf/Anderson_ WEIS2012.pdf.

[168] Βλ. ΣυμβΠλημΒερ 83/2015 (αδημοσίευτο), σελ. 5.

Η βασική δομή και χαρακτηριστικό των ψηφιακών δεδομένων τα κατατάσσει στα στοιχεία σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα. Με άλλα λόγια είναι στοιχεία, τα οποία αποκτούν, τουλάχιστον στον παρόντα χρόνο, υπόσταση μόνο στο ψηφιακό περιβάλλον των υπολογιστικών μηχανών, τις οποίες σε αυτό εδώ το στάδιο τις αξιολογούμε ως λειτουργικό σύνολο αποτελούμενο από το λογισμικό (software) και το υλισμικό (hardware).

Βέβαια ο εργώδης αγώνας δρόμου της επιστήμης της πληροφορικής, δεν συναντά φραγμούς ακόμη και στο ζήτημα της «αισθητικοποίησης» των ψηφιακών δεδομένων. Οι συναντήσεις και οι εμπλοκές των ανθρώπων με τα προσωπικά ψηφιακά δεδομένα που δημιουργούν είναι ένας νέος και συναρπαστικός τομέας ερευνητικού ενδιαφέροντος σε αυτήν την εποχή της υπεροχής των ψηφιακών δεδομένων. Όπως και σε άλλο σημείο αναφέρουμε, μάζες προσωπικών πληροφοριών δημιουργούνται συνεχώς μέσω της χρήσης ψηφιακών τεχνολογιών από ανθρώπους και χρησιμοποιούνται για διάφορους σκοπούς από μια σειρά φορέων. Οι άνθρωποι βρίσκονται αντιμέτωποι με το αίνιγμα του τρόπου ερμηνείας, ελέγχου και αντίληψης των ζωντανών δεδομένων τους. Ο επιστημονικός δε κόσμος εξετάζει και την πρόκληση του πώς τα προσωπικά ψηφιακά δεδομένα και στην κυκλοφορία τους μπορούν να γίνουν πιο αντιληπτά και επομένως ερμηνεύσιμα στους ανθρώπους με τη χρήση τρισδιάστατων υλικών[169].

Β) διακρίσεις των ψηφιακών δεδομένων σε κατηγορίες.

Στο επίπεδο αυτό τα ψηφιακά δεδομένα, ανάλογα με το είδος τους μπορούν να αξιολογηθούν και να κατηγοριοποιηθούν[170] σε:

i. (ηλεκτρονικά) *ακατέργαστα δεδομένα* (raw data) τα οποία είναι πρωτότυπες ηλεκτρονικές μορφές που μπορούν να αποθηκευτούν σε μέσο που μπορεί να φιλοξενήσει και να αποθηκεύσει ηλεκτρονικά δεδομένα, χωρίς όμως από αυτά να μπορεί να εξαχθεί αξιοποιήσιμο ψηφιακό δεδομένο.

ii. *δεδομένα υπολογιστή* (computer evidence), τα οποία αντλούνται από τον ηλεκτρονικό υπολογιστή και αφορούν λειτουργίες και λογισμικό που εκτελείται στον ηλεκτρονικό υπολογιστή. Από εδώ αντλείται σημαντική πληροφορία αναφορικά με την

[169] Βλ. *D. Lupton*, Feeling your data: Touch and making sence of personal digital data, New Media and Society 19 (10), 2017, http://www.researchprofiles.canberra.edu.au/

[170] Βλ. *Αλ. Καργόπουλος*, Ανακριτικές πράξεις επί ψηφιακών δεδομένων: Δικαιικοί άξονες και προβληματισμοί, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 202.

δυνατότητα διαχείρισης και το είδος των δεδομένων που αναμένεται να αντλήσει κανείς, λ.χ. αν υποστηρίζεται λογισμικό για αρχεία κειμένου ή/και εικόνας ήχου.

iii. *δεδομένα διαδικτύου* (internet data), που είναι δεδομένα που αφορούν στην περιήγηση στο διαδίκτυο και την χρήση προσφερομένων σχετικών εφαρμογών. Τα διαδικτυακά δεδομένα, ως αποδεικτικά στοιχεία μπορούν να χωριστούν σε αυτό που είναι διαθέσιμα στο κοινό (π.χ. δημοσιεύσεις φόρουμ, όπου το φόρουμ δεν απαιτεί σύνδεση για προβολή) και σε εκείνα που είναι ιδιωτικά (π.χ. πληροφορίες λογαριασμού Facebook). Μπορεί να υπάρχουν περιθώρια για την απόκτηση και των δύο (π.χ. καταγράφοντας το κείμενο μιας ανάρτησης φόρουμ και κατόπιν ζητώντας τα στοιχεία λογαριασμού του χρήστη που έκανε την ανάρτηση από τον κάτοχο του φόρουμ).

iv. *μεταδεδομένα* (metadata)[171] τα οποία είναι πληροφορίες που ενσωματώνει το εκάστοτε πρόγραμμα στα αρχεία που παράγει. Πρόκειται για πληροφορίες σχετικά με την χρονοσήμανση επεμβάσεων στο αρχείο, όπως η δημιουργία, η προσπέλαση, η τροποποίηση, η διαγραφή, η ανάκτηση, η εκτύπωση, η μεταφορά, η μετακίνηση σε άλλη θέση καθώς και το μέγεθος του αρχείου. Αυτή η μονοσήμαντη πληροφορία μπορεί να δώσει πορισματικό στοιχείο αναφορικά με το μοτίβο διαχείρισης του αρχείου, δηλαδή την συχνότητα επισκεψιμότητάς του, ή την προσπάθεια αλλοίωσης ή εξαφάνισης ιχνών.

v. όταν η αναφορά γίνεται στον ειδικό τομέα των *ηλεκτρονικών επικοινωνιών*[172], τότε στην περίπτωση αυτήν εντοπίζουμε α) τα *δεδομένα κίνησης* (traffic data), τα οποία αναφέρονται στα δεδομένα, που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μίας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται, μεταξύ άλλων, ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή ή και χρήστη, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων, πληροφορίες σχετικά με το πρωτόκολλο, τη μορφοποίηση, τη δρομολόγηση της επικοινωνίας καθώς και το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία,

β) στα *δεδομένα θέσης* (location data), τα οποία αναφέρονται στα δεδομένα, που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μίας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών,

---

[171] Βλ. *Β. Κάτος*, Ψηφιακά Πειστήρια, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 66 επ.
[172] Βλ. σχετικά αρ. 4 Ν 3471/2006 (ΦΕΚ Α 133/28.06.2006), όπως ισχύει, ΒΔ Νόμος.

γ) στα *δεδομένα συνδρομητή* (subscriber data), που είναι στοιχεία αναφορικά με την ταυτότητα του κατόχου[173] ή του χρήστη της υπηρεσίας τηλεπικοινωνιών και αφορούν στο όνομα, επώνυμο, διεύθυνση του προσώπου, αλλά και σε άλλα στοιχεία ταυτοποίησης[174].

δ) στα *δεδομένα περιεχομένου συνομιλιών* (content data), τα οποία αναφέρονται στο περιεχόμενο της επικοινωνίας, είτε αυτό είναι γραπτό (ηλεκτρονικό ταχυδρομείο, μηνύματα), είτε προφορικό[175].

Γ) τεχνικά χαρακτηριστικά και χαρακτηριστικά περιεχομένου των ψηφιακών δεδομένων.

Η ειδική (ψηφιακή) μορφή των δεδομένων, που αποτελούν το αντικείμενο της έρευνας αυτής, τα διαφοροποιεί και στις τεχνικές τους διαστάσεις από εκείνα της υλικής (παραδοσιακής) μορφής των πειστηρίων στην ανακριτική διαδικασία διαμορφώνοντας νέα δεδομένα και αυξημένες απαιτήσεις κατά το στάδιο της ανακριτικής έρευνας.

Τα *τεχνικά* χαρακτηριστικά των ψηφιακών δεδομένων, είναι ένα έτερο επίπεδο αναφοράς, το οποίο επίσης είναι καθοριστικό αναφορικά με τον τρόπο προσέγγισής τους από τον ερευνητή, όταν τα εντοπίσει στα πλαίσια της ανακριτικής έρευνας, κείθεν δε εκκινούν και οι ειδικότερες διαδικασίες διαχείρισής τους για την ασφαλή εξαγωγή και συγκέντρωσή τους.

Στα πλαίσια αυτά σημειώνεται ότι τα ψηφιακά δεδομένα παρουσιάζουν καταρχήν ιδιαίτερη *ευμεταβλητότητα*[176]. Πολύ εύγλωττα θα μπορούσαν χαρακτηριστούν ως ιδιαίτερα εύθραυστα[177] καίτοι η αναφορά σε φθορά και θραύση ταιριάζει σε υλικές δομές. Το ευμετάβλητο στην δομή των ψηφιακών δεδομένων έχει να κάνει με την ιδιαίτερη ευαισθησία τους στην παραμικρή μεταβολή στην χρήση ή στην κατάσταση του μηχανισμού φιλοξενίας (με κάθε έννοιας χρήσης) ή αποθήκευσής τους. Το άνοιγμα ή το κλείσιμο ενός ηλεκτρονικού υπολογιστή φέρει σημαντικές αλλαγές στην προσωρινή μνήμη (RAM) με αποτέλεσμα

[173] Βλ. αρ. 2 περ. 6 ΠΔ 47/2005, σύμφωνα με το οποίο συνδρομητής είναι το φυσικό ή νομικό πρόσωπο, το οποίο έχει συμβληθεί με πάροχο υπηρεσιών ηλεκτρονικών επικοινωνιών ή πάροχο δικτύου επικοινωνιών για την παροχή τέτοιων υπηρεσιών.
[174] Βλ. ΑΔΑΕ 234/2009, ΦΕΚ Β΄ 2359/20.11.2009.
[175] Βλ. Ν 2225/1994, ΦΕΚ Α 121/20.07.1994, ΠΔ 47/2005, ΦΕΚ Α 64/10.03.2005.
[176] Βλ. *Β. Κάτος*, Ψηφιακά Πειστήρια, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ Νομική Βιβλιοθήκη 2019, 66.
[177] Βλ. *Ε. Καρρά – Τανισκίδου*, Δικανική Υπολογιστών (ComputerForensics), 2014, https://core.ac.uk/download/pdf/38466068.pdf

ενδεχόμενα σημαντικές πληροφορίες να αλλοιωθούν με μια απρόσεκτη ενέργεια, που στην διαχείριση μιας απλής συσκευής δεν θα δημιουργούσε αλλαγές.

Το ιδιαίτερα ευπαθές στο τεχνικό status των ψηφιακών δεδομένων μπορεί να οδηγήσει σε τροποποιήσεις ακόμη και με μόνη την απλή συνήθη χρήση ή την επεξεργασία τους. Σαφώς το άνοιγμα ενός αρχείου μπορεί να δώσει νέα μεταδεδομένα που θα αλλοιώσουν την προηγούμενη κρίσιμη προσπέλαση από τον δράστη. Σε άλλη δε περίπτωση ένα εσφαλμένο κατέβασμα αρχείου, καίτοι σαν ενέργεια μαρτυρεί κάτι, θα οδηγήσει τα επί μέρους αρχεία εικόνας ήχου λ.χ. στο χώρο μνήμης που αφορά στα κατακερματισμένα αρχεία, τα οποία ως ατελής αλυσίδα, δεν θα επιτρέψουν την ανάδειξη και πρακτική αξιοποίηση του αρχείου και δεν θα κομίσουν αναφορικά με το στοιχείο αυτό καμιά απόδειξη.

Και βέβαια η χρήση μπορεί να ενέχει πάντοτε και το ενδεχόμενο του σφάλματος, λ.χ. μια απρόσεκτη διαχείριση μπορεί να οδηγήσει σε σβήσιμο του αρχείου (είναι άλλο ζήτημα η δυνατότητα ανάκτησής του) ή σε μεταφορά του σε άλλη τοποθεσία στον ηλεκτρονικό υπολογιστή ή σε μη επιθυμητή διάδοσή του σε τρίτον (λ.χ. ένα εσφαλμένο συνημμένο αρχείο οποιασδήποτε μορφής σε μια σωστή διεύθυνση ηλεκτρονικού ταχυδρομείου [e-mail] ή μια αποστολή σε εσφαλμένη διεύθυνση ηλεκτρονικού ταχυδρομείου).

Στον αντίποδα και σε ένα σχήμα οξύμωρο, τα δεδομένα αυτά χαρακτηρίζονται από *ανθεκτικότητα*, ήτοι μηχανισμούς που διαθέτουν τα ίδια για ανασύσταση και ανασυγκρότηση. Πρόκειται για λειτουργικούς μηχανισμούς άμυνας στην απώλεια των στοιχείων που υπάρχουν εξ ορισμού στο χρησιμοποιούμενο λογισμικό. Αυτή η λειτουργική διάρθρωση του ψηφιακού δεδομένου του δίνει μια δυναμική διατήρησης και ενίσχυσης της υπόστασής του.

Διαφοροποιημένα από τα τεχνικά είναι κάποια *ουσιαστικά* χαρακτηριστικά των ψηφιακών δεδομένων, τουλάχιστον όσον αφορά το στοιχείο της αξιοποίησής τους. Με λίγα λόγια, κάτι εξαχθέν με τεχνικά άρτιο τρόπο, ενδεχόμενα να μην προσφέρει ουσιαστική πληροφορία. Κύριο τέτοιο χαρακτηριστικό τους είναι το γεγονός ότι είναι αμιγώς *περιγραφικά*. Δίνουν ένα μονοσήμαντο περιγραφικό στίγμα αναφορικά με συγκεκριμένο γεγονός, που συνέβη στον ηλεκτρονικό κόσμο, χωρίς αναλυτική, κριτική ή πορισματική προσέγγιση ή ανάδειξη σύνδεσης ή συσχέτισης με άλλα δεδομένα, πλην της πηγής από την οποία εξάγονται κάτι που προκύπτει από τη διαδρομή αναζήτησης και όχι ως πρωτογενής πληροφορία. Όπως είναι απολύτως φυσικό αλλά και λογικά συνεπές, η σημασία της διατήρησης της ακεραιότητας των ψηφιακών δεδομένων είναι ιδιαίτερα σημαντική καθόσον

αποτελεί την βασική προϋπόθεση για την συναγωγή ασφαλούς, κατά το δυνατόν, συμπεράσματος. Από τη στιγμή λοιπόν που το ίδιο το δεδομένο αποδίδει περιγραφικά ένα στοιχείο και όχι σχέσεις και συμπεράσματα, η συσχέτισή του και η συνακόλουθη συναγωγή κάποιου συμπεράσματος, σαφώς και προϋποθέτει σταθερή βάση εκκίνησης. Το ευμετάβλητο ως τεχνικό χαρακτηριστικό των ψηφιακών δεδομένων, που είδαμε κι επισημάναμε παραπάνω, σαφώς και μεταφέρει τον χαρακτήρα του αυτόν και στις σκέψεις, συλλογισμούς και πορίσματα που θα στηριχθούν σε αυτό.

Βέβαια παρά την απλοϊκά αναδειχθείσα περιγραφική διάσταση των ψηφιακών δεδομένων, τα εξ αυτών ουσιαστικά συναγόμενα συμπεράσματα, χωρίς συσχέτισή τους με άλλα δεδομένα είναι σημαντικά και αποτελούν αποδεικτική κατάδειξη πέρα από αυτό που περιγράφει το δεδομένο. Έτσι λ.χ. σε ένα αρχείο εικόνας ήχου σε επίπεδο παιδικής πορνογραφίας (αρ. 348 Α Π.Κ.), η προσπάθεια διαγραφής του σε συγκεκριμένο χρονικό σημείο, πριν ή μετά την πρώτη προσπέλασή του, έχει να καταδείξει στοιχείο αναφορικά με την πρόθεση του χρήστη, κάτι ιδιαίτερα χρήσιμο για την μετέπειτα υπερασπιστική του τακτική.

Δ) το ζήτημα της ασφάλειας στο ψηφιακό περιβάλλον και η ειδικότερη σχέση και αναφορά στα ψηφιακά δεδομένα.

Συνυφασμένη με την αποδεικτική δύναμη των ψηφιακών πειστηρίων, είναι, όπως αναφέρθηκε σε αρκετά σημεία ανωτέρω, η προβληματική της *ακεραιότητάς* τους, προκειμένου η εξ αυτών αναδυόμενη πραγματικότητα να είναι μια πληροφορία ασφαλής για τον σχηματισμό δικανικής πεποίθησης. Η γενικότερη προβληματική αναδεικνύει ως σημαντική πτυχή της αποδεικτικής αξιοποίησής τους και το ζήτημα της ασφάλειας γενικότερα στην διαχείριση της χρήσης του διαδικτύου. Και τούτο τόσο αναφορικά με την προστασία από την διακίνηση προσωπικών δεδομένων[178] κατά τις επικοινωνίες όσο και αναφορικά με την διατήρηση των σχετικών ψηφιακών δεδομένων αναλλοίωτων[179]. Δεν σπανίζουν περιπτώσεις όπου η ανάδειξη αλλοίωσης των ψηφιακών δεδομένων, οδήγησε σε

[178] Βλ. το ενδιαφέρον εστιάζεται στην ελεύθερη ανάπτυξη της προσωπικότητας, στην προστασία της αξίας του ανθρώπου και του συνυφασμένου με τον σεβασμό αυτόν προστατευτικού πλαισίου αναφορικά με την διαφύλαξη του απορρήτου στην επικοινωνία, *Ι. Αγγελή*, Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο, ΠοινΔικ 2001, 1294.

[179] Βλ. *Chr. Stergiou, K. Psannis, B.-G. Kimb, Br. Gupta*, Secure integration of IoT and Cloud Computing, https://www.researchgate.net/profile/Kostas_Psannis/publication/311065854_Secure_Integration_of_Internet-of-Things_and_Cloud_Computing/links/5a44ca35aca272d2945c4b1b/Secure-Integration-of-Internet-of-Things-and-Cloud-Computing.pdf

ανατροπή της δίωξης, η οποία είχε στηριχθεί στο αλλοιωμένο ψηφιακό δεδομένο και στο (συνεπώς) εσφαλμένο αποδεικτικό πόρισμα[180].

Το ζήτημα της *ασφάλειας*[181] στον κυβερνοχώρο σαφώς και είναι από μόνο του ένα μεγάλο τεχνικό κεφάλαιο[182] και μια νομική (πολλές φορές και τεχνική) σπαζοκεφαλιά στον τρόπο με τον οποίον πρέπει να αντιμετωπιστεί. Η επιβολή κυρωτικού κανόνα δικαίου από μόνη της δεν φαίνεται να εξυπηρετεί άριστα το ζητούμενο που είναι η προληπτική προστασία και όχι η κατασταλτική επέμβαση του νόμου, καθόσον λειτουργεί κατασταλτικά και οριακά ενεργεί εγκληματοπροληπτικά. Η παραδοχή ότι ο νόμος παρακολουθεί τις τεχνικές εξελίξεις και τις μεθόδους των δραστών αδυνατώντας[183] να τις προλάβει είναι μια οδυνηρή αλήθεια. Στο μέτρο που κινούμαστε στα απολύτως αναγκαία πεδία αναφέρονται κατωτέρω βασικές περιγραφικές αναφορές για την ασφάλεια στον κυβερνοχώρο αλλά με άμεση συνοχή με την διασφάλιση της ακεραιότητας των ψηφιακών δεδομένων, ώστε να είναι καίρια αλλά και έγκυρη η δικαστική αξιοποίησή τους.

Η ασφάλεια για την οποία γίνεται λόγος ανωτέρω παρίσταται τόσο ως ασφάλεια ενός υπολογιστικού συστήματος (computer system security) με στόχο τη διαφύλαξη των υπολογιστικών πόρων από μη εξουσιοδοτημένη χρήση και την προστασία πληροφορίας, άρα και του σχετικού εξαγωμένου δεδομένου, από ακούσια ή σκόπιμη βλάβη, αποκάλυψη ή τροποποίησή της όσο και ως ασφάλεια κατά την επικοινωνία (communication security): στόχος η προστασία δεδομένων κατά τη μετάδοση σε δίκτυα υπολογιστών και κατανεμημένα συστήματα[184].

Την σημασία στην αξία της ασφάλειας στο περιβάλλον του διαδικτύου την αναδεικνύει και η ύπαρξη διακριτού επιστημονικού τομέα που ασχολείται με την «Ασφάλεια στην Τεχνολογία της Πληροφορίας (IT Security)». Πρόκειται για κλάδο της επιστήμης της πληροφορικής, οποίος ασχολείται με την προστασία των υπολογιστών, των δικτύων που τους συνδέουν και των δεδομένων σε αυτά τα συστήματα, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή χρήση τους.

---

[180] Βλ. Υπόθεση Howze v. Western Express, Inc., 101 Fed. R. Evid. Serv. 107, WL 4180898 (N.D. Ala., 2016.

[181] Βλ. *S. Srinivasan*, Digital Forensics Curriculum in Security Education, Journal of Information Technology Education: Volume 12, 2013 Innovations In Practice, http://www.jite.informingscience.org/ documents/Vol12/JITEv 12IIPp147-157Srinivasan1232.pdf

[182] Βλ. *Σ. Πετρίδου*, Διαρροή Προσωπικών Δεδομένων: Ζητήματα Ασφάλειας, εκπαιδευτικό υλικό σε Τεχνολογίες Πληροφορικής κι Επικοινωνιών/Compus/Uom.

[183] κατά τον *Ι. Αγγελή*, Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο, ΠοινΔικ 2001, 1294, «*ο νομοθέτης δεν «προφταίνει» να παρακολουθεί τις τεχνικές εξελίξεις…*»

[184] Βλ. *Σ. Πετρίδου*, Διαρροή Προσωπικών Δεδομένων: Ζητήματα Ασφάλειας, σε Τεχνολογίες Πληροφορικής κι Επικοινωνιών/Compus/Uom.

Σχετίζεται με θέματα όπως αυτά της *πρόληψης* (prevention), που αφορά στη λήψη μέτρων για να προληφθούν φθορές σε συστατικά ενός πληροφοριακού συστήματος (π.χ. τοποθέτηση κλειδαριάς, κρυπτογράφηση), της *ανίχνευσης* (detection), η οποία αναφέρεται στην λήψη μέτρων για την ανίχνευση του πότε, πώς και από ποιον προκλήθηκε φθορά σε συστατικά ενός πληροφοριακού συστήματος (π.χ. κύκλωμα με κάμερες, αρχεία καταγραφής – log files) αλλά και της *αντίδρασης* (reaction), η οποία σχετίζεται με την λήψη μέτρων για την ανάκτηση ή αποκατάσταση των συστατικών του πληροφοριακού συστήματος (π.χ. κλήση αστυνομίας, επαναφορά αρχείων από backup).

Βασικές, ουσιαστικές αλλά και σωρευτικά συντρέχουσες παράμετροι, οι οποίες επιτρέπουν την δικανική αξιοποίηση των ψηφιακών δεδομένων από την ανακριτική έρευνα, ικανές να στηρίζουν αιτιολογημένα και με ουσιαστικό προσανατολισμό την ανάδειξη της αλήθειας είναι οι ακόλουθες:

i. Η *Εμπιστευτικότητα* (Confidentiality), η οποία αφορά στην αποφυγή μη εξουσιοδοτημένης αποκάλυψης της πληροφορίας. Σύμφωνα με την αρχή αυτήν οι πόροι ενός συστήματος πρέπει να είναι προσπελάσιμοι μόνο από εξουσιοδοτημένες οντότητες. Η προσβολή της συνίσταται στην διαρροή ευαίσθητων πληροφοριών μπορεί να γίνει με πιο παραδοσιακές μεθόδους από την ψηφιακή υποκλοπή, π.χ. με την κλοπή φορητών υπολογιστών από την κατοχή του προσώπου ή της οντότητας, της οποίας δεδομένα διαφυλάσσονται. Ως μέτρα προστασίας προτείνονται ο έλεγχος πρόσβασης και κρυπτογράφηση.

ii. Η *Ακεραιότητα* (Integrity), που αφορά στην αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας. Οι τεχνικοί τρόποι τροποποίησης των πληροφοριακών πόρων ενός πληροφοριακού συστήματος μπορούν να αφορούν στην εγγραφή, αλλαγή, δημιουργία, σβήσιμο δεδομένων. Διατηρείται βέβαια η ακεραιότητα όταν οι ενέργειες αυτές λαμβάνουν χώρα μόνο από εξουσιοδοτημένες οντότητες και στα πλαίσια νόμιμης δράσης.

iii. Η *Διαθεσιμότητα* (Availability), που σχετίζεται με την εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι προσπελάσιμα χωρίς αδικαιολόγητη καθυστέρηση σε εξουσιοδοτημένους χρήστες. Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών (DOS attack).

Για την προστασία όλων των ανωτέρω και στην γενικότερη θεώρηση του ζητήματος της προστασίας των δεδομένων, η νομοθεσία, σε διεθνές αλλά και εθνικό επίπεδο επιβάλλει στους παρόχους ηλεκτρονικών επικοινωνιών την υποχρέωση για λήψη κατάλληλων τεχνικών

και οργανωτικών μέτρων προκειμένου το μεν να αποφεύγονται ή να περιορίζεται ο κίνδυνος από τέτοιες προσβολές, το δε να ενεργοποιούνται σχετικοί μηχανισμοί άμεσης κατά το δυνατόν ενημέρωσης για τα υποκείμενα των δεδομένων.

Μεταξύ των μέτρων αυτών συγκαταλέγονται η χρήση ανεξάρτητων πηγών ενέργειας, παροχή περισσοτέρων διαύλων επικοινωνίας, κατάλληλη παραμετροποίηση υπηρεσιών και η *κρυπτογραφία*. Σκοπός της τελευταίας είναι η διαφύλαξη της ιδιωτικότητας (privacy) αλλά και της εμπιστευτικότητας (confidentiality). Ουσιαστικά πρόκειται για ενέργειες διαφύλαξης με την έννοια της απόκρυψης του περιεχομένου μιας μεταφοράς δεδομένων.

Επιπρόσθετα υποδεικνύεται η αυθεντικοποίηση (authenticity) ή η ακεραιότητα (integrity), που αφορούν στην λήψη προληπτικών μέτρων προσωποποιημένης πληροφορίας αναφορικά με τον αποστολέα δεδομένων, που επιτρέπει στον παραλήπτη, να εξασφαλίζει στοιχεία[185], τα οποία επιβεβαιώνουν την πραγματική «πατρότητα» της αποστολής δεδομένων καθώς και το ότι τα δεδομένα δεν έχουν υποστεί μη εξουσιοδοτημένες και άρα μη νόμιμες, τροποποιήσεις.

Πιο συνήθης στην πράξη είναι η χρησιμοποίηση κλειδιού σε ένα κρυπτογραφικό σύστημα. Οι διάφορες μορφές κρυπτογράφησης αναφέρονται είτε σε δημόσιο κλειδί, είτε σε ιδιωτικό κλειδί είτε σε συνδυασμό δημοσίου και ιδιωτικού κλειδιού. Με τον τρόπο αυτόν τα δεδομένα διακινούνται σε μορφή μη αναγνώσιμη αφού έχει προηγηθεί η κρυπτογράφηση τους, συνήθως σε αλφαριθμητική δομή. Ο αποστολέας και ο παραλήπτης των δεδομένων γνωρίζουν και χρησιμοποιούν ένα κλειδί, το οποίο δεν είναι γνωστό σε τρίτον. Αυτή η περίπτωση αφορά στο συμμετρικό λεγόμενο κλειδί. Σε προηγμένη εκδοχή η κρυπτογραφία διαλαμβάνει την κατοχή ενός ζεύγους κλειδιών, ήτοι ενός δημοσίου κλειδιού, το οποίο δημοσιοποιείται και ενός ιδιωτικού κλειδιού, το οποίο δεν μπορεί να εντοπίζεται μέσα από την χρήση του δημοσίου κλειδιού.

[185] Βλ. *Σ. Πετρίδου*, Διαρροή Προσωπικών Δεδομένων: Ζητήματα Ασφάλειας, σε Τεχνολογίες Πληροφορικής κι Επικοινωνιών/Compus/Uom, όπου η αυθεντικοποίηση εκκινεί από στοιχεία που έχει ο χρήστης είτε από στοιχείο που γνωρίζει (π.χ. password, PIN) είτε από κάτι που κατέχει (π.χ. passport, smart card), αλλά και από χαρακτηριστικά του ίδιου του χρήστη ως τέτοιων νοουμένων και χαρακτηριστικών με την χρήση βιομετρικών (biometric) τεχνικών αναγνώρισης (π.χ. δακτυλικό αποτύπωμα, χαρακτηριστικά προσώπου). Σχετική και η αυθεντικοποίηση από μια πράξη (π.χ. υπογραφή)

8. Η ΚΑΤΑΣΧΕΣΗ ΤΩΝ ΨΗΦΙΑΚΩΝ ΔΕΔΟΜΕΝΩΝ

κατ' αρθρο 265 Κ.Ποιν.Δ.

Προσεγγίζοντας το κεντρικό σημείο της θεματικής της επιστημονικής αναζήτησης, φτάνουμε στην κατάσχεση των ψηφιακών δεδομένων ως ανακριτική πράξη κατά τον Κ.Ποιν.Δ. Οι ιδιαιτερότητες που παρουσιάζει η αναφορά στην κατάσχεση των ψηφιακών δεδομένων, λόγω της ιδιαίτερης (άυλης) φύσης τους, επιβάλλει μια προοδευτική πορεία προσέγγισης σε επίπεδο βήμα – βήμα, ώστε να γίνει περισσότερο ευκρινής και κατανοητή η νομική, πέρα από την τεχνική, ιδιαιτερότητά της. Έτσι εισαγωγικά και μόνο γίνεται μια πρώτη επαφή με την κατάσχεση ως ανακριτική πράξη ενταγμένη στο πλαίσιο της έρευνας της προδικασίας, για την συγκέντρωση αποδεικτικού υλικού, πάντα προς την κατεύθυνση των σκοπών της ανάκρισης κατ' άρθρο 239 Κ.Ποιν.Δ.[186]

i. Η Κατάσχεση ως ανακριτική/ερευνητική πράξη.

Σύμφωνα με τις ρητές αναφορές σε προηγούμενες θέσεις, διαχωρίζουμε την παρακολούθηση της δράσης των πολιτών, που είναι αμιγώς διοικητικής υφής δράση της αστυνομικής αρχής[187], από την δράση των αστυνομικών ως ανακριτικών υπαλλήλων, κατά τα άρθρα 31 και 250 επ. Κ.Ποιν.Δ. Η σημασία της επισήμανσης αυτής, έχει να κάνει με τον θεμελιώδη διαχωρισμό της νόμιμης και της παράνομης συγκέντρωσης αποδεικτικού υλικού. Η (προληπτική) ιχνηλάτηση λοιπόν, με άλλα λόγια η παρακολούθηση της διαδρομής της δράσης χρήστη ως ενδεχόμενη εγκληματική συμπεριφορά στον ψηφιακό χώρο, έχει να κάνει με την παρακολούθηση και ιδίως με τη νομιμότητα και το παραδεκτό αυτής και μόνο με αυτήν. Μόνο όμως η καταγραφή των ενεργειών της αστυνομίας (τμήμα ασφάλειας), που θα λάβει τη μορφή διαβιβαστικού εγγράφου ενεργειών της, μπορεί να αποτελέσει εισαγωγικό στοιχείο του φακέλου, που θα υποβληθεί στην εισαγγελική αρχή για αξιολόγηση. Συνεπώς, δεν μπορεί να λάβει χώρα καμιά *προληπτική* πράξη ανακριτικής έρευνας, ακόμη και αν υπάρχει κίνδυνος να μείνει αναξιοποίητο ή να τύχει απώλειας αποδεικτικό υλικό. Όπως

[186] Βλ. ανωτερω υπό 6. Συνοπτικές Αναφορές στην Δικονομική Διάρθρωση Σχετικά με την Ανακριτική Έρευνα, σελ. 65 και ιδίως 69 επ., όπου και μερικές ενστάσεις αναφορικά με τη νομιμότητα της πρακτικής αυτής.
[187] Βλ. αρ. 11 Ν 4249/2014, ΒΔ Νόμος

εύστοχα παρατηρείται ο νόμος δεν προβλέπει σε καμιά περίπτωση, και συνεπώς δεν ανέχεται, την προκαταβολική εξασφάλιση αποδεικτικού υλικού[188].

Βέβαια η διαχείριση της συμπεριφοράς του δράστη στα στάδια της προπαρασκευής τέλεσης αξιόποινης πράξης ενδιαφέρει την Πολιτεία στο πλαίσιο της ασφάλειας των πολιτών και ενδεχομένως και των θεσμών. Σε καμιά περίπτωση όμως δεν εκκινεί τον μηχανισμό της δικαιοσύνης και της ποινικής καταστολής ή μια επικουρική διεργασία παρόμοια. Πολύ δε περισσότερο στην περίπτωση της υπόνοιας[189] τέλεσης αξιόποινης πράξης, η σχετική απαγόρευση για την συλλογή αποδεικτικού υλικού προκαταβολικά (λ.χ. καταγραφή συνομιλιών κλπ χωρίς προηγούμενη άρση απορρήτου ή χωρίς την ειδική εποπτεία στις περιπτώσεις των ειδικών ανακριτικών πράξεων[190]) δεν μπορεί να αξιοποιηθεί αποκτώντας νομιμοποίηση με την μετέπειτα άσκηση ποινικής δίωξης ή την έκδοση παραγγελίας από τον αρμόδιο εισαγγελικό λειτουργό.

Από τη στιγμή όμως που υπάρξει η παραγγελία από τον εισαγγελικό λειτουργό, τότε οι δράσεις πρέπει να είναι ταχύτατες ώστε να αποφευχθεί ο κίνδυνος απώλειας και της παραμικρής ακόμη αξιοποίησης αποδεικτικής ευχέρειας[191].

Περαιτέρω, η κατάσχεση ως ανακριτική πράξη γενικότερα, αλλά και ειδικά η κατάσχεση ψηφιακών δεδομένων, συνεπάγεται στις πλείστες περιπτώσεις την επιβολή απαγόρευσης διάθεσης ή/και κατοχής, στο ατομικό αγαθό της περιουσίας και της ιδιοκτησίας, μια στέρηση που αναφέρεται πρώτα και κύρια στην φυσική εξουσίαση, άλλως εξουσία διάθεσης και διαχείρισης των συγκεκριμένων ψηφιακών στοιχείων (πειστηρίων, υλικών φορέων και δεδομένων). Απαγόρευση διάθεσης υπάρχει ακόμη και όταν με την διαδικαστική πράξη της κατάσχεσης δεσμεύεται το αντικείμενο νομικά και ως προς την φυσική του κατοχή και χρήση κατά τον τρόπο που προορίζεται αλλά ως φυσική υπόσταση παραμένει στον χώρο οριζομένου του ιδιοκτήτη (κατηγορουμένου ή υπόπτου) ως μεσεγγυούχου. Στην περίπτωση δε της αφαίρεσής του και της φύλαξής του από την αρμόδια

---

[188] Βλ. *Θ. Δαλακούρας*, Ποινικό Δίκαιο τόμος Ι, 2012, σελ. 192, *Π. Παναγιωτόπουλος*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 1540.

[189] Βλ. ΓνωμΕισΑΠ 2032/1994,

[190] Βλ. *Θ. Δαλακούρας*, Ειδικές ανακριτικές πράξεις κατ' αρ. 253 Α ΚΠΔ και ηλεκτρονικό έγκλημα, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2018, 247 επ., *ίδιος*, Οι ειδικές ανακριτικές πράξεις του άρθρου 6 του Ν 2928/2001, ΠοινΧρ 2001, 1022, *Μ. Καϊάφα – Γκμάντι*, Η πρόσφατη νομολογία του ΕΔΔΑ για την αστυνομική διείσδυση και το δικαίωμα σε δίκαιη δίκη, ΠοινΧρον 2011, 59 επ., *Ν. Λίβος*, Το Οργανωμένο έγκλημα, έννοια και δικονομικοί τρόποι αντιμετώπισης του, σε Το οργανωμένο έγκλημα από τη σκοπιά του ποινικού δικαίου, Πρακτικά Ζ' Πανελ. Συνεδρ. ΕΕμπΔ 2000, 17.

[191] Διατηρεί την σημασία της, με τον ιδιαίτερο τρόπο διατύπωσής της, η θέση «*... αι πρώται ώραι είναι ανεκτίμητοι, ο δε παρερχόμενος χρόνος είναι η αλήθεια που φεύγει*» [Χ. Γιώτης, Ανακριτική μετά 26 χρόνων, εν Αθήναις, τύποις: «ΕΛΛΑΣ», 1934, σελ. 364-5] ως παράθεση από τον *Π. Παναγιωτόπουλο*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 1535.

αρχή, τότε έχουμε την περίπτωση και της απώλειας της κατοχής, που προστίθεται στην απαγόρευση νομικής και πραγματικής λειτουργικής διαχείρισης του αντικειμένου που κατασχέθηκε.

Με την ανωτέρω δομή της η κατάσχεση εντάσσεται στις αναφερόμενες ως έχουσες *επαχθή* χαρακτήρα διαδικαστικές πράξεις και κατατάσσεται λόγω του χαρακτήρα της αυτού στα *«μέτρα δικονομικού καταναγκασμού»*[192]. Ανάλογα ανακριτικά μέτρα, που χαρακτηρίζονται από το στοιχείο της προσβολής, στα όρια της αποστέρησης απόλαυσης, σημαντικής ατομικής ελευθερίας, είναι η σύλληψη, η προσωρινή κράτηση (που στρέφονται κατά της ελευθερίας), της κατ' οίκον έρευνας (που στρέφεται κατά της οικιακής ειρήνης και του οικιακού ασύλου). Σημαντικό στοιχείο είναι ο προσανατολισμός στην επιβολή του μέτρου να αφορά στην εξυπηρέτηση του ανακριτικού σκοπού (αρ. 239 Κ.Ποιν.Δ) και να μην αποτελεί σε καμιά περίπτωση η επιβολή των μέτρων αυτών «προκαταβολή» κολασμού, άλλως «προτιμωρητικό» καταναγκασμό[193].

Οι παραδοσιακές προσλαμβάνουσες παραστάσεις αναφορικά με τα εγκληματολογικά πειστήρια, που αφορούσαν σε έγγραφα, υλικά αντικείμενα (οχήματα, όπλα κλπ), τραπεζογραμμάτια (ημεδαπά ή αλλοδαπά), τιμαλφή, λοιπά στοιχεία δηλωτικά αξιών κλπ. καλύπτονταν επαρκώς από το σχετικό πλέγμα διατάξεων του Κ.Ποιν.Δ. αναφορικά με την κατάσχεση, ως μέτρο δικονομικού καταναγκασμού στα πλαίσια εξασφάλισης αποδεικτικού υλικού, πάντοτε για την εξυπηρέτηση των αναγκών της προδικασίας και της ανακριτικής έρευνας. Προβληματισμός βέβαια ανέκυψε αναφορικά με τα ψηφιακά δεδομένα, που με την άυλη υπόστασή τους, σαφώς δεν επέτρεπαν λογικές υπαγωγής στις διατάξεις του Κώδικα που ρύθμιζαν ζητήματα κατάσχεσης σε αντικείμενα με υλική υπόσταση. Και τούτο ήταν προφανές[194].

Την λύση αναφορικά με τον προβληματισμό σχετικά με την αναγκαιότητα επιβολής ενός μέτρου δικονομικού καταναγκασμού, όπως στην περίπτωσή μας είναι η κατάσχεση των ψηφιακών πειστηρίων από τα οποία αντλούνται τα ψηφιακά δεδομένα, την έδινε η θεωρία αλλά και η νομολογία, όταν καλούνταν να αξιολογήσει σχετικές προσφυγές κατηγορουμένων επί διατάξεων ανακριτών ή προβολής ισχυρισμών ακυροτήτων, στην βάση της προσβολής ή

[192] Έτσι και *Ν. Χωραφάς*, Ποινικόν Δίκαιον, τομ. 1ος, εκδ. 9η, 1978, σελ. 184, *Θ. Δαλακούρας*, Αρχή της αναλογικότητας και μέτρα δικονομικού καταναγκασμού, 1993, *Π. Παναγιωτόπουλος*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 1534.

[193] Βλ. *Ν. Ανδρουλάκης*, Τα όρια της ανακριτικής δράσεως και η αρχή της «αναγκαιότητας», ΠοινΧρον 1975, σελ. 15 επ.

[194] Βλ. μεταξύ άλλων και *Θ. Δαλακούρας*, Νέος Κώδικας Ποινικής Δικονομίας, συνοπτική ερμηνεία κατ' άρθρο, Νομική Βιβλιοθήκη 2019, σελ. , *Λ. Μαργαρίτης*, Νέος Κώδικας Ποινικής Δικονομίας, Αιτιολογική έκθεση Ν 4620/2019, Νομική Βιβλιοθήκη, σελ. 383.

μη της αρχής της αναλογικότητας και της αρχής της αναγκαιότητας[195]. Αυτά ως προς την δυνατότητα (αναγκαιότητα) επιβολής της κατάσχεσης. Ως προς την πρακτική της εκτέλεση, η δογματική πρόταση, που ακολουθούνταν αφορούσε την ένταξη των ψηφιακών δεδομένων στην έννοια των εγγράφων και αναλογικά γινόταν η σχετική εφαρμογή των διατάξεων του Κώδικα.

Πλέον με το Ν 4620/2019, δόθηκε άλλη διάσταση στο νομικό πλαίσιο, που αφορά στην κατάσχεση ψηφιακών πειστηρίων, μέσα από την εναρμόνιση της εθνικής νομοθεσίας με τις διεθνείς συμβάσεις αλλά και συνταγματικές επιφυλάξεις υπέρ του νόμου αναφορικά με την περιστολή ατομικών ελευθεριών. Επιπρόσθετα, με την ισχύουσα δομή της διάταξης του άρθρου 239 Κ.Ποιν.Δ, δόθηκε ρητή πλέον διατύπωση στην υποχρέωση τήρησης των παραπάνω αρχών, σκοπού και αναλογικότητας, στην ανακριτική διαδικασία και ιδιαίτερα στην επιβολή των μέτρων δικονομικού καταναγκασμού. Φυσικά η κρίση ανήκει στην αναφαίρετη ανεξαρτησία του ανακριτή ως δικαστή, που είναι επιφορτισμένος, πάντα μετά από γνώμη του εισαγγελέα, να διατάξει το μέτρο, μόνο που πλέον είναι σαφής η σχετική νομοθετική και όχι απλά δικαιική δέσμευσή του.

ii. Η Κατάσχεση των ψηφιακών δεδομένων κατά τον ΕλλΚ.Ποιν.Δ. Οι πρώτοι προβληματισμοί.

Η ιδιαιτερότητα των ψηφιακών δεδομένων αλλά και γενικότερα οι ερευνητικές απαιτήσεις στην εξιχνίαση του ηλεκτρονικού εγκλήματος (με κάθε έννοια και μορφή του στην βάση των όσων αναπτύχθηκαν ανωτέρω στην σχετική θέση[196]) ως απλή λογική επέβαλαν την θεσμοθέτηση ειδικού πλαισίου διατάξεων που να ρυθμίζουν το συγκεκριμένο δικονομικό μέτρο. Προοδευτικά με το Ν 4411/2016 άρχισε η υλοποίηση και της συμβατικής δέσμευσης της χώρας μας για την σχετική προσθήκη στην ποινική διαδικασία, που σαφώς έχει μορφή εκσυγχρονισμού και εναρμόνισης με άλλα ευρωπαϊκά δικονομικά συστήματα, με προσανατολισμό πάντα την δίωξη κι εξιχνίαση του ηλεκτρονικού εγκλήματος στα πλαίσια μιας συντονισμένης δυναμικής και συνεργασίας αρχών.

Ο νομικός καθορισμός των πλαισίων διαχείρισης στα θεσμικά όρια της ανακριτικής έρευνας, των ψηφιακών δεδομένων, που σχετίζονται με κάθε έγκλημα αλλά ειδικότερα με

[195] Βλ. *Αργ. Καρράς*, Η αναίρεση στην Ποινική Δίκη, εκδ. Σάκκουλα, Αθήνα – Θεσσαλονίκη 2013, [αναγκαιότητα σελ. 232], [ειδικές ανακριτικές πράξεις σελ. 231, 235, 237]
[196] Βλ. ανωτέρω υπό 2. Γενικές Αναφορές στο Ηλεκτρονικό Έγκλημα. *i. Εννοιολογικός προσδιορισμός του ηλεκτρονικού εγκλήματος*, σελ. 22 επ.

συμπεριφορές που εντάσσονται στην έννοια του ηλεκτρονικού εγκλήματος, ρυθμίζεται από την διάταξη του άρθρου 265[197] του νεοπαγούς Κ.ΠοινΔ. Έτσι:

α. Κατά την εισαγωγική δομή της διάταξης του άρθρου 265, καθορίζονται τα ψηφιακά πειστήρια στα οποία μπορεί να αναζητηθούν δεδομένα ως αποδεικτικά στοιχεία για την εξιχνίαση του ηλεκτρονικού εγκλήματος. Εφόσον δε εντοπιστούν τέτοια στοιχεία και κριθεί αναγκαίο για την ανακριτική έρευνα, δύναται να επιβληθεί κατάσχεση ψηφιακών δεδομένων.

Η λογική του πράγματος αναδεικνύει ότι η όποια σχετική κατάσχεση ψηφιακών πειστηρίων και δεδομένων σαφώς και θα είναι η κατάληξη της συνδυαστικής λειτουργίας της αστυνομικής έρευνας (του αρ. 96 επ. ΠΔ 141/1991 και αρ. 11 Ν 4249/2014), η οποία

[197] Βλ. «Άρθρο 265. - Κατάσχεση ψηφιακών δεδομένων. 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.»

αξιοποίησε ενδεχομένως πληροφορίες, εντοπίστηκαν και τέθηκαν υπόψη της παράνομες συμπεριφορές στο διαδίκτυο, εντόπισε τα σχετικά ίχνη τέλεσης ηλεκτρονικού εγκλήματος, ενήργησε τις σχετικές εξακριβώσεις, συγκέντρωσε στοιχεία κι ενημέρωσε σχετικά τον αρμόδιο εισαγγελέα, ο οποίος με την σειρά του εξέδωσε την σχετική παραγγελία για την ανακριτική πλέον έρευνα.

β. Τα ζητήματα που ξεκινούν μετά την παραγγελία του εισαγγελέα, έχουν να κάνουν με τις ενέργειες, οι οποίες πρέπει να προηγηθούν της όποιας επέμβασης των αστυνομικών, δρώντων πλέον ως ανακριτικών υπαλλήλων. Είναι σαφές ότι *«δικαίωμα σφάλματος» δεν* υπάρχει στις ενέργειες της δικαστικής εξουσίας και των διωκτικών αρχών. Και όταν γίνεται λόγος για σφάλμα, εννοείται ότι αναφερόμαστε στην νομική και νομιμοποιητική δομή και βάση των πρακτικών και μεθόδων της έρευνας. Συνακόλουθα οι όποιες ενέργειες των αστυνομικών – ανακριτικών υπαλλήλων στα πλαίσια της έρευνας θα πρέπει να έχουν σταθερή κι έγκυρη νομιμοποιητική βάση, σε βαθμό που δεν επιτρέπει επισφάλεια και δεν επιδέχεται αμφισβήτηση.

Μόνη η κατ' άρθρο 11 Ν 4249/2014 πρόβλεψη ότι η αστυνομική αρχή χρησιμοποιεί επιστημονικές και τεχνικές μεθόδους διαλεύκανσης των εγκλημάτων και διαθέτει εγκληματολογικά εργαστήρια, τα οποία παρέχουν τις υπηρεσίες τους και σε άλλες αρχές, δεν μπορεί να αποτελέσει νομιμοποιητική βάση για την οποιαδήποτε δράση της αστυνομίας. Η συγκεκριμένη διάταξη αναφέρεται στα μέσα, που δύναται να χρησιμοποιεί η αστυνομική αρχή για την επίτευξη των θεσμικών στόχων της, όχι όμως και το πότε η χρήση τους βασίζεται σε ορθή νομιμοποιητική βάση. Τα ίδια ισχύουν και αναφορικά με την πρόβλεψη του άρθρου 96 ΠΔ 141/1991 αναφορικά με τις ενέργειες που διαλαμβάνει η αστυνομική έρευνα. Εκεί λ.χ. παρατηρούμε ότι για μια νόμιμη κατ' οίκον έρευνα απαιτείται η προηγούμενη συναίνεση (όχι έγκριση) του ενοίκου και συνεπώς η μη ρητή συναίνεσή του τερματίζει την, σε συγκεκριμένη χρονική στιγμή, προσπάθεια της αστυνομικής έρευνας, τουλάχιστον για αναζήτηση στον χώρο της οικίας.

Περαιτέρω η έρευνα σε ηλεκτρονικές επικοινωνίες, δεν φαίνεται να μπορεί να ενσωματωθεί και υπαχθεί μέσα στην θεματική των αστυνομικών ερευνών του άρθρου 96 ΠΔ 141/1991[198]. Η απλή δε αναφορά στα μέσα που χρησιμοποιεί η αστυνομική αρχή, δεν δίνει επίσης ξεκάθαρη εικόνα για το αποτέλεσμα στο οποίο μπορεί να εξυπηρετήσουν αυτά στα πλαίσια μια αναζήτησης ενός ηλεκτρονικού εγκλήματος.

[198] Εν όψει και του ειδικότερου νομικού πλαισίου του Ν 2225/1994.

Εύλογα προκύπτει ως ερώτημα το τί είναι εκείνο το οποίο θα αποτελέσει την απαρχή για μια εισαγγελική παραγγελία, που θα ανοίξει τον δρόμο στην ανακριτική έρευνα για την εξιχνίαση του ηλεκτρονικού εγκλήματος;

iii. Η προσπάθεια για λήψη εισαγγελικής παραγγελίας για την έναρξη της ανακριτικής έρευνας. Η προβληματική της πρώτης πληροφόρησης για την διάπραξη ηλεκτρονικού εγκλήματος.

α. Θα μπορούσε να αποτελέσει απάντηση στο ερώτημα, με το οποίο κατέληξε η προηγούμενη ενότητα, η αξιοποίηση πληροφοριών, που περιήλθαν σε γνώση της αστυνομικής αρχής; Η συγκεκριμένη αναφορά με την μορφή στερεότυπης δομής στις μαρτυρικές καταθέσεις, που συνθέτουν το πρώιμο ανακριτικό υλικό από τους αστυνομικούς υπαλλήλους που εξετάζονται ως μάρτυρες, ιδίως στις υποθέσεις ναρκωτικών, δεν μπορεί να αποτελέσει πειστική απάντηση. Η πληροφορία στο κοινό έγκλημα, προκειμένου να καταστεί αξιοποιήσιμο μέγεθος επιβάλλεται να έχει μια ελάχιστη αναγκαία πραγματική βάση, η οποία μπορεί να προκύψει, ή μάλλον να ενισχυθεί, εφόσον είναι ισχνή, από την εξέταση του αστυνομικού υπαλλήλου του αντιστοίχου τμήματος (λ.χ. Τμήμα Δίωξης Ναρκωτικών). Έτσι, το αντικειμενικό *τίποτα* μπορεί να καταστεί πρακτικά *κάτι*. Μια αόριστη και ενδεχόμενα ανύπαρκτη πληροφορία, εμφιλοχωρούσα στην μαρτυρική κατάθεση του αστυνομικού υπαλλήλου, φερομένη ως πρώτο έναυσμα για την έρευνα, μπορεί, ίσως θα πούμε εδώ, να νομιμοποιήσει μια καθόλα παράνομη έρευνα.

Την σημασία της φήμης, άλλως της πληροφόρησης, την αντιμετώπισε με σκεπτικισμό ο νομοθέτης κι έτσι στην διάταξη του άρθρου 224 Κ.Ποιν.Δ[199]. Τόσο στην ισχύουσα όσο και στην παλαιότερη διατύπωσή της, αξιώνοντας από εκείνον που καταθέτει βάσει πληροφόρησης και όχι από άμεση αντίληψη, να δηλώνει τα στοιχεία της πηγής της πληροφόρησης. Η διαφοροποίηση της νέας διάταξης από την παλαιότερη εκδοχή της, είναι η επιφύλαξη υπέρ του ειδικότερου νόμου αναφορικά με την υποχρέωση του μάρτυρα να κατονομάσει την πηγή της πληροφόρησης. Πρόκειται για διαφοροποίηση η οποία ήρθε να καλύψει νομοθετικά εκείνο που μέχρι σήμερα ενεργούσε νομολογιακά η δικαστηριακή πρακτική. Η αρχική λοιπόν απαγόρευση της κάλυψης της πηγής πληροφόρησης, δεν

[199] Βλ. άρθρο 224 Κ.Ποιν.Δ. «- *Πώς έμαθε ο μάρτυρας όσα καταθέτει. Ο μάρτυρας πρέπει να αποκαλύπτει πώς έμαθε όσα καταθέτει. Αν πρόκειται για γεγονότα που άκουσε από άλλους, πρέπει σε κάθε περίπτωση να κατονομάσει ταυτόχρονα και εκείνους από τους οποίους τα άκουσε, εκτός αν στο νόμο ορίζεται διαφορετικά. 2. Αν ο μάρτυρας δεν κατονομάζει την πηγή των πληροφοριών του, η κατάθεσή του δεν μπορεί να ληφθεί υπόψη*.»

προέβλεπε εξαίρεση για τις καταθέσεις των αστυνομικών[200], που στην τεχνική τους διάρθρωση ξεκινούσαν πανομοιότυπα, με εκφράσεις του τύπου «*ύστερα από αξιοποίηση πληροφοριών…*» ή «*από πληροφορίες που περιήλθαν στην υπηρεσία…*» και άλλα όμοια. Η επικείμενη δε κύρωση της απαγόρευσης αξιοποίησης[201] της μαρτυρικής αυτής κατάθεσης κατά το αρ. 224 § 2 Κ.Ποιν.Δ., δημιουργούσε έντονες και εύλογες αποδεικτικές αδυναμίες στις υποθέσεις καθόσον σταθερά οι μάρτυρες απόδειξης αστυνομικοί και στην επ' ακροατηρίω κατάθεσή τους απέφευγαν να αποκαλύψουν την πηγή της πληροφόρησής τους, στερώντας από τον κατηγορούμενο και την υπεράσπισή του δυνατότητα ανάδειξης σφαλμάτων στην συγκέντρωση του αποδεικτικού υλικού. Ωστόσο μια ποινική δίκη ήταν σε εξέλιξη βάσει μιας μη αξιοποιήσιμης μαρτυρικής κατάθεσης, που όμως ήταν ίσως το μοναδικό αποδεικτικό στοιχείο στο οποίο μπορούσε να στηριχθεί η παραγγελία του εισαγγελέα. Πλέον η ρήτρα επικουρικότητας[202] του αρ. 224 § 1 Κ.Ποιν.Δ., ενισχύει το διωκτικό έργο της αστυνομίας, νομιμοποιεί την απόκρυψη της πηγής της πληροφόρησης, χωρίς όμως να παρέχονται οι εγγυήσεις που αποκλείουν σε λογική βάση, τις σκέψεις περί νομιμοποίησης παρανόμως κτηθέντων αποδεικτικών στοιχείων.

Πολύ δε περισσότερο τέτοιες πρακτικές δεν φαίνεται να μπορούν πειστικά να αποτελέσουν πρώιμη έρευνα στον χώρο του ηλεκτρονικού εγκλήματος. Η πληροφόρηση, ως σοβαρή ένδειξη διάπραξης αξιόποινης συμπεριφοράς, στο ηλεκτρονικό έγκλημά δεν μπορεί παρά να προέρχεται από τον ψηφιακό κόσμο. Ποια η αξιοπιστία μιας κατάθεσης (προστατευμένης πηγής πληροφόρησης) ότι ο Χ ετοιμάζεται να κατεβάσει και διαμοιράσει αρχείο εικόνας – ήχου με παιδική πορνογραφία; ή ότι ενεργεί αποστολές ηλεκτρονικών μηνυμάτων στην δομή του phishing; Όταν μάλιστα ο ίδιος δεν θα είναι σε θέση να δώσει υλικό που να αποδεικνύει την καταγγελλόμενη συμπεριφορά; Τί θα ήταν πρακτικά εκείνο, το οποίο θα μπορούσε να δικαιολογήσει (όχι να νομιμοποιήσει) ρεαλιστικά και πρακτικά μια τέτοια πληροφόρηση;

Κάτι τέτοιο θα μπορούσε να εξυπηρετήσει η παρακολούθηση (προφανώς και σε πραγματικό χρόνο) ηλεκτρονικών επικοινωνιών σε όλες τις διαστάσεις και τεχνικές

---

[200] Βλ. Για τους σχετικούς προβληματισμούς αναφορικά με την υποχρέωση ή μη της αποκάλυψης της πηγής της ενημέρωσης του μάρτυρα σε *Ε. Τσαγκαράκης*, ο μάρτυρας εξ ακοής στην ποινική δίκη, ΠοινΔνη 2010, 725, *Π. Μπρακουμάτσος*, Ερμηνευτικές παρατηρήσεις και προτάσεις στο Ν 2408/1996, ΠοινΧρον 1996, 1193, *Π. Καίσαρης/Σ. Τσάκος*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 1320-1.

[201] Βλ. *Λ. Μαργαρίτης*, Οι δικονομικού περιεχομένου διατάξεις του Ν 2408/1996, Υπερ 1997, 519.

[202] Η οποία πρέπει να αναγιγνώσκεται σε συνδυασμό με τις διατάξεις των άρθρων 254 (ειδικές ανακριτικές πράξεις επί ορισμένων εγκλημάτων) και 255 (ειδικές ανακριτικές πράξεις επί εγκλημάτων διαφθοράς) Κ.Ποιν.Δ.

δυνατότητες. Είναι όμως κάτι τέτοιο νομικά επιτρεπτό; Προβλέπεται δυνατότητα της αστυνομικής αρχής να παρακολουθεί ποιος επικοινωνεί, πού, με ποιόν, πόσο (στοιχεία θέσης και κίνησης)[203] και ποιο είναι το περιεχόμενο της επικοινωνίας; Μπορεί η παρακολούθηση αυτή να γίνεται σε πραγματικό χρόνο[204];

Ναι! Θα απαντούσε κανείς, αν βέβαια δεχόμασταν ότι η αστυνομία μπορεί, στο όνομα του έργου της πρόληψης τέλεσης αξιοποίνων πράξεων, να ισοπεδώνει κάθε νομοθετικό κείμενο και κάθε αρχή δικαίου, ξεκινώντας από το ίδιο το Σύνταγμα και τις Διεθνείς Συμβάσεις, που λειτουργούν στο εσωτερικό δίκαιο ως νόμοι αυξημένης τυπικής ισχύος, όπως η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου, που ισχύει όπως τροποποιήθηκε από τα Πρωτόκολλα υπ' αριθ. 11 και 14 συνοδευόμενη από τα Πρωτόκολλα υπ' αριθ. 1, 4, 6, 7, 12, 13 και 16 και τα εξ αυτών των νομοθετημάτων εξαγόμενα νομικά στοιχεία που διαμορφώνουν, μεταξύ άλλων, τις αρχές του δικαίου και τα ατομικά δικαιώματα.

Όπως θα δούμε και παρακάτω, η πρακτική της αστυνομίας, ήταν (και εν μέρει διατηρείται) η υποβολή ψηφιακού αιτήματος για λήψη αρχείου που παρέπεμπε είτε βάσει της ονομασίας του είτε βάσει της μορφής και των διαδρομών διαμοιρασμού του, σε αξιόποινο περιεχόμενο. Σχετική ήταν η χρήση του λογισμικού TLO[205]. Με τον τρόπο αυτόν η αστυνομική αρχή «έβλεπε» σε ποιες IP γινόταν ο σχετικός διαμοιρασμός στις peer2peer εκδοχές και η συναφής κατοχή του αξιόποινου αρχείου. Με τον τρόπο αυτόν, ουσιαστικά παρακολουθούσε την δράση στο διαδίκτυο. Ερωτήματα τίθενται αναφορικά με την νομιμότητα της πρακτικής αυτής, που ναι μεν εντάσσεται στη λογική της εξ ορισμού διάδρασης στο διαδίκτυο, δεν παύει όμως να αποτελεί μια ενέργεια κεκαλυμμένης έρευνας[206].

β. Η πρακτική έχει αναδείξει ότι για την στήριξη μιας αίτησης για έρευνα η αστυνομική αρχή αιτείται, πριν από οτιδήποτε, την *άρση του απορρήτου των επικοινωνιών*.

---

[203] Βλ. αρ. 2 §§ 3 και 4 Ν 3471/2006, ΦΕΚ Α 133/28.06.2006, «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997.», όπως ισχύει μετά τις τροποποιήσεις που επέφερε ο Ν 4070/2012 (ΦΕΚ Α 82/20.04.2012).

[204] Βλ. αρ. 3 § 1 ΠΔ 47/2005 (ΦΕΚ Α 64/10.03.2005).

[205] Βλ. κατωτέρω υπό 9. Οι αρχές που διέπουν την έρευνα αναφορικά με τα ψηφιακά πειστήρια και τα ψηφιακά δεδομένα, *ii. Οι Αρχές που διέπουν την ανακριτική έρευνα ως ερευνητική προσέγγιση της μελέτης, Α) Η αρχή της νομιμότητας*, σελ. 159.

[206] Η νομιμοποίησής της για τις ειδικές κατηγορίες εγκληματικής δράσης στην περίπτωση των άρθρων 254 και 255 Κ.Ποιν.Δ., είναι ένα άλλο ζήτημα, διότι αν αρκούσε αυτή η νομική υποδοχή τότε η παραπομπή στις συγκεκριμένες διατάξεις θα ήταν ρητή. Επιπρόσθετα και πάλι λύση δεν δίδεται ακόμη κι έτσι καθόσον στο χρονικό σημείο που γίνεται η προσποίηση αυτή δεν υπάρχει εισαγγελική εντολή για έναρξη ανακριτικού πεδίου έρευνας.

Στον εισαγγελέα λοιπόν υποβάλλεται αίτηση για την ενεργοποίηση της διαδικασίας του Ν 2225/1994. Πρόκειται για διαδικασία, που παρά τις εγγυήσεις που παρέχει η παρέμβαση δικαστικού σχηματισμού (Δικαστικού Συμβουλίου) ή σε όλως εξαιρετικά επείγουσες περιπτώσεις η επέμβαση του αρμοδίου εισαγγελέα[207], δεν παύει να συνιστά *νομιμοποίηση* μιας επέμβασης στον σκληρό πυρήνα ατομικών ελευθεριών, όπως στην ιδιωτική ζωή, στην ελευθερία της έκφρασης και στα προσωπικά δεδομένα. Το γεγονός ότι αγγίζει ιδιαίτερα ευαίσθητες περιοχές και δικαιώματα, κατά κύριο λόγο, συνυφασμένα με την ιδιωτικότητα αλλά και τον αυτοκαθορισμό του ατόμου ως κοινωνική μονάδα ενταγμένη σε σύνολο και κοινωνικά υποσύνολα, επιβάλλει την συσταλτική ερμηνευτική προσέγγιση των ενδεχομένων *γκρίζων ζωνών*, που πρακτικά ή λογικά ανακύπτουν κατά την εφαρμογή του ειδικού αυτού νομοθετήματος.

Ας μην λησμονείται επίσης το γεγονός ότι πολύς επιστημονικός λόγος αναλώθηκε για ζητήματα που σχετίζονται με τα στοιχεία επικοινωνίας, που καλύπτονται από το απόρρητο της επικοινωνίας και οι ενστάσεις και αντενστάσεις αναφορικά με την διατήρηση και διάθεση[208] σε στοιχεία επικοινωνίας όπως είναι τα εξωτερικά στοιχεία της επικοινωνίας, η ανάδειξη της ταυτότητας του καλούντος κλπ, δεν είχαν ξεκάθαρη και από μιας αρχής και αναντίρρητη αντιμετώπιση. Σημαντική, στην σχετική εξέλιξη του επιστημονικού λόγου αναφορικά με τα κρίσιμα αυτά ζητήματα, ήταν η παρέμβαση του Αρείου Πάγου και ειδικότερα της Εισαγγελίας του Ανωτάτου Ακυρωτικού[209] αλλά και με σχηματισμό Δικαστηρίου του Αρείου Πάγου[210], όχι χωρίς επιστημονικό αντίλογο[211].

Παρατίθεται απλά για το ενιαίο της αναφοράς ότι στα πλαίσια ενός εννοιολογικού καθορισμού, κατά τις νομολογιακές παραδοχές αλλά κι εκείνες τις θεωρητικές απόψεις, τα *δεδομένα θέσης* υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη (γεωεντοπισμός), ενώ τα *δεδομένα κίνησης* αφορούν στα εξωτερικά στοιχεία της επικοινωνίας, τα οποία έχουν να κάνουν με πληροφορίες αναφορικά με στοιχεία καλούντος και καλουμένου, τον αριθμό, τη διεύθυνση, την ταυτότητα της σύνδεσης ή του τερματικού

[207] Βλ. αρ. 4 § 6 Ν 2225/1994.
[208] Βλ. Ν 3917/2011 (ΦΕΚ Α 22/21.02.2011), «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημοσίους χώρους και συναφείς διατάξεις». Πρόκειται για ισχύον νομοθέτημα, το οποίο ενσωμάτωσε στην ελληνική έννομη τάξη την Οδηγία 2006/24/ΕΚ. Σημειώνεται ότι η Οδηγία αυτή κηρύχθηκε ανίσχυρη με την απόφαση του ΔΕΕ της 08.04.2014 C-293/2012 και C-594/2012 «Digital Rights Ireland Ltd.» (ΔiΜΕΕ 3/2014, σελ. 359).
[209] Βλ. ΓνωμΕισΑΠ 2/2017, ΒΔ Νόμος, ΓνωμΕισΑΠ 9/2009, ΒΔ Νόμος.
[210] Βλ. ΠλΟλΑΠ 1/2017, ΒΔ Νόμος.
[211] Βλ. ΑΔΕΑ 1/2005, http://www.adae.gr/fileadmin/docs/nomoi/893-2005.pdf.

εξοπλισμού του συνδρομητή ή και χρήστη, τους κωδικούς πρόσβασης, τα δεδομένα θέσης, την ημερομηνία και ώρα έναρξης και λήξης και τη διάρκεια της επικοινωνίας, τον όγκο των διαβιβασθέντων δεδομένων, πληροφορίες σχετικά με το πρωτόκολλο, τη μορφοποίηση, τη δρομολόγηση της επικοινωνίας καθώς και το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία[212].

Σαφώς η διάταξη του άρθρου 4 Ν 2225/1994, όπως ισχύει, περιλαμβάνει πολλά αδικήματα, κακουργηματικής τάξης, που καλύπτουν σημαντικό μέρος αν όχι το σύνολο από το φάσμα της σοβαρής, και δη της ηλεκτρονικής, εγκληματικότητας. Μάλιστα η εφαρμογή της επεκτείνεται και στα πειθαρχικά αδικήματα[213].

Περαιτέρω όμως μη συμβατή με το όλο πνεύμα της αρχής της αναγκαιότητας, του σκοπού και της αναλογικότητας, παρίσταται η δυνατότητα μέσα από το αρ. 5 § 6 Ν 2225/1994 να διατηρούνται τα δεδομένα μέχρι και για 10 μήνες, όταν στην βασική διάταξη για την ανακριτική έρευνα ο Κ.Ποιν.Δ. (αρ. 239 § 2) θεσμοθετώντας την αρχή της αναλογικότητας, δίνει σταθερή παράμετρο την οποία δεν μπορεί να υπερβεί ο εφαρμοστής του νόμου.

Έτερο ζήτημα που πρέπει να τύχει σχετικής ερμηνευτικής προσέγγισης είναι εκείνο του κατά πόσο οι σχετική δυνατότητα για τις υπό εγγυήσεις άρση του απορρήτου επιτρέπουν και την καταγραφή και αποτύπωση των δεδομένων περιεχομένου επικοινωνίας σε υλικό φορέα[214].

Ακόμη κι έτσι όμως η βασική προβληματική που απασχολεί εδώ παραμένει. Η απαίτηση του αρ. 4 § 3 Ν 2225/1994 για άρση του απορρήτου μόνο στις περιπτώσεις που *αιτιολογημένα* διαπιστώνεται ότι η διερεύνηση της υπόθεσης ή της εξακρίβωσης του τόπου διαμονής του κατηγορουμένου είναι *αδύνατη ή ουσιωδώς δυσχερής* χωρίς αυτήν, διατηρεί τον αρχικό προβληματισμό.

Και τούτο διότι χρονικά είμαστε στο σημείο κατά το οποίο η αστυνομική αρχή ζητά την έκδοση ενός βουλεύματος ή διάταξης για την άρση του απορρήτου ώστε νόμιμα να μπορέσει να συλλέξει ψηφιακή απόδειξη. Όμως το αρ. 4 § 3 Ν 2225/1994 αξιώνει (πέρα από τις λοιπές παραμέτρους που εκτέθηκαν και παραπάνω) διερεύνηση της *υπόθεσης* ή της

[212] Βλ. *Αλ. Κραγιόπουλος*, Ανακριτικές πράξεις επί ψηφιακών δεδομένων: Δικαιικοί άξονες και προβληματισμοί, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2018, 203 επ.
[213] Βλ. ΓνωμΑΠ 2/2017, ΠοινΧρον 2017, 630 = ΠοινΔνη 2017, 676.
[214] Βλ. *Γ. Μπουρμάς*, Η νομιμότητα των ερευνών σε ηλεκτρονικά δίκτυα και δεδομένα στις περιπτώσεις εγκλημάτων στον Κυβερνοχώρο, δημοσιευμένη στην ΠοινΔνη 2019, 556, *Θ. Δαλακούρας*, Ειδικές ανακριτικές πράξεις κατ' αρ. 253 Α ΚΠΔ και ηλεκτρονικό έγκλημα, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2018, 262 με τις εκεί παραπομπές σε Λίβο.

εξακρίβωσης του τόπου διαμονής του *κατηγορουμένου*. Και φυσικά στο σημείο αυτό ποινική δίωξη ακόμη δεν υπάρχει, ούτε δικογραφία στην εισαγγελία έχει σχηματιστεί, ούτε φυσικά μπορεί να γίνει λόγος για κατηγορούμενο, που στην τεχνική δικονομική ορολογία απαιτεί άσκηση ποινικής δίωξης. Επιπρόσθετα το Δικαστικό Συμβούλιο, πρέπει να εκφέρει αιτιολογημένη κρίση σχετικά με την αποδοχή του αιτήματος για την άρση. Δεν ισχύει η ίδια απαίτηση σωρευτικής παρουσίας προϋποθέσεων στην περίπτωση απόρριψης, αναφορικά ειδικότερα με την αξίωση για αιτιολόγηση της δικανικής κρίσης. Επί ποιού υλικού όμως θα στηρίξει την απόφασή του το δικαιοδοτικό όργανό; Πώς θα διατάξει την άρση του απορρήτου επικοινωνίας του Χ όταν δεν υπάρχει υλικό, που να προέρχεται από νόμιμη ερευνητική δράση;

Εννοείται ότι η μετέπειτα συλλογή και αξιοποίηση στοιχείων που θα προκύψουν από την έρευνα θα έχει ως νομιμοποιητική βάση το βούλευμα του Δικαστικού Συμβουλίου. Αυτό όμως είναι φαύλος κύκλος. *Ακόμη δεν μπορεί να εντοπιστεί η πρώτη πληροφορία.*

iv. Η προσπάθεια για λήψη εισαγγελικής παραγγελίας για την έναρξη της ανακριτικής έρευνας. Η πρώτη ενημέρωση της εισαγγελικής αρχής.

Η πρακτική έχει αναδείξει ότι η αστυνομική αρχή που υποβάλλει την σχετική αίτηση για άρση του απορρήτου επικαλείται σχετική αναφορά άλλης αρχής δίωξης είτε στα πλαίσια συνεργασίας είτε στα πλαίσια εκπλήρωσης συμβατικής της υποχρέωσης, όπως λ.χ. όταν αιτείται την παροχή στοιχείων αστυνομική δομή του επιπέδου της INTERPOL. Αυτή η αίτηση συνδρομής νομοτεχνικά μπορεί να διατηρεί στοιχεία νομιμοποίησης για την υποβολή του αιτήματος στο αρμόδιο Δικαστικό Συμβούλιο για την έκδοση διάταξης (απόφασης[215] - εντολής) για την άρση του απορρήτου των επικοινωνιών, που θα κινηθεί στα καθορισμένα πλαίσια που ορίζει το Δικαστικό Συμβούλιο με ρητή αναφορά στον σκοπό που εξυπηρετεί η άρση αλλά και στην αιτιολόγηση[216] της εντολής που εκδίδει. Ωστόσο παραμένει το ερώτημα αναφορικά με την *πρώτη πληροφόρηση* της αρχής που λογικά αναζητείται. Αναφέρομαι πλέον στην αρχή που υπέβαλε το αίτημα (στο παράδειγμα η INTERPOL) το οποίο πλέον μεταφέρει στο δικαστικό περιβάλλον η ξένη αστυνομική αρχή.

Πέραν της παρακολούθησης των επικοινωνιών σε τηλεπικοινωνία και διαδίκτυο, προφανώς με την χρήση ειδικού προηγμένου τεχνολογικού εξοπλισμού (ανωτέρω

[215] Βλ. αρ. 2 § 3 ΠΔ 47/2005.
[216] Βλ. αρ. 5 §§ 1 και 2 Ν 2225/1994.

αναφέρθηκε το TLO), που αναζητά αρχεία μέσα από λέξεις ή εκφράσεις κλειδιά ή τον ψηφιακό τους μορφότυπο κατά την επεξεργασία, δεν φαίνεται πειστική οποιαδήποτε άλλη περίπτωση ενημέρωσης της αστυνομικής αρχής, σύμφωνα και με τις αναφορές που προηγήθηκαν σχετικά με το ισχνό αποδεικτικό αποτέλεσμα που μπορεί να αναμένει κανείς από μια καταγγελία για συμπεριφορά που εξελίσσεται στον ψηφιακό χώρο. Λ.χ. θα ήταν θεωρητική μόνο η παραδοχή να εκθέσει κάποιος σε τρίτον την από μέρους του κατοχή ψηφιακού υλικού παιδικής πορνογραφίας και δη με την παρουσίαση[217] έστω μέρους αυτής, ώστε να αξιοποιηθεί ως πρωτόλειο υλικό η καταγγελία του τρίτου στον οποίον παρουσίασε ο δράστης το παράνομο υλικό κατοχής του. Και τούτο καθόσον η απλή λογική αλλά και το προφίλ των δραστών αυτών, τους θέτει μακριά από την δημοσιότητα και την έκθεση του «πάθους» τους σε *άσχετους* τρίτους, μάλιστα δε είθισται να είναι χρήστες τεχνολογίας με προχωρημένες γνώσεις και τεχνικές επιλογές προστασίας και απόκρυψης της συνήθειας και των ιχνών τους, δρουν δε κρυφά και κατά μόνας.

Ο προβληματισμός που αναπτύσσεται εδώ αφορά στην περίπτωση της πρώτης έρευνας όταν και αναζητείται ο εντοπισμός του ίχνους που εκκινεί τις λοιπές δράσεις των αρχών. Αυτό μπορεί να είναι μια IP που προέκυψε από την αναζήτηση μέσω εντοπισμού διαμοιρασμού επιλήψιμου ψηφιακού αρχείου. Βέβαια εντοπισμός IP δεν συνεπάγεται και εντοπισμό του δράστη, καθόσον στην IP ενός router μπορεί να συλλειτουργούν περισσότεροι χρήστες από χωριστές υπολογιστικές μηχανές.

Είναι άλλη η λογική του πράγματος όταν η έρευνα αναδεικνύει είτε άλλους υπαιτίους εντός της ιδίας (in rem) έρευνας, είτε οδηγεί, μέσα από την άρση του απορρήτου και την έρευνα στις IP's σε νέα ευρήματα, που ενδεχόμενα θα αξιοποιηθούν μέσα από μια χωριστή διαδικασία. Έτσι λ.χ. είναι η αναζήτηση εκείνων που κατεβάζουν και διαμοιράζουν ταυτόχρονα αρχείο παιδικής πορνογραφίας σε τρίτους.

Επανερχόμενοι στον βασικό προβληματισμό και δια της αφαιρετικής οδού προσεγγίζοντας τα πράγματα, δεν καταλείπεται άλλη λογική εκδοχή εκτός από την περίπτωση της χρησιμοποίησης μεθόδων που χρησιμοποιεί το αρμόδιο τμήμα ασφαλείας τη αστυνομίας, περί προληπτικής παρακολούθησης, οι οποίες μέθοδοι σε καμιά περίπτωση δεν έχουν αντοχές συνταγματικής νομιμότητας καθόσον προσβάλλουν θεμελιώδεις ατομικές

[217] Κατά την ορθότερη άποψη η απλή θέαση του υλικού από τον τρίτο, μετέπειτα καταγγέλλοντα, δεν αποτελεί αξιόποινη συμπεριφορά, βλ. *Γ. Νούσκαλης*, Κατοχή και διανομή/διάθεση πορνογραφικού υλικού ανηλίκων (άρθρο 348 Α ΠΚ): Η νομολογιακή προσέγγιση κρισίμων ζητημάτων ουσιαστικού και δικονομικού δικαίου σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη 2019, σελ. 86, *του ιδίου*, Παιδική πορνογραφία, ΠοινΔνη 2006, 161. Διατυπώνεται και η αντίθετη θέση ότι ακόμη και στην απλή θέαση διαδικτυακά υπάρχει προσωρινή αποθήκευση στην μνήμα RAM κείθεν δε πληρούται και το στοιχείο της (έστω στιγμιαίας) κατοχής.

ελευθερίες και δη στον πυρήνα τους, όπως είναι το απόρρητο της επικοινωνίας στο καθαρό περιεχόμενό της και όχι στα στοιχεία θέσης και κίνησης, που παρατηρήσαμε ανωτέρω.

Δεν μπορεί να υπάρχει άλλη επιστημονική θέση παρά εκείνη της αποδοκιμασίας των πρακτικών αυτών, οι οποίες ούτε νόμιμη βάση έχουν, προσβάλλουν τις προαναφερόμενες ατομικές ελευθερίες αλλά και αρχές του συντάγματος όπως είναι ο σεβασμός στην αξιοπρέπεια του ανθρώπου (αρ. 2 § 1 Συντ), στην προστασία του απορρήτου της επικοινωνίας (αρ. 19 Συντ), στην ιδιωτικότητα και την προσωπική ελευθερία (αρ. 1, 5 και 8 ΕΣΔΑ). Εννοείται ότι νομικό φραγμό υψώνει και το πλέγμα των διατάξεων του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) και ο Ν 4624/2019, που εξεδόθη στα πλαίσια συμμόρφωσης της χώρας μας με τον Κανονισμό.

Η προληπτική αυτή δράση της αστυνομίας, ακόμη και με την επίκληση του συμφέροντος της κοινότητας από την πρόληψη από εγκληματικές δράσεις και την εν γένει ασφάλεια του κοινωνικού συνόλου, δεν άγει άμεσα σε νομιμοποίηση όλων των μεθοδεύσεων αυτών. Απαραίτητη προϋπόθεση για τη ηθική και νομική παραδοχή των πρακτικών αυτών είναι η αξιολόγησή τους στο περιβάλλον της αρχής της αναλογικότητας, της αναγκαιότητας και του σκοπού. Και στο περιβάλλον αυτό δεν επιβιώνουν τέτοιες πρακτικές. Προσπαθώντας να δώσω την θέση μου αυτήν με ένα παράδειγμα θα ανατρέξω στην περίπτωση της παρακολούθησης από ιδιώτη, που μέχρι την τροποποίηση του Π.Κ. δεν ήταν αξιόποινη, σήμερα όμως μπορεί να οδηγήσει σε καταδίκη για απειλή[218]. Και τούτο είναι άσχετο με το εάν το θύμα έχει να αποκρύψει ή όχι κάτι. Αξιόποινη πλέον είναι η αίσθηση περιορισμού της ελευθερίας του με την έννοια του σταθερού ελέγχου (με την έννοια της παρακολούθησης) της δράσης του.

Έτσι λοιπόν ακόμη και αν δεν έχει να κρύψει τίποτε το υποκείμενο των δικαιωμάτων, μια συνθήκη ψηφιακής παρακολούθησης της δράσης του σε σταθερή βάση σαφώς και δημιουργεί άλλη συνθήκη, περιορισμού της ελευθερίας. Δικαίωμα δεν είναι μόνο να μπορώ να αναζητώ στο διαδίκτυο αλλά και το να διατηρώ την ιδιωτικότητα της αναζήτησής μου αυτής, χωρίς τούτο να προϋποθέτει το αν έχω να κρύψω κάτι ή όχι, που ενδεχόμενα να έχει και μια ηθική νομιμοποίηση στα πλαίσια της φιλοσοφικής προσέγγισης του αυτοπροσδιορισμού ως στοιχείου σεβασμού της αξιοπρέπειας του ανθρώπου. Σε μια πιο οπτικοποιημένη αλλά και πρακτική εκδοχή της θέσης μου, παρομοιάζω την παρακολούθηση αυτήν με μια συνθήκη κατά την οποία η απόθεση των αστικών μου απορριμάτων αμέσως

[218] Βλ. αρ. 333 § 1 εδ. β΄ ΠΚ.

μετά την απομάκρυνση και αποξένωσή μου από αυτά (ρίψη στον σχετικό κάδο) θα αποτελεί σταθερά και τακτικά αντικείμενο έρευνας από αστυνομικό.

Η ίδια λογική βάση στηρίζει και την εξ ορισμού ενημέρωση του χρήστη όταν συνδέεται στο διαδίκτυο μέσω δημοσίου δίκτυο, ότι «οι επιλογές σας θα είναι ορατές από τρίτους». Αυτό ή παρόμοιο μήνυμα μπορεί να σημαίνει ότι ο χρήστης κρίνεται προληπτικά ύποπτος; Σαφώς όχι, είναι όμως μια ενημέρωση για κάτι που ο μέσος χρήστης εκτιμά ως σημαντική παράμετρο για την συνέχιση της χρήσης του.

Στο παρόν σημείο δεν γίνεται περαιτέρω ανάπτυξη και σχολιασμός και τούτο για την ενότητα της ροής της θεματικής που παραμένει η δικονομική πρόβλεψη για την κατάσχεση των ψηφιακών στοιχείων. Φυσικά η σχετική ανάπτυξη γίνεται σε χωριστή θεματική της μελέτης αναφορικά με τις σχετικές θέσεις που έχει αναδείξει με τη νομολογία του το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ)[219].

Παρακολουθώντας συνεπώς στο σημείο αυτό την σχετική ροή που έχει αναδείξει η πρακτική, οδηγούμαστε στο υλικό το οποίο πλέον έχει συλλεγεί νομίμως μετά την άρση του απορρήτου, με την διαδικασία που προαναφέρθηκε. Εφόσον το υλικό υποστηρίζει μια εικόνα εγκληματικής συμπεριφοράς σε περιβάλλον ηλεκτρονικού εγκλήματος, το αρμόδιο τμήμα ασφαλείας, μετά την συλλογή στοιχείων από την αστυνομική έρευνα[220], υποβάλλει με σχετικό διαβιβαστικό, αίτημα και την πληροφορία στον αρμόδιο εισαγγελικό λειτουργό κι εκείνος ενεργεί κατά νόμο αφού τα αξιολογήσει και εντοπίσει ενδείξεις ενοχής, οπότε παραγγέλλει σχετικά.

ν. Η εκτέλεση της εισαγγελικής παραγγελίας για την έναρξη της ανακριτικής έρευνας.

Η παραγγελία για ανακριτική έρευνα φέρνει την διαδικασία στο περιβάλλον του Κ.Ποιν.Δ. και δίνει το δικαίωμα πλέον στους ανακριτικούς υπαλλήλους να ενεργήσουν πράξεις έρευνας. Αφού διαδικαστικά οι ανακριτικοί υπάλληλοι εντόπισαν τον χώρο της επέμβασης ο οποίος προέκυψε από την άρση του απορρήτου των ηλεκτρονικών επικοινωνιών δια της IP διεύθυνσης, που αποτέλεσε το στοιχείο της έρευνας για τον

[219] Βλ. κατωτέρω υπό 11. Κατάσχεση ψηφιακών δεδομένων και δικαιώματα κατηγορουμένου υπό το φως των εγγυήσεων προστασίας των ατομικών δικαιωμάτων και της νομολογίας του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων Ανθρώπου (ΕΔΔΑ), σελ. 193 επ.

[220] Η αναφορά γίνεται σταθερά στην έρευνα που βασίζεται στις διατάξεις των άρθρων 96 ΠΔ 141/1991 και 11 Ν 4249/2014.

εντοπισμό του οποίου στοιχείου επετράπη η σχετική άρση του απορρήτου, ερχόμαστε στην δράση του πρώτου αποκριτή (first responder). Πρόκειται για τον ανακριτικό υπάλληλο, ο οποίος πρέπει να διαθέτει ειδικές γνώσεις πληροφορικής και ηλεκτρονικών επικοινωνιών, αλλά να έχει και ανάλογη εμπειρία από την διαχείριση ψηφιακών πειστηρίων και τον τρόπο αντίδρασης των υπολογιστικών μηχανών διασυνδεδεμένων σε δικτυακό περιβάλλον, σε τοπικό δίκτυο ή στο διαδίκτυο[221]. Να έχει γνώσεις στον τομέα της ασφάλειας δικτύων και στα ηλεκτρονικά δίκτυα γενικότερα. Μεταξύ δε των στοιχείων του εξοπλισμού που φέρει μαζί του πρέπει να είναι και ειδικό λογισμικό για την εξυπηρέτηση των σκοπών της έρευνας. Σημειώνουμε ότι την κατάσχεση μπορεί να ενεργήσει ο επιλαμβανόμενος ανακριτικός υπάλληλος, ήτοι αστυνομικός, λιμενικός, τελωνειακός ή υπάλληλος της φορολογούσας αρχής (στα οικονομικά εγκλήματα φοροδιαφυγής).

Πλέον η έρευνα κινείται στο χώρο της ανάκρισης και έχουν εφαρμογή όλες οι αρχές, δεσμεύσεις, περιορισμοί αλλά και αρμοδιότητες των ανακριτικών υπαλλήλων στις οποίες αναφερθήκαμε ανωτέρω αλλά και σε άλλα σημεία της μελέτης.

Για τις ενέργειες, που αφορούν πρακτικά ζητήματα, το πρώτο μέλημα στην ασφάλιση του χώρο όπου επιχειρεί ο πρώτος αποκριτής, για τον εξοπλισμό που πρέπει να φέρει μαζί του και γενικότερα για τη σειρά από βήματα στην έρευνα και την απεικόνιση του χώρου πριν την επέμβαση γίνεται διεξοδικότερα λόγος κατωτέρω[222] σε χωριστή ενότητα, όπου και παραπέμπω.

Αντικείμενο της μελέτης στο σημείο αυτό είναι οι δικονομικές δυνατότητες και οι νομικές δεσμεύσεις αναφορικά με την κατάσχεση των ψηφιακών στοιχείων που εντοπίζονται και σημαίνονται βάσει των ενεργειών που διαλαμβάνονται στην θεματική πρωτόκολλο έρευνας και διαχείρισης των ψηφιακών πειστηρίων και των ψηφιακών δεδομένων στην οποία θεματική έγινε η αναφορά αμέσως παραπάνω.

vi. Η κατάσχεση των ψηφιακών πειστηρίων και των ψηφιακών δεδομένων στα πλαίσια της ανακριτικής έρευνας.

Πλέον ο πρώτος αποκριτής έχει μπροστά του τις δικονομικές δυνατότητες να δεσμεύσει στοιχεία, που εντόπισε στον χώρο της έρευνας και σχετίζονται με το υπό έρευνα

[221] Βλ. *Β. Κάτος*, Ψηφιακά Πειστήρια σε Θ. Δαλακούρα, Ηλεκτρονικό έγκλημα, Νομική Βιβλιοθήκη 2019, σελ. 75.
[222] Βλ. κατωτέρω υπό 10. Πρωτόκολλο έρευνας και διαχείρισης των ψηφιακών πειστήριων και των ψηφιακών δεδομένων σελ. 173 επ.

ηλεκτρονικό έγκλημα. Εννοείται ότι το αντικείμενο της έρευνάς του δεν περιορίζεται από τον ψηφιακό ή μη τύπο των ευρημάτων. Σε περίπτωση συνεπώς που εντοπιστούν στοιχεία που μπορούν να αξιοποιηθούν στην έρευνα για την ταυτοποίηση του προσώπου του υπόπτου ή άλλων τυχόν συμμετόχων στην αξιόποινη δράση, και τα στοιχεία αυτά θα τύχουν ερευνητικής δέσμευσης προκειμένου να αξιοποιηθούν αποδεικτικά για την υποστήριξη της κατηγορίας.

Το ειδικότερο ερευνητικό πεδίο όμως της μελέτης αυτής επικεντρώνεται στην κατάσχεση των ψηφιακών δεδομένων και ειδικότερα στην ερμηνευτική ανάπτυξη και ανάλυση της νεοπαγούς διάταξης του αρ. 265 Κ.Ποιν.Δ. Παρακολουθούμε στην συνέχεια τις δικονομικές δυνατότητες και το πλαίσιο διαδικασίας που αναπτύσσεται αναφορικά με την ειδική όσο και απαιτητική αυτή κατάσχεση. Ξεκινώντας από την ευχέρεια δράσης που επιτρέπει ο νόμος στον πρώτο αποκριτή.

Στο σημείο αυτό κρίνεται βασική ενδιαφέρουσα μια διάκριση στην διαχείριση της δέσμευσης και της μετέπειτα αξιοποίησης των ψηφιακών δεδομένων. Αρχικά είναι η κατάσχεσή τους, που ενεργείται με τους τρόπους που θα παρακολουθήσουμε στην συνέχεια, ως δέσμευση και αποξένωση από τον ύποπτο ή κατηγορούμενο, ενεργείται από τον ανακριτικό υπάλληλο που επιχειρεί στον χώρο της έρευνας, ο οποίος ολοκληρώνει την νομική πράξη με τις μεθόδους τεχνικά ασφαλούς δέσμευσης και αφαίρεσης των ψηφιακών στοιχείων, την σύνταξη της ειδικής έκθεσης και την ασφαλή αποστολή στο τμήμα ψηφιακών πειστηρίων, που είναι διακριτό στάδιο έρευνας επί των κατασχεθέντων, όπου ενεργείται η εξαγωγή και ανάλυση των ψηφιακών δεδομένων καταλήγοντας στην έκθεση πραγματογνωμοσύνης, η οποία θα είναι και η γραμματική απόδοση των δεδομένων, που θα τα καταστήσει εύληπτα και κατανοητά από τον δικαστή.

Α. Η δικονομική ευχέρεια του πρώτου αποκριτή – ανακριτικού υπαλλήλου, που αφορά στην κατάσχεση των ψηφιακών στοιχείων καταλαμβάνει κατά την διάταξη του αρ. 265 Κ.Ποιν.Δ. την δέσμευση 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. Κατ' αρχήν ο ανακριτικός υπάλληλος στοχεύει στον εντοπισμό των πειστηρίων, από τα οποία μπορεί να αντλήσει ψηφιακή πληροφορία, που να σχετίζεται με την υπό έρευνα αξιόποινη πράξη.

Τα συστήματα υπολογιστών μπορούν να λάβουν πολλές μορφές, αλλά και να δώσουν πολλές πληροφορίες. Οι σχετικές εμπορικές προτάσεις αναφέρονται σε φορητούς υπολογιστές, επιτραπέζιους υπολογιστές, συστήματα που βασίζονται σε βιομηχανικούς διακομιστές (rack-servers), μικροϋπολογιστές και κεντρικούς («μεγάλους») υπολογιστές (mainframes). Περαιτέρω, πρόσθετα εξαρτήματα και περιφερειακές συσκευές περιλαμβάνουν μόντεμ, δρομολογητές, κόμβους (διανομείς) σε δίκτυο υπολογιστών (hubs), εκτυπωτές, σαρωτές και σταθμούς σύνδεσης. Πρόκειται για συναρμογή (σύστημα) από οτιδήποτε μπορεί να φιλοξενήσει, επεξεργαστεί, διαχειριστεί και να αποθηκεύσει ψηφιακά δεδομένα ή ακατέργαστα ηλεκτρονικά δεδομένα. Εδώ συγκαταλέγονται πλακέτες κυκλωμάτων, μικροεπεξεργαστές, ο σκληρός δίσκος της υπολογιστικής μηχανής, εξωτερικός σκληρός δίσκος, μνήμες, ελεύθερες ή σε συναρμογή υφιστάμενες και συνδέσεις διασύνδεσης. Υποστηρικτικά εργαλεία για την διαχείριση των ψηφιακών δεδομένων, όπως οθόνη ή συσκευή προβολής αρχείων εικόνας ήχου, πληκτρολόγιο, συσκευή εισόδου (το γνωστό «ποντίκι» - mouse), περιφερειακές ή εξωτερικά συνδεδεμένες μονάδες δίσκου, κινητά τηλέφωνα, ταμπλέτες, συσκευές και εξαρτήματα, όπως μονάδες usb, αφαιρούμενα μέσα κλπ.

Το σύστημα υπολογιστή και τα στοιχεία του πρέπει να σχετίζονται με την υπό έρευνα αξιόποινη συμπεριφορά, που συνιστά ηλεκτρονικό έγκλημα. Το σύστημα δε του υπολογιστή ενδέχεται να διαλαμβάνει σημαντικά, ίσως και πολύτιμα στοιχεία αναφορικά με την έρευνα. Το υλικό, το λογισμικό, τα έγγραφα, οι φωτογραφίες, τα αρχεία εικόνας, ήχου ή εικόνας – ήχου, το ηλεκτρονικό ταχυδρομείο και τα συνημμένα του, βάσεις δεδομένων, οικονομικές πληροφορίες, ιστορικό περιήγησης στο διαδίκτυο, αρχεία καταγραφής συνομιλιών, λίστες φίλων, αρχεία καταγραφής συμβάντων, δεδομένα που είναι αποθηκευμένα σε εξωτερικές συσκευές, συμπεριφορές χρήσης σε υπολογιστική νέφους και ταυτοποίηση πληροφοριών που

σχετίζονται με το σύστημα του υπολογιστή και τα συστατικά του. Όλα αυτά είναι πιθανά στοιχεία που υποστηρίζουν την απόδειξη της κρίσιμης πληροφορίας.

Σε ένα σύστημα προσωπικού υπολογιστή είναι βέβαιο ότι μεταξύ των στοιχείων που εμπεριέχονται θα εντοπιστούν και άσχετα με την ερευνώμενη συμπεριφορά δεδομένα, μερικά από τα οποία θα είναι προσωπικά δεδομένα του υπόπτου ή ενδεχόμενα θα αφορούν τρίτα πρόσωπα. Για παράδειγμα αναφέρονται αρχεία φωτογραφιών από προσωπικές στιγμές του υπόπτου ή φωτογραφίες φίλων του ή φωτογραφίες που είναι στην κατοχή του για επαγγελματικό λόγο, αρχεία κειμένου εντελώς άσχετα με την έρευνα κλπ. Σε ρεαλιστική βάση μιλώντας, ίσως το μεγαλύτερο ποσοστό να αφορά σε *άσχετα* με την έρευνα ψηφιακά δεδομένα.

Σε μια σχηματική ανάπτυξη της θέσης αυτής, έστω ότι γίνεται έρευνα σε δικηγορικό γραφείο στα πλαίσια αναζήτησης στοιχείων τέλεσης αξιόποινης συμπεριφοράς κατοχής και διαμοιρασμού αρχείων εικόνας ήχου παιδικής πορνογραφίας. Η έρευνα στο σύστημα προσωπικού επαγγελματικού υπολογιστή του δικηγόρου σαφώς και υπάρχει υλικό από σειρά υποθέσεων εντολέων του (υλικό άσχετο με την έρευνα), προσωπικά αρχεία που δεν έχουν καμιά σχέση με την παιδική πορνογραφία, λ.χ. σκαναρισμένα πιστοποιητικά υγείας του υπόπτου, ή αντίγραφο ποινικού μητρώου του υπόπτου δικηγόρου, εφαρμογές από συμμετοχή του σε online games ή σε στοιχηματικές πλατφόρμες, που είναι νόμιμες. Έστω περαιτέρω ότι όλα τα αρχεία είναι αποθηκευμένα στον σκληρό δίσκο του συστήματος προσωπικού επαγγελματικού υπολογιστή του υπόπτου δικηγόρου.

Το ερώτημα που τίθεται άμεσα αφορά την δυνατότητα κατάσχεσης του αρ. 265 § 1 α΄ Κ.Ποιν.Δ. στα δεδομένα υπολογιστή που είναι αποθηκευμένα σε αυτόν, στα οποία έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση. Έχει δικαίωμα ο ανακριτικός υπάλληλος να κατάσχει όλα τα ανωτέρω δεδομένα;

Στα πλαίσια της αρχής της *αναλογικότητας*, που είναι εφαρμοστέα στην ανάκριση[223], ο νομοθέτης *δεν* επιβάλλει την συνολική κατάσχεση των ψηφιακών πειστηρίων («*ό,τι* βρεθεί στον χώρο»), σα να κατευθύνεται στις επιλογές του από ενδοιασμούς και ανασφάλεια, που μόνο σε άτομα που δεν διαθέτουν γνώσεις πληροφορικής θα δικαιολογούνταν, αλλά φυσικά δεν θα ήταν επιτρεπτές κατά την άσκηση δημόσιας εξουσίας. Το *δεν* επιβάλλει προκύπτει από την γραμματική διατύπωση που επέλεξε ο νομοθέτης όχι τόσο στην διατύπωση της παρ.

[223] Βλ. κατωτέρω υπό 9. Οι Αρχές που διέπουν την έρευνα αναφορικά με τα ψηφιακά πειστήρια και τα ψηφιακά δεδομένα *ii. Οι Αρχές που διέπουν την ανακριτική έρευνα ως ερευνητική προσέγγιση της μελέτης, Ε) η αρχή της αναγκαιότητας και της αναλογικότητας*, σελ. 164.

1 στην αρχή της («…κατάσχεση ψηφιακών δεδομένων *μπορεί* να επιβληθεί:…»), όσο στην ειδικότερη αναφορά αμέσως μετά («…στο σύνολό του ή *σε μέρος αυτού*…»).

Δεν κατάσχεται λοιπόν *ό,τι* είναι συνδεδεμένο σε σύστημα υπολογιστή (ή σε δίκτυο), ούτε κάθε ηλεκτρονική συσκευή, ούτε αναγκαστικά ολόκληρο το σύστημα του υπολογιστή ή το σύνολο των υπολογιστών και των περιφερειακών συστημάτων με τα οποία είναι συνδεμένο. Είναι δεδομένο ότι η κατάσχεση είναι ένα καταναγκαστικό δικονομικό μέτρο, το οποίο προσβάλλει ευθέως, (ίσως όχι μόνο) το συνταγματικώς κατοχυρωμένο δικαίωμα στην ιδιοκτησία και την περιουσία. Υπερβολές κατά την άσκηση της εξουσίας στο στάδιο της ανακριτικής έρευνας προσβάλλουν την αρχή της αναλογικότητας, είναι εκτεθειμένες στη νομική έννοια της κατάχρησης, κείθεν δε της παράνομης δράσης.

Η κατάσχεση των αρχείων των εντολέων του δικηγόρου, για να πειραματιστούμε στην υπόθεση εργασίας, που αναπτύξαμε ανωτέρω με την μορφή παραδείγματος, σαφώς και δεν έχει να δώσει στοιχεία αναφορικά με την υπό έρευνα υπόθεση καθόσον είναι εντελώς ξένα από το αντικείμενο της έρευνας. Εννοείται ότι ο ερευνητής θα αναζητήσει μέσα σε αυτά αρχεία που ενδεχομένως τα έκρυψε ο ύποπτος λ.χ. καλύπτοντάς τα σε επάλληλες τοποθεσίες αρχειοθέτησης ώστε να χαθούν ενδεχόμενα ίχνη σε μια ενδεχόμενη έρευνα, η οποία θα βασιζόταν σε μια αναζήτηση με την συνήθη πρακτική. Έστω λοιπόν όμως ότι μια αρχειοθέτηση δίνει διαδρομή που μοιάζει με αρχειοθέτηση στοιχείων εντολέα αλλά στην κατάληξή της οδηγεί σε ύποπτο αρχείο. Λ.χ. μια διαδρομή ***file://C:/Users/kostasf/Desktop/M_Papadopoulou%20Astika%20Diazigio%20Pistopoiitika%20XX1.avi***. Θα πρόκειται για συνήθη δομή φακέλου κάποιας εντολέος (ενδεχομένως με πραγματική σχέση με το δικηγορικό γραφείο) λ.χ. ονόματι Μ. Παπαδοπούλου, που έχει υπόθεση διαζυγίου, το οποίο ολοκληρώθηκε και έχουν εκδοθεί πιστοποιητικά τα οποία είναι αποθηκευμένα σκαναρισμένα σε αρχείο κειμένου μορφής .pdf, όμως μέσα στον σχετικό ψηφιακό υποφάκελο υπάρχει και το ύποπτο (ερευνώμενο) αρχείο XX1.avi (αρχείο εικόνας – ήχου).

Η σχετική έρευνα θα πρέπει να αναζητήσει σε όλον τον σκληρό δίσκο αλλά μόνος ο εντοπισμός ενός τέτοιου (υπόπτου) αρχείου είναι ικανός να επιβάλλει την κατάσχεση όλου του σκληρού δίσκου; Όλου του συστήματος υπολογιστή; Και ποια η τύχη στα αρχεία των εντολέων του δικηγόρου, που είναι άσχετα με την έρευνα αλλά ιδιαίτερα σημαντικά για την εξέλιξη των υποθέσεών τους και από τα οποία πολλά μπορεί να είναι η ψηφιακή τους μορφή η μοναδική που έχει στην διάθεσή του ο δικηγόρος για τον χειρισμό της υπόθεσής τους; Τονίζεται βέβαια το γεγονός ότι τα στοιχεία στους φακέλους των εντολέων είναι προσωπικά

δεδομένα τους, ενώ σε μια εκδοχή της υπόθεσης σε γραφείο ποινικολόγου (το ίδιο ισχύει και στην περίπτωση ενός ιατρού), τότε τα δεδομένα αυτά είναι *ειδικών κατηγοριών* (ευαίσθητα)[224]. Πέρα από το ζήτημα της νομιμότητας στην επιθετική (υπερχειλή και υπερβολική) αυτή αφαίρεση των στοιχείων των πελατών του, να προστεθεί και η πρακτική δυσχέρεια από την πολύμηνη έως και πολυετή[225] στέρησή τους στην περίπτωση αναμονής μέχρι την επιστροφή της έρευνας.

Και για μια περαιτέρω απόχρωση στην έρευνα, έστω ότι σε ψηφιακό φάκελο εντολέα του δικηγόρου, υπάρχει υλικό πορνογραφίας ανηλίκου το οποίο ελήφθη ψηφιακά από άλλη δικογραφία. Έστω λοιπόν το επιλήψιμο αρχείο εικόνας X2X.jpg το οποίο εντοπίζεται στα πλαίσια της ανακριτικής έρευνας. Σαφώς για τον εντολέα του δικηγόρου δεν υφίσταται ζήτημα καθόσον για την δική του κατοχή του υλικού κινείται ήδη ποινική δικογραφία και νέα δίωξη δεν θα γίνει. Διατηρείται όμως το αρχείο αυτό στο σύστημα υπολογιστή του δικηγόρου που ήδη ελέγχεται για την συγκεκριμένη αξιόποινη πράξη ο ίδιος. Θα διωχθεί και για το αρχείο αυτό (επαναλαμβάνω ότι για το αρχείο αυτό δεν υπήρξε αναζήτηση, ούτε σχετίζεται η IP του δικηγόρου με την λήψη του αρχείου αυτού);

Το ζήτημα της έκτασης της κατάσχεσης σε δικηγορικό γραφείο και στο σύνολο του συστήματος υπολογιστή, απασχόλησε και το ΕΔΔΑ σε ιδιαίτερα επίπεδα για την επίλυση των προβληματισμών αναφορικά με ενέργειες άρσης απορρήτου σε δικηγορικό γραφείο στην αναζήτηση ιχνών οικονομικών συναλλαγών δικηγόρου με τον ύποπτο, που ήταν εντολέας της. Εξετάζοντας την αναγκαιότητα και την αναλογικότητα της επέμβασης, το ΕΔΔΑ[226] επισήμανε ότι η διαδικασία άρσης του απορρήτου έλαβε χώρα χωρίς τη συμμετοχή και εν αγνοία της προσφεύγουσας δικηγόρου. Επομένως, η προσφεύγουσα δεν μπόρεσε να εκθέσει τα επιχειρήματά της. Επιπλέον, παρότι το εθνικό δίκαιο προέβλεπε ότι στη διαδικασία αυτή έπρεπε να ζητηθεί η γνώμη του δικηγορικού συλλόγου, κάτι τέτοιο δεν είχε συμβεί. Παρατηρήθηκε επίσης ότι η προσφεύγουσα δεν είχε τη δυνατότητα να προσβάλει αποτελεσματικά την άρση του απορρήτου ούτε διέθετε οποιοδήποτε ένδικο βοήθημα με το οποίο να αμφισβητήσει το μέτρο. Λόγω της έλλειψης δικονομικών εγγυήσεων και

[224] Βλ. αρ. 9 ΓΚΠΔ το οποίο αναφέρεται σε δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

[225] Η σχετική διαδικασία εξέτασης δεν είναι κάτι άμεσο, ούτε και χρονικά σύντομο.

[226] Βλ. ΕΔΔΑ, *Brito Ferrinho Bexiga Villa-Nova κατά Πορτογαλίας*, προσφυγή αριθ. 69436/10, 1 Δεκεμβρίου 2015, αλλά και όμοιες σκέψεις στην ΕΔΔΑ, *Pruteanu κατά Ρουμανίας*, προσφυγή αριθ. 30181/05, 3 Φεβρουαρίου 2015

αποτελεσματικού δικαστικού ελέγχου επί του μέτρου αναστολής του επαγγελματικού απορρήτου, το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι υπήρξε παράβαση του άρθρου 8 της ΕΣΔΑ.

Επίσης στην υπόθεση *Kırdök κ.α. κατά Τουρκίας* της 03.12.2019 (αριθ. 14704/12)[227], το ΕΔΔΑ ασχολήθηκε με το παράπονο δικηγόρων για την κατάσχεση των ηλεκτρονικών τους δεδομένων από τις δικαστικές αρχές για την άσκηση ποινικής δίωξης κατά άλλου δικηγόρου (Ü.S.), ο οποίος μοιράζονταν το γραφείο τους. Η αστυνομία διεξήγαγε έρευνες στο γραφείο που μοιράζονταν με τους προσφεύγοντες. Όλα τα δεδομένα που ήταν αποθηκευμένα στο σκληρό δίσκο του υπολογιστή που χρησιμοποιούνταν *από κοινού* από τους δικηγόρους αντιγράφηκαν σε ένα υλικό φορέα USB το οποίο ανήκει στην κα Hanbayat. Βασιζόμενοι στο άρθρο 8 (δικαίωμα σεβασμού της ιδιωτικής ζωής, της κατοικίας και της αλληλογραφίας) και άρθρο 13 (δικαίωμα για αποτελεσματική προσφυγή), οι προσφεύγοντες ισχυρίστηκαν ότι το επαγγελματικό απόρρητο τω δικηγόρων, βασιζόμενο στην ύπαρξη εχεμύθειας και εμπιστευτικότητας μεταξύ των σχέσεων τους με τους πελάτες τους, παραβιάστηκε λόγω του ότι τα εν λόγω ψηφιακά αρχεία αναφορικά με τις υποθέσεις αυτών των πελατών αντιγράφηκαν από τις δικαστικές αρχές κατά τη διάρκεια μιας έρευνας και ότι τα εν λόγω αντίγραφα κατασχέθηκαν παρά το γεγονός ότι ήταν *άσχετα* με τη διεξαγωγή της έρευνας σε σχέση με άλλο δικηγόρο. Το ΕΔΔΑ δέχθηκε τους ισχυρισμούς αυτούς[228].

Περαιτέρω και ως παράδειγμα αναφορικά με την έννοια του συστήματος υπολογιστή, τίθεται προβληματισμός αναφορικά με τη δέσμευση μιας συμβατικής τηλεόρασης, η οποία μπορεί να είναι συνδεδεμένη με το σύστημα υπολογιστή τον οποίον απλώς εξυπηρετεί ως οθόνη, στα πλαίσια της παρουσίασης αρχείων εικόνας – ήχου ή εγγράφων βάσει διαχείρισής τους από εφαρμογές και προγράμματα που είναι εγκατεστημένα και *τρέχουν* στον υπολογιστή και ουσιαστικά δεν αλληλεπιδρά με το σύστημα υπολογιστή. Είναι δεδομένο ότι η σύνδεση του υπολογιστή σε μια άλλη οθόνη δεν επιφέρει καμιά μεταβολή στο τελικό αποτέλεσμα και συνεπώς δεν υπάρχει καμιά σχέση αλληλεπίδρασης μεταξύ υπολογιστή και τηλεόρασης.

Και στις δύο περιπτώσεις των παραδειγμάτων, η όποια τελική κρίση θα έχει ως βάση την αρχή της αναλογικότητας, σε συνδυασμό με τις αρχές του σκοπού και της αναγκαιότητας.

---

[227] Βλ. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-198805%22]}

[228] Περαιτέρω σχολιασμός και ανάλυση της υπόθεσης κατωτέρω υπό 11. Κατάσχεση ψηφιακών δεδομένων και δικαιώματα κατηγορουμένου υπό το φως των εγγυήσεων προστασίας των ατομικών δικαιωμάτων και της νομολογίας του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων Ανθρώπου (ΕΔΔΑ), σελ. 193 επ.

Ιδίως αναφορικά με την αρχή της αναγκαιότητας, το κριτήριο για μια ασφαλή επιλογή, κατά την άποψή μου, το δίνει η απάντηση στην ερώτηση, *τί θα έχανε η έρευνα χωρίς την υπερβολή*; Με άλλα λόγια, η κρίση για τον βαθμό που θα υπήρχε δυσχέρεια ή προσκόμματα στην πρόοδό της, είναι το στοιχείο (κριτήριο) που οδηγεί στην πιο ασφαλή, από πλευράς νομιμότητας, απάντηση. Η κατάσχεση λοιπόν μιας τηλεόρασης (στην απλή εκδοχή του προβληματισμού) που δεν έχει να δώσει κανένα στοιχείο, απλά και μόνο επειδή ήταν συνδεμένη με τον υπολογιστή και εξελήφθη ότι είναι τμήμα του συστήματος υπολογιστή, προφανώς κείται εκτός πνεύματος της διάταξης που μας απασχολεί. Στην πιο σύνθετη εκδοχή της δέσμευσης των αρχείων από το δικηγορικό γραφείο εφόσον δεν προκύπτει κανένα αρχείο από αυτά που αποτελούν αντικείμενο έρευνας, κάτι που τεχνικά εξακριβώνεται στον χώρο, σαφώς και δεν πρέπει να κατασχεθούν τα συγκεκριμένα δεδομένα. Και όταν αναφέρουμε για έρευνα στον χώρο, ας δοθεί εδώ η πληροφορία ότι μια τέτοια ανακριτική έρευνα για κατάσχεση ψηφιακών δεδομένων μπορεί να διαρκέσει από μια ώρα μέχρι και περισσότερα εικοσιτετράωρα, χρόνος που ποικίλει αναφορικά με τις επιλογές του επικεφαλής. Επιλογές που φυσικά δεν στερούνται ρηγμάτων στη νομιμότητα της πρακτικής που θα εφαρμοστεί κάθε φορά.

Κατά την ίδια προσέγγιση δεν μπορούν να κατασχεθούν όλα τα συστήματα υπολογιστών, ανεξάρτητα μεταξύ τους, που βρίσκονται στον χώρο, απλά και μόνο για τον λόγο αυτόν. Ο πρώτος αποκριτής έχει την ευχέρεια, και με τεχνικές μεθόδους, αναζητήσεις απλές ή διαβαθμισμένες, αφού λάβει μέτρα εξασφάλισης της αποφυγής αλλοίωσης των δεδομένων στον υπολογιστή[229], θα μπορέσει και θα εξετάσει στον χώρο και δεν θα επέμβει σε υπολογιστή που δεν σχετίζεται με την ερευνώμενη πράξη, με άλλα λόγια δεν θα κινηθεί στα όρια της υπερβολής, προσβάλλοντας δικαιώματα του κατηγορουμένου ή υπόπτου.

Β. Η επόμενη κατηγορία πεδίου κατάσχεσης αφορά σε κατάσχεση σε ένα *μέσο αποθήκευσης δεδομένων υπολογιστή* στο οποίο υπάρχουν αποθηκευμένα δεδομένα υπολογιστή και έχει φυσική πρόσβαση εκείνος που διενεργεί την ανάκριση.

[229] Βλ. κατωτέρω υπό 10. Πρωτόκολλο έρευνας και διαχείρισης των ψηφιακών πειστηρίων και των ψηφιακών δεδομένων *iii. Η πρώτη επέμβαση – είσοδος στον χώρο της έρευνας*, σελ. 179, όπου η ειδικότερη ανάλυση του πρωτοκόλλου ανάπτυξης των ερευνών.

Τα (αφαιρούμενα) μέσα αποθήκευσης δεδομένων υπολογιστή, είναι υλικοί υποδοχείς ψηφιακών δεδομένων, συσκευές αποθήκευσης δεδομένων [όπως κάρτες Secure Digital (SD) mini και micro, Smart Media (SM), υποδοχέας Memory Stick)], που συνήθως χρησιμοποιούνται για την αποθήκευση, αρχειοθέτηση, μεταφορά και μεταφορά δεδομένων και άλλων πληροφοριών. Οι υλικοί αυτοί υποδοχείς αντιμετωπίζονται ως λειτουργικό ενιαίο συμπεριλαμβανομένου του προγράμματος, που παρέχει τη δυνατότητα με τη συναρμογή τους σε πληροφοριακό σύστημα να εκτελέσουν μια λειτουργία παρουσίασης των γεγονότων, πληροφοριών ή εννοιών που έχουν αποθηκευμένα, πάντα σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα. Οι συσκευές αποθήκευσης ποικίλλουν σε μέγεθος και στον τρόπο με τον οποίο αποθηκεύουν και διατηρούν δεδομένα.

Οι σχετικές παρατηρήσεις, οι οποίες διατυπώθηκαν και αναπτύχθηκαν αναφορικά με την έκταση των ερευνών στον χώρο σχετικά με το υλικό που εντοπίζεται κατά την πρώτη επέμβαση, διατηρούν την ισχύ τους και στην περίπτωση αυτήν. Προς αποφυγή άσκοπης επανάληψης γίνεται παραπομπή στον οικείο χώρο, όπου οι σχετικές αναφορές και προβληματισμοί με τις ανάλογες δογματικές παρατηρήσεις και απόψεις.

Γ. Ιδιαίτερα κρίσιμα ζητήματα κλήθηκε να καλύψει η περίπτωση, η οποία αφορά 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 (σύμφωνα με την διατύπωση της επίμαχης διάταξης), 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. Στην περίπτωση που εξετάζουμε έχουμε την πρώτη επαφή του Κ.Ποιν.Δ. με την νεφοϋπολογιστική (cloud computing).

Από την διατύπωση της διάταξης προκύπτει ένα ερμηνευτικό πρόβλημα. Κατά την γραμματική ανάγνωση της διάταξης προκύπτει ότι το ενδιαφέρον του νομοθέτη στρέφεται α) σε *απομακρυσμένο* σύστημα υπολογιστή και στα ψηφιακά δεδομένα που βρίσκονται σε αυτόν, β) με τον οποίο, ο υπολογιστής στον οποίον έχει φυσική πρόσβαση ο ερευνητής, είναι *διασυνδεδεμένος*, γ) στα δεδομένα που είναι αποθηκευμένα και προσβάσιμα μέσω συστήματος *νεφοϋπολογιστικής*. Το ερώτημα που τίθεται είναι αν απομακρυσμένο σύστημα και σύστημα νεφοϋπολογιστικής είναι έννοιες ταυτόσημες και αλληλοκαλυπτόμενες.

Η απάντηση είναι αρνητική καθόσον το *απομακρυσμένο* σύστημα υπολογιστή, με τον οποίο, ο υπολογιστής στον οποίον έχει φυσική πρόσβαση ο ερευνητής, είναι *διασυνδεδεμένος*, αφορά κάθε μορφή ζεύξης, λ.χ. μια ασύρματη ή ενσύρματη διασύνδεση, ή μια ζεύξη με Bluetooth, με υπολογιστή που βρίσκεται σε άλλο χώρο (απομακρυσμένο) με τον οποίον είναι διασυνδεμένος ο ελεγχόμενος υπολογιστής βάσει τοπικού δικτύου και όχι αναγκαστικά μέσω διαδικτύου. Η έννοια της δικτύωσης ή του διαδικτύου δεν είναι δεδομένη στην περίπτωση αυτή. Αντίθετα στην περίπτωση του συστήματος *νεφοϋπολογιστικής*, όπως αναλυτικότερα εκτίθεται κατωτέρω, ο ελεγχόμενος υπολογιστής είναι συνδεμένος με έναν άλλον υπολογιστή (server), που είναι διασυνδεμένος μέσω διαδικτύου και ασύρματα και μάλιστα στις πλείστες των περιπτώσεων, χωρίς ο χρήστης να γνωρίζει την τοποθεσία όπου τεχνολογικά υποστηρίζονται και έτσι εξυπηρετούνται οι σχετικές παρεχόμενες υπηρεσίες. Συνεπώς ό,τι είναι *σύστημα νεφοϋπολογιστικής* είναι *απομακρυσμένο* σύστημα, το αντίθετο όμως δεν ισχύει καθόσον υπάρχουν και οι περιπτώσεις της απλής ζεύξης με άλλον υπολογιστή, εκτός περιβάλλοντος *νεφοϋπολογιστικής*.

Η ανάπτυξη όμως της διάταξης στο δεύτερο εδάφιο της γ΄ περίπτωσης ξεκινά με το «*…Στην τελευταία περίπτωση, τα ψηφιακά δεδομένα που είναι αποθηκευμένα και προσβάσιμα μέσω συστήματος και υπηρεσιών νεφοϋπολογιστικής (cloud services)* …». Αν ως τελευταία περίπτωση εννοήσουμε το απομακρυσμένο μέσο αποθήκευσης, η διατύπωση δεν άγει σε ασφαλές πόρισμα και ενδεχόμενα δημιουργεί σύγχυση καθόσον ο server δεν είναι μόνο μέσο αποθήκευσης αλλά και χώρος (σημείο) παροχής υπολογιστικών πόρων, που επιτρέπει περισσότερες ενέργειες στον χρήστη. Θα μπορούσε λοιπόν η διατύπωση να καθορίσει σε μια παρατακτική σύνδεση και όχι ως νοηματική συνέχεια, την θέση του νομοθέτη αναφορικά με τις υπηρεσίες νεφοϋπολογιστικής (cloud services).

Από τεχνολογικής άποψης, το υπολογιστικό νέφος (cloud computing) είναι η διάθεση υπολογιστικών πόρων και μεγάλου αποθηκευτικού χώρου ψηφιακών δεδομένων μέσω διαδικτύου (π.χ. servers, apps κλπ), από κεντρικά συστήματα που βρίσκονται απομακρυσμένα από τον τελικό χρήστη, τα οποία τον εξυπηρετούν αυτοματοποιώντας διαδικασίες, παρέχοντας ευκολίες και ευελιξία σύνδεσης[230]. Κατά το ΕΠΣΕΤ[231], ως υπολογιστικό νέφος ορίζεται η κατ' αίτηση διαδικτυακή κεντρική διάθεση υπολογιστικών πόρων (όπως δίκτυο, εξυπηρετητές, εφαρμογές και υπηρεσίες) με υψηλή ευελιξία, ελάχιστη προσπάθεια από τον χρήστη και υψηλή αυτοματοποίηση. Κατά την διάδραση στο περιβάλλον του υπολογιστικού νέφους η αποθήκευση, η επεξεργασία και η χρήση δεδομένων, λογισμικού και υπηρεσιών γίνεται διαδικτυακά, μέσω απομακρυσμένων υπολογιστών σε κεντρικά Datacenters. Υπηρεσίες όπως η κατ' αίτηση παροχή εικονικών μηχανών, το διαδικτυακό ηλεκτρονικό ταχυδρομείο ή τα κοινωνικά δίκτυα, συχνά βασίζονται στην τεχνολογία του υπολογιστικού νέφους. Ο λόγος για τον οποίον επιλέγουν την συγκεκριμένη τεχνολογία οι χρήστες αφορά στην εξοικονόμηση πόρων από την αγορά και συντήρηση λογισμικού, τη συντήρηση ακριβών εξυπηρετητών και εγκαταστάσεων αποθήκευσης δεδομένων. Το SaaS (Software as a Service) αποτελεί μια από τις εκδοχές[232] του υπολογιστικού νέφους και αναφέρεται σε λογισμικό, που προσφέρεται διαδικτυακά ως υπηρεσία στο νέφος.

---

[230] Βλ. https://el.wikipedia.org/wiki/%CE%A5%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%B9%CE%BA%CF%8C_%CE%BD%CE%AD%CF%86%CE%BF%CF%82#cite_note-1

[231] Εθνικό Πληροφοριακό Σύστημα Έρευνας και Τεχνολογίας, http://www.epset.gr/el/content/ypologistiko-nefos-cloud-computing

[232] Βασικές κατηγορίες μοντέλων νεφοϋπολογιστικής: α) *Software-as-a-Service (SaaS)*: Αντί να εγκαταστηθεί λογισμικό στο μηχάνημα και στον υπολογιστή του πελάτη επιβαρυνοντάς τον με τακτικές επιδιορθώσεις, συχνές εκδόσεις κτλ., εφαρμογές όπως το Word, CRM (Διαχείριση Σχέσεων Πελατών), ERP (Enterprise Resource) Προγραμματισμός, διατίθενται (φιλοξενούνται) μέσω του διαδικτύου για την κατανάλωση του τελικού χρήστη. β) *Platform-as-a-Service (PaaS)*: Αντί ο πελάτης να χρειαστεί να αγοράσει - πληρώσει τις άδειες λογισμικού για πλατφόρμες όπως και τα λειτουργικά συστήματα, τις βάσεις δεδομένων και το ενδιάμεσο λογισμικό, μπορεί να το κάνει χρησιμοποιοντας την πλατφόρμα και τα εργαλεία (όπως το Java, το .NET, Python, Ruby on Rails), γ) *Infrastructure-as-a-Service (IaaS)*: Πρόκειται για τις απλές-βασικές υλικές συσκευές (raw υπολογιστές) όπως είναι οι εικονικοί υπολογιστές, οι διακομιστές, οι συσκευές αποθήκευσης, η μεταφορά μέσω δικτύου, οι οποίες βρίσκονται φυσικά σε ένα κεντρικό σημείο (κέντρο δεδομένων). Υπάρχει η δυνατότητα να προσπεραστούν και να χρησιμοποιηθούν από το διαδίκτυο χρησιμοποιώντας τα συστήματα ελέγχου ταυτότητας σύνδεσης και τους κωδικούς πρόσβασης από οποιοδήποτε dumb τερματικό ή συσκευή. δ) *Desktop-as-a-Service (DaaS)*: Η υπηρεσία επιφάνεια εργασίας προσφέρει μια υποδομή εικονικής επιφάνειας εργασίας (Virtual Desktop Infrastructure - VDI) που φιλοξενείται από έναν πάροχο λύσεων λογισμικού cloud και βασίζεται συνήθως σε ένα μοντέλο μηνιαίας συνδρομής. Το DaaS χρησιμοποιεί μια αρχιτεκτονική πολλαπλών μισθώσεων, πράγμα που σημαίνει ότι μια μοναδική εμφάνιση μιας εφαρμογής εξυπηρετείται σε πολλούς χρήστες, που αναφέρονται ως «ενοικιαστές». Ο πάροχος λύσεων λογισμικού cloud είναι υπεύθυνος για τη διαχείριση του cloud και της υποκείμενης υποδομής και το επίπεδο εξυπηρέτησης μπορεί να διαφέρει ανάλογα με τις ανάγκες των χρηστών. Το τελικό αποτέλεσμα αυτής της υποδομής είναι ότι οι χρήστες μπορούν να έχουν πρόσβαση στα δεδομένα και τις εφαρμογές τους από σχεδόν οποιαδήποτε συσκευή, οπουδήποτε.

Όπως γίνεται αντιληπτό, με την αναζήτηση στη νεφοϋπολογιστική αναφερόμαστε σε έκφραση - όρο της πληροφορικής επιστήμης, που αφορά σε διακριτό επιστημονικό πεδίο, το οποίο σαφώς ερμηνεύεται και εξηγείται με τους κανόνες και τις αρχές της συγκεκριμένης επιστήμης. Κατ' εκτίμηση, η ορθολογική αντιμετώπιση της συνθήκης στην οποία αναφέρεται η περίπτωση του άρθρου 265 § 1 περ. γ΄ Κ.Ποιν.Δ. επιβάλλει τον σεβασμό και την τήρηση των στοιχείων που δανειζόμαστε από την επιστήμη της πληροφορικής για την ανάλυση και την κατανόηση της υπηρεσίας αυτής. Η ένταξη του ειδικού τεχνικού όρου σε ένα κείμενο νομοτεχνικά δομημένο δεν είναι αδόκιμη αλλά θα οδηγήσει σε εσφαλμένα αποτελέσματα αν τύχει διαχείρισης, παράφρασης κι ερμηνείας μέσα, αλλά και αυστηρά αποκλειστικά, μόνο από το πνεύμα και την φιλοσοφία της νομικής επιστήμης.

Ενώ λοιπόν στον τομέα της πληροφορικής η δομή διαδίκτυο, παγκόσμιος ιστός, ηλεκτρονικές συσκευές διαχείρισης και αποθήκευσης δεδομένων, εξυπηρετητές και όλη η δομή της ιντερνετικής νέφους έχουν βάση, εξήγηση αλλά και τεχνολογική ερμηνεία μέσα από την μεταγωγή πακέτων δεδομένων με πρωτόκολλα επικοινωνίας και το ενδιαφέρον στρέφεται στην υπηρεσία της επικοινωνίας και την δομή των δικτύων που την υποστηρίζουν, στον χώρο της νομικής επιστήμης, όπου διεκδικεί λειτουργική διάρθρωση και λογική ένταξη η *νεφοϋπολογιστική*, τα πράγματα δεν είναι ξεκάθαρα. Εδώ η νεφοϋπολογιστική δεν αξιολογείται και δεν αξιοποιείται στην βάση της τεχνικής της ανάλυσης, αλλά αναλύεται ώστε να καταστεί διαχειρίσιμη σε ένα άλλο περιβάλλον (νομικό) για το οποίο ούτε κατασκευάστηκε, ούτε εντάσσεται λειτουργικά κατά την τακτική της εφαρμογή.

Για να γίνουμε πιο συγκεκριμένοι. Κινούμαστε ήδη στο νομικό περιβάλλον της κατάσχεσης. Μια νομική έννοια, η οποία έχει μέσα από την πρακτική εφαρμογή αλλά και την λειτουργική εμφάνισή της, σε όλους τους τομείς του δικαίου, αποκτήσει μια συγκεκριμένη λειτουργική απεικόνιση και νομική παραδοχή. Όπως την αναφέραμε και σε άλλο σημείο της μελέτης, είναι η νομική εκείνη πράξη με την οποία δεσμεύεται (με την

έννοια της αποστέρησης) το δικαίωμα εξουσίασης του ιδιοκτήτη ή κατόχου. Με άλλα λόγια δεσμεύεται και αποκλείεται, τόσο νομικά αλλά και πρακτικά, με την αφαίρεση του αντικειμένου, η σχέση φυσικής εξουσίασης μεταξύ του φυσικού προσώπου (ιδιοκτήτη ή κατόχου) και του αντικειμένου. Η ικανότητα δηλαδή του τελευταίου (ιδιοκτήτη ή κατόχου) να καθορίζει τις τύχες του αντικειμένου.

Ο *φυσικός* αυτός αποκλεισμός του κατόχου από το πράγμα, δεν έχει την ίδια μορφή, δομή και κατανόηση στην περίπτωση της νεφοϋπολογιστικής.

Στην αρχική πορεία της μελέτης και της ανάλυσής μας αναφορικά με την αναζήτηση, εντοπισμό και δέσμευση ψηφιακών δεδομένων, η προσλαμβάνουσα παράσταση αφορούσε στην τοπική και μόνο έρευνα. Ο ερευνητής εντόπιζε ηλεκτρονικές συσκευές και μέσα σε αυτές θα αναζητούσε το προϊόν της (ηλεκτρονικής) εγκληματικής πράξης, με την μορφή ψηφιακής δομής αρχείων εικόνας, ήχου ή εικόνας ήχου ή και επιπέδου μηνυμάτων επικοινωνίας. Η έρευνα περιοριζόταν σε περαιτέρω σε αναζητήσεις σε υλικούς φορείς – υποδοχείς, όπως είναι τα CD, DVD, κάρτες μνήμης, σκληρούς δίσκους, περιφερειακές μνήμες κλπ, που εντοπίζονταν στον χώρο της έρευνας.

Προοδευτικά η διαδικτυακή εργασία (κι επικοινωνία) συνάντησε τις υπηρεσίες νεφοϋπολογιστικής (cloud services), που παρείχαν πολλές (περισσότερες) δυνατότητες στον χρήστη και κυρίως την ευχέρεια να μην επιβαρύνεται με την αποθήκευση και την αναζήτηση νέων χώρων αποθήκευσης, που ενδεχόμενα δεν παρείχαν και ιδιαίτερες δυνατότητες κατά την αναζήτηση του επιθυμητού αρχείου, όταν και με τις συμβατικές μορφές αποθήκευσης έπρεπε να ανατρέξουν σε σειρά αποθηκευτικών μέσων. Πρόκειται για υπηρεσίες όπως το DropBox, το OneDrive, OneNote. Υπηρεσίες που επιτρέπουν πέρα από το στοιχείο της απομακρυσμένης αποθήκευσης, την χρησιμοποίηση υπολογιστικών πόρων, εφαρμογών και λογισμικού, την μεγαλύτερη παροχή ασφάλειας αναφορικά με την ακεραιότητα των αποθηκευμένων ψηφιακών δεδομένων αλλά και την σύγχρηση αρχείων, στοιχείο ιδιαίτερα σημαντικό όταν γίνεται λόγος για συμμετοχική δράση στο εγκληματικό προσκήνιο, που μας απασχολεί.

Όπως αναφέρθηκε παραπάνω στις εισαγωγικές αναφορές, οι υπηρεσίες νεφοϋπολογιστικής (cloud services) παρέχουν στον χρήστη τις εξής δύο βασικές δυνατότητες. Στην πρώτη περίπτωση μπορεί να αποθηκεύσει και ασφαλίσει την εργασία του και γενικότερα τα αρχεία, τα οποία επιθυμεί να έχει στην κατοχή του σε απομακρυσμένο εξυπηρετητή (server) αλλά και στο ίδιο το σύστημα υπολογιστή που διαθέτει. Αυτό μπορεί

να εξυπηρετεί ζητήματα ασφάλειας από ενδεχόμενη απώλεια αρχείου από κακή δική του χρήση (λ.χ. απρόσεκτη διαγραφή και ελλιπείς γνώσεις ανάκτησης αρχείου) ή από επίθεση από κακόβουλο λογισμικό στον υπολογιστή του ή από αστοχία υλικού ή καταστροφή του υπολογιστή. Η περίπτωση της απώλειας από δολιοφθορά (λ.χ. κλοπή) δεν μπορεί να μην συμπεριληφθεί σε όλα τα ανωτέρω. Σε μια από τις ανωτέρω ατυχείς συνθήκες, ο χρήστης ανησυχεί μόνο για την υλική απώλεια αλλά το αρχείο που τον ενδιαφέρει υπάρχει σε πρώτη αναζήτησή του μέσα από την αποθήκευσή του στον απομακρυσμένο server.

Στην δεύτερη περίπτωση ο χρήστης μπορεί να επιλέξει την κατ' αποκλειστικότητα αποθήκευση των αρχείων και της εργασίας του στον απομακρυσμένο server. Στην περίπτωση αυτή το αρχείο ανεξάρτητα από το πού δημιουργήθηκε, τελικά αποθηκεύεται αποκλειστικά στο νέφος (cloud) και αντίγραφό του δεν υπάρχει στο σύστημα υπολογιστή και συνεπώς δεν θα εντοπιστεί σε ενδεχόμενη αναζήτηση από τον ερευνητή.

Η χρήση των υπηρεσιών νεφοϋπολογιστικής (cloud services) γίνεται με την δημιουργία λογαριασμού στην εκάστοτε εφαρμογή που επιλέγει ο χρήστης. Κατά την αρχική διαμόρφωση του λογαριασμού, όπως σε όλες σχεδόν τις διαδικτυακές επικοινωνιακές *φωλιές*, ο χρήστης ταυτοποιείται βάσει κωδικού ονομασίας (username) και κωδικού πρόσβασης (password). Ανάλογα με τον βαθμό ασφαλείας στην επαφή με τον λογαριασμό μπορεί να απαιτηθεί είτε αλφαριθμητικός συνδυασμός μείζονος αριθμού χαρακτήρων και με απαίτηση διατήρησης αριθμών, γραμμάτων, κεφαλαίων και μικρών χαρακτήρων, είτε να απαιτηθεί και δεύτερος κωδικός πρόσβασης σε κάθε νέα χρήση. Φυσικά ο κωδικός ονομασίας (username) δεν άγει με σαφήνεια σε ταυτοποίηση. Μόνη η παραπομπή σε κάποιο όνομα, ή ονοματεπώνυμο δεν δίνει ταυτοποίηση. Δεν είναι λίγες οι περιπτώσεις κατά τις οποίες υπάρχει *κατασκευή* ονομασίας παραπλανητική (αναφερόμενη λ.χ. σε χαρακτήρα καρτούν, ή σε μυθικό ή τηλεοπτικό χαρακτήρα). Ακόμη δε περισσότερο όταν η δημιουργία του λογαριασμού γίνεται ακριβώς για την απομάκρυνση του κινδύνου εντοπισμού του κατόχου, τότε είναι πλέον από σαφές ότι η επιλογή της ονομασίας θα παραπέμπει σε ο,τιδήποτε άλλο εκτός από το πρόσωπο που ενδιαφέρει την έρευνα.

Εδώ εγείρονται και οι περισσότεροι προβληματισμοί. Χωρίς να αξιολογούμε την καταγραφή στο νόμο, επιχειρούμε να βρούμε τις προβληματικές που εγείρουν οι υπηρεσίες νεφοϋπολογιστικής (cloud services) στην έρευνα. Το πρώτο ζήτημα είναι αυτό του εντοπισμού του χρήστη μέσα από την ταυτοποίηση του λογαριασμού και του χρήστη του με το πρόσωπο, ή τα στοιχεία που αφορά η έρευνα. Όπως αναπτύχθηκε παραπάνω, όπου και παραπέμπω προς αποφυγή άσκοπης επανάληψης, η ταυτοποίηση είναι δυσχερής έως

αδύνατη, εφόσον κρατήσουμε στην υπόθεση εργασίας την έλλειψη συνεργασίας από τον ύποπτο, κάτι που είναι και το σύνηθες. Το φαινόμενο της δημιουργίας ψεύτικου προφίλ δεν μπορεί να αποκλειστεί.

Αντιλαμβανόμαστε φυσικά ότι αν ένας δράστης επιλέγει (για λόγους που αφορούν την εγκληματολογία ή την δικαστική ψυχολογία ή ακόμη και την υπερασπιστική του στρατηγική, παραγωγικά αίτια που εκφεύγουν του αντικειμένου της μελέτης αυτής) να συνεργαστεί με την έρευνα, ή στην περίπτωση που τα στοιχεία εισόδου εντοπίζονται στον περιβάλλοντα χώρο (σε πρόχειρη σημείωση ή στην επιφάνεια εργασίας ως διευκόλυνση του χρήστη), τότε πρόβλημα, *κατ' αρχήν*, δεν υπάρχει. Τεχνικά στην περίπτωση αυτήν, όπως και σε κάθε περίπτωση που θα διατεθούν τα στοιχεία ταυτοποίησης για την είσοδο στον λογαριασμό, η κατάσχεση μπορεί να λάβει τη μορφή αποκλεισμού του χρήστη μέσω αλλαγής τους, με νέο username και password, που θα είναι στην διάθεση του μόνο της ανακριτικής αρχής και συνεπώς αποκλείεται (= αφαιρείται) με τον τρόπο αυτόν η *εξουσίαση* του ψηφιακού δεδομένου (υλικού) από τον δράστη. Αυτή μπορεί να είναι μια πρόσφορη λύση, όμως ο πλήρης αποκλεισμός από ένα προσωπικό, ενδεχόμενα και επαγγελματικό, ηλεκτρονικό αρχείο στο σύνολό του, δεν επιτρέπεται στα πλαίσια της αρχής της αναλογικότητας και του σκοπού.

Στην μάλλον πιθανότερη εκδοχή, ο δράστης δεν θα συνεργαστεί. Περαιτέρω και για προσέγγιση των αληθινών συνθηκών που αφορά η ανακριτική έρευνα, στους συλλογισμούς μας πρέπει να έχουμε ως δεδομένο ότι ο δράστης που επιχειρεί αξιόποινα στον ψηφιακό κόσμο δεν είναι ένας απλός χρήστης αλλά άτομο που διαθέτει τουλάχιστον εμπειρικές γνώσεις τεχνικών απόκρυψης των ιχνών του, όχι κατ' ανάγκη βασιζόμενες σε ιδιαίτερα απαιτητικές πρακτικές. Έστω λοιπόν ότι εντοπίζεται στον υπολογιστή του εγκατεστημένη η εφαρμογή που του επιτρέπει να επιχειρεί στο περιβάλλον της νεφοϋπολογιστικής υπηρεσίας (cloud service) OneDrive[233].

Το ερώτημα που άμεσα εγείρεται είναι η μορφή ανταπόκρισης του υπόπτου στο αίτημα του ερευνητή να ανακοινώσει τον κωδικό ονομασίας (username) και τον κωδικό πρόσβασης (password) στην υπηρεσία του. Φυσικά περιπτώσεις τυχαίων ευρημάτων όπως πρόχειρες σημειώσεις ή αποθήκευση των κωδικών κατά την είσοδο στην εφαρμογή, ιδίως όταν για δική του ευχέρεια ο δράστης έχει συσχετίσει και smartphone, δεν αποκλείεται να

[233] Με την υπηρεσία αυτήν ο χρήστης μπορεί να έχει σταθερά τα αρχεία του στο νέφος αλλά κατ' απαίτηση (on demand) να έχει τα αρχεία που επιθυμεί στον υπολογιστή του και να επιδρά offline, οπότε η επικαιροποίηση θα γίνεται αυτόματα με την online σύνδεση του υπολογιστή.

δώσει λύση. Στην βασική όμως δομή του προβληματισμού, μια πιθανή εκδοχή θα είναι να δηλώσει ότι δεν έχει λογαριασμό και συνεπώς δεν έχει να δώσει κανένα στοιχείο, δικαιολογώντας την ύπαρξη της υπηρεσίας, ακόμη και με την μορφή συντόμευσης στην επιφάνεια εργασίας του υπολογιστή του, ως δυνατότητα που του παρασχέθηκε από τον πωλητή της συσκευής με την εγκατάσταση του λειτουργικού ή με την αφιλοκερδή προσφορά φιλικού του προσώπου, το οποίο διαθέτει γνώσεις πληροφορικής και τις εφαρμόζει εύκολα, παρέχει δε τις υπηρεσίες του απλόχερα. Ας μην λησμονούμε ότι μέλημα του δράστη είναι να δώσει μια απάντηση που θα του επιτρέψει να αποφύγει την άμεση εμπλοκή, ώστε να εξασφαλίσει χρόνο αντίδρασης, και όλα αυτά στα πλαίσια μια κοινότυπης εγκληματικής στρατηγικής με προσανατολισμό την σύγχυση στην έρευνα, κείθεν δε την απόκτηση περισσότερου χρόνου για αναπρογραμματισμό της δράσης του και συγκάλυψη των ιχνών της. Το ότι μια μεταγενέστερη έρευνα μπορεί να τον διαψεύσει δεν τον απασχολεί ιδιαίτερα, απλά διότι θα είναι …… *μεταγενέστερη*, θα έχει δηλαδή ήδη κερδίσει τον χρόνο που του ήταν απαραίτητος. Αλλά ακόμη και αν δεν προφασιστεί έλλειψη σχέσης με την νεφοϋπολογιστική υπηρεσία και πάλι μπορεί είτε ρητά να αρνηθεί, όπως και αν εκτιμηθεί μεταγενέστερα η στάση του, να σωπάσει απλά ή τέλος να δηλώσει ότι έχει λησμονήσει τους κωδικούς. Πιστευτός ή όχι, έχει σημασία;

Εξ άλλου δικονομικά η σιωπή του κατηγορουμένου (ή του υπόπτου ανάλογα με το στάδιο της προδικασίας) όσο και η ρητή άρνησή του να συνεργαστεί δεν μπορεί με κανέναν τρόπο να αξιοποιηθεί και να αξιολογηθεί εναντίον του. Και τούτο καθόσον σύμφωνα με το άρθρο 104 §§ 1 και 3 Κ.Ποιν.Δ.[234] «*1. Ο ύποπτος ή ο κατηγορούμενος έχουν δικαίωμα, σιωπής και μη αυτοενοχοποίησης. 2. ……, 3. Η άσκηση του δικαιώματος σιωπής και μη αυτοενοχοποίησης δεν μπορεί να αξιοποιηθεί σε βάρος των υπόπτων και των κατηγορουμένων.*», ενώ περαιτέρω σύμφωνα με το άρθρο 273 § 2 εδ. β΄ Κ.Ποιν.Δ. «*…Ο κατηγορούμενος έχει δικαίωμα να αρνηθεί να απαντήσει…*». Πρόκειται για ρύθμιση δικονομικά συνεπή στο τεκμήριο αθωότητας του κατηγορουμένου[235] και στην αρχή της

[234] Πρόκειται για ρύθμιση η οποία στο περιβάλλον του νέου Κ.Ποιν.Δ. έλαβε πρωτεύουσα θέση στα δικονομικά δικαιώματα του κατηγορουμένου, συνδυαζόμενη με την διάταξη του άρθρου 273 § 2 εδ. β΄, του ιδίου νομοθετήματος, ως εκδήλωση ηθικής και νομικής συμμόρφωσης προς την αρχή του σεβασμού της αξίας του ανθρώπου, σύμφωνα με το πνεύμα των άρθρων 2 § 1 και 5 § 1 του Συντάγματος και 6 § 1 και 3 εδ. α΄ ΕΣΔΑ, έτσι και *Θ. Δαλακούρας*, Ο Νέος Κώδικας Ποινικής Δικονομίας, συνοπτική ερμηνεία κατ' άρθρο του Ν 4620/2019, 2η εκδ. Νομική Βιβλ., 2019, σελ. 88 με τις εκεί παραπομπές σε ίδιο (Η σιωπή του κατηγορουμένου στην ποινική δίκη, Αρμ 1986, σελ. 317), Στ. Παπαγεωργίου – Γονατά.

[235] Βλ. *Αργ. Καρράς*, Ποινικό Δικονομικό Δίκαιο, 2017, εκδ. ε΄, σελ. 564, *Στ. Αλεξιάδης*, το τεκμήριο αθωότητας του κατηγορουμένου, ΕΕΕυρΔ 1986, σελ. 52, *Δ. Γιαννουλόπουλος*, Η γνωστοποίηση του δικαιώματος σιωπής στον κατηγορούμενο και η ανάγκη εναρμόνισης της ελληνικής νομοθεσίας με το διεθνές και συγκριτικό δίκαιο, ΠοινΔικ 2012, 640.

απαγόρευσης της αυτενοχοποίησης[236]. Η παραβίαση των δικαιωμάτων αυτών, με οποιονδήποτε τρόπο ή με την με οποιονδήποτε τρόπο ή μέσο άσκηση πίεσης, έστω και ψυχολογικής προς τον κατηγορούμενο προκειμένου να παραιτηθεί των, ας άνω, δικαιωμάτων του, συνιστά απόλυτη ακυρότητα[237]. Συνεπώς ένας δράστης με ισχυρές αντιστάσεις και ενδεχόμενα με γνώση των δικονομικών του δικαιωμάτων, δεν θα καμφθεί, δεν θα συνεργαστεί και δεν θα επιτρέψει, τουλάχιστον την στιγμή εκείνη της έρευνας, την πρόσβαση στην υπηρεσία νεφοϋπολογιστικής, επιβάλλοντας στην ανακριτική αρχή να αιτηθεί νέα άρση του απορρήτου της επικοινωνίας μέσα από την διαδικασία του αρ. 4 Ν 2225/1994, που μας απασχόλησε ανωτέρω στην ενότητα αυτήν.

Δρώντας περαιτέρω βάσει σχεδιασμού ή αυτοματισμών, αφού ήδη εξασφάλισε χρόνο, θα έχει τη δυνατότητα να επιχειρήσει από άλλον υπολογιστή πρόσβαση στην υπηρεσία και θα διαγράψει από το νέφος κάθε ενοχοποιητικό αρχείο. Διαφορετικά μπορεί να μην ενεργεί ο ίδιος είτε διότι προσήχθη και εξετάζεται, είτε διότι θέλει να δημιουργήσει άλλοθι για τον εαυτό του με μια έξωθεν μαρτυρία, που σε καθεστώς ελευθερίας θα τον παρουσιάζει «αδρανή». Στην περίπτωση αυτήν έστω ότι έχει κάποιον συνεργό, που διαθέτοντας τους σχετικούς κωδικούς θα έχει την δυνατότητα εκείνος να διαγράψει και δη κεκαλυμμένα, λ.χ. μέσα από ένα internet cafe ή από τον υπολογιστή ενός ανυποψίαστου φίλου του, που θα του παραχωρήσει την χρήση, σαφώς αγνοώντας το τί εκείνος επιχειρεί. Αυτές οι πρακτικές δεν απαιτούν ιδιαίτερο σχεδιασμό καθόσον ένα απλό μήνυμα αποσταλέν κρυφά στο κινητό ή μέσω εφαρμογής σε smartphone, μπορεί να λειτουργήσει ακόμη και την ίδια την ώρα της έρευνας ή καθοδόν για τον χώρο, όπου ειδοποιήθηκε για την έρευνα λ.χ. από οικείο του.

Ως ερώτημα, για την ανάδειξη της ευρύτερης προβληματικής, θα μπορούσε ίσως να τεθεί εδώ, το κατά πόσο ο πάροχος της υπηρεσίας νεφοϋπολογιστικής διατηρεί ή μπορεί να διατηρήσει ένα τέτοιο αρχείο ως δική του ιδιοκτησία[238] (άλλως διαμορφώνοντας δικαιώματα κοινής κτήσης με τον χρήστη) καθόσον βρίσκεται μέσα στον server, με τον οποίον ο πάροχος διατηρεί με σχέση κυριότητας και σχετικής πρωτοβουλίας αναφορικά με την επιλογή του

[236] Βλ. *Β. Αδάμπας/Χ. Αθανασίου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 1635.
[237] Βλ. *Θ. Δαλακούρας*, Ο Νέος Κώδικας Ποινικής Δικονομίας, συνοπτική ερμηνεία κατ' άρθρο του Ν 4620/2019, 2η εκδ. Νομική Βιβλ., 2019, σελ. 88
[238] Βλ. *D. Gray,* Data Ownership In The Cloud, σε https://dataconomy.com/2014/03/data-ownership-in-the-cloud/, σύμφωνα με τον οποίον, ορισμένες εταιρείες, βάσει συμβατικού όρου με το χρήστη, προσπαθούν να παραμείνουν σε σχέση με τα δεδομένα διατηρώντας κάθε πρόσβαση στα δεδομένα των πελατών τους. Ορισμένες δωρεάν υπηρεσίες διατηρούν το δικαίωμα να διατηρήσουν τα δεδομένα των χρηστών στις πλατφόρμες τους, ενώ άλλες κατέχουν μόνο ένα μέρος των δεδομένων που μεταφορτώνονται στους διακομιστές τους.

server. Ο πάροχος στην παρούσα αναφορά σχετίζεται με την προσφερόμενη υπηρεσία νεφοϋπολογιστικής[239] και όχι με εκείνη της απλής παροχής διαύλου ηλεκτρονικής επικοινωνίας και μόνο. Έτσι λ.χ. ο πάροχος στον οποίον γίνεται η αναφορά είναι η Google LLC[240] και όχι λ.χ. η Cosmote A.E. ως τηλεπικοινωνιακός πάροχος (κανάλι επικοινωνίας).

Μια ιδιοκτησία, την οποία βέβαια είναι αμφίβολο αν θα είναι διατεθειμένος ο πάροχος να την μοιραστεί με τις αρχές[241], μπροστά στον κίνδυνο να χάσει την αξιοπιστία του αναφορικά με την υποχρέωση εχεμύθειας, προς τους χρήστες – πελάτες του. Οφείλω όμως στο σημείο αυτό να αναφέρω νομολογιακό δεδομένο, σύμφωνα με το οποίο ο ιστοχώρος «Twitter» έδωσε στοιχεία λογαριασμών, στοιχεία χρήσης και περιεχομένου αρχείων χρήστη στην Διεύθυνση Διεθνούς Αστυνομικής Συνεργασίας (η οποία με τη σειρά της υπέβαλε σχετικό αίτημα στις Ελληνικές Αρχές) αναφορικά με τον διαμοιρασμό υλικού παιδικής πορνογραφίας[242].

Στην περίπτωση αυτήν ο ανακριτικός υπάλληλος θα έχει ερευνήσει το σύστημα υπολογιστή και ενδεχόμενα και άλλες ψηφιακές υπολογιστικές μηχανές που εντόπισε στον χώρο (λ.χ. το smartphone του υπόπτου) αλλά δεν θα εντοπίσει κανένα ύποπτο αρχείο.

Στην περίπτωση τώρα που η τεχνική έρευνα θα γίνει offline είναι ξεκάθαρο ότι την κρίσιμη στιγμή της κατάσχεσης, η έρευνα στα κατασχεθέντα υλικά πειστήρια δεν θα αποδώσει το παραμικρό αποδεικτικό στοιχείο, εφόσον πάντα η υπόθεση εργασίας αναφέρεται σε αξιόποινη συμπεριφορά κατά την οποία ο δράστης αποθήκευσε στοιχεία μόνο στο (υπολογιστικό) νέφος.

Αυτές είναι μερικές ιδιαιτερότητες της νεφοϋπολογιστικής, που σαφώς διαμορφώνουν ένα πλαίσιο αρκετά διαφορετικό από εκείνο της παραδοσιακής δομής της

---

[239] Βλ. Ν 4411/2016 Κεφάλαιο Ι – Ορολογία, Άρθρο 1 – Ορισμοί: … γ. "*πάροχος υπηρεσιών*" σημαίνει: ……ι. κάθε δημόσιος ή ιδιωτικός φορέας που παρέχει στους χρήστες των υπηρεσιών του την δυνατότητα να επικοινωνούν μέσω ενός συστήματος υπολογιστή, και *ιι. κάθε άλλος φορέας που επεξεργάζεται ή αποθηκεύει δεδομένα υπολογιστών είτε για λογαριασμό αυτής της υπηρεσίας επικοινωνίας, είτε των χρηστών αυτής της υπηρεσίας.*

[240] μία από τις μεγαλύτερες εταιρείες διαδικτυακών υπηρεσιών. Ιδρύθηκε από τον Λάρρυ Πέιτζ και τον Σεργκέι Μπριν το 1996, https://el.wikipedia.org/wiki/Google, το σύνθημα της οποίας είναι «Our mission is to organize the world's information and make it universally accessible and useful»

[241] Βλ. σχετικά το νόμο των Ηνωμένων Πολιτειών Stored Communications Act (SCA), ο οποίος παρέχει στην κυβέρνηση το δικαίωμα να κατασχέσει δεδομένα που έχουν αποθηκευτεί από μια αμερικανική εταιρεία, ακόμη και αν φιλοξενούνται αλλού. Η ερμηνεία αυτού έδειξε ότι η Microsoft και άλλοι τεχνολογικοί γίγαντες παραπέμπουν την κυβέρνηση στο δικαστήριο, ισχυριζόμενοι ότι ήταν παράνομο να χρησιμοποιήσει το SCA για να αποκτήσει ένταλμα αναζήτησης για τη διάγνωση και κατάσχεση δεδομένων που έχουν αποθηκευτεί πέρα από τα εδαφικά όρια των Ηνωμένων Πολιτειών. Η Microsoft υπέστη πλήγμα όταν ένας δικαστής περιφερειακού δικαστηρίου στη Νέα Υόρκη αποφάσισε ότι οι κυβερνητικές εξουσίες αναζήτησης των ΗΠΑ επεκτείνονται σε δεδομένα που είναι αποθηκευμένα σε ξένους διακομιστές, σε https://content.next.westlaw.com/8-516-9283?transitionType=Default&contextData=(sc.Default)&__lrTS=20200510055504698.

[242] Βλ. ΣυμβΕφΘεσ 831/2019, ΠοινΔικ 2020, 216 επ. και ιδίως σελ. 219.

κατάσχεσης ως ανακριτικής πράξης. Για πρώτη λοιπόν φορά με το Ν 4620/2019, όπως ισχύει, επιχειρείται η αντιμετώπιση, στην βάση της αφαίρεσης της φυσικής εξουσίασης επί των αρχείων που διαχειρίζεται σε απομακρυσμένο υπολογιστή ο δράστης, μέσα στο περιβάλλον την κατάσχεσης πειστηρίων. Κατά τη νομοθετική λοιπόν επιλογή, 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.

Σε μια απλούστευση της διατύπωσης που επελέγη, αν αφαιρέσουμε συντακτικά τον σύνδεσμο «*δεν*», και δώσουμε έτσι μια καταφατική διάσταση στην έκφραση, αυτή θα ήταν «*… 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*». Ουσιαστικά γίνεται προσπάθεια να εξομοιωθεί το «παράθυρο» με την ίδια την ψηφιακή θέση στην οποία αυτό παραπέμπει. Ό,τι απεικονίζεται ως δράση στην οθόνη του συστήματος υπολογιστή όμως, δεν σημαίνει ότι αντιστοιχεί και σε αρχείο του συγκεκριμένου υπολογιστή.

Για να γίνει πιο κατανοητός ο προβληματισμός, έστω ότι ο ανακριτικός υπάλληλος έχει φυσική πρόσβαση στον ηλεκτρονικό υπολογιστή, τον οποίον εντόπισε στον χώρο της έρευνας και τον οποίον κατάσχει (βάσει των περιορισμών και αρχών ευρευνητικής συμπεριφοράς, που θα μας απασχολήσουν σε άλλη αυτοτελή θεματική), ασφαλίζει και αποθηκεύει. Όταν στο εργαστήριο, στο αρμόδιο για τα ψηφιακά δεδομένα τμήμα, γίνει η offline ανίχνευση, τότε δεν θα βρεθεί κανένα ύποπτο αρχείο. *Τί έχει λοιπόν κατασχεθεί;* Ας μην λησμονούμε ότι όλη η δομή της διάταξης στηρίζεται στην πρώτη φράση της «… *Η κατάσχεση ψηφιακών δεδομένων μπορεί να επιβληθεί σε ……*».

Μόνη η αναφορά του ερευνητή, με την μορφή μαρτυρικής κατάθεσης, ή και με απόδοση στην ειδική έκθεση, ότι εντοπίστηκε *κατέβασμα* (downloading) ύποπτου αρχείου, δεν έχει την υλική της αντιστοιχία στο αποδεικτικό υλικό που θα συνοδεύει την κατηγορία. Ο κατηγορούμενος έχει αναφαίρετο δικαίωμα βάσει και των ελευθεριών και δικαιωμάτων

του από το αρ 8 της ΕΣΔΑ σε πρόσβαση στο υλικό που συνοδεύει την κατηγορία που του αποδίδεται[243].

Αναφέρθηκε πρόχειρα παραπάνω και επαναλαμβάνεται εδώ ως σημείο αναφοράς έναρξης προβληματισμού, ότι για την πρόοδο της έρευνας ο εισαγγελέας, ή σε μεταγενέστερο προδικαστικό στάδιο, ο ανακριτής, θα αιτηθεί την άρση του απορρήτου ηλεκτρονικών επικοινωνιών ζητώντας από τον πάροχο υπηρεσίας, που εξυπηρετεί τον ύποπτο χρήστη, βάσει της IP, να δώσει στοιχεία για διασύνδεση με λογαριασμό στη υπηρεσία νεφοϋπολογιστικής. Είναι πάνω από βέβαιο ότι αυτή θα είναι μια λογική επέκταση της αρχικής άρσης (τηλεπικοινωνικακού) απορρήτου (μέσα από νέο βούλευμα), η οποία τεχνικά θα έχει αποβεί άκαρπη και, ανεξάρτητα από την ευδοκίμηση του δευτέρου αιτήματος μετά την έλλειψη στοιχείων από την πρώτη έρευνα, στην οποία είναι μέλλον και αβέβαιο γεγονός το αν θα ανταποκριθεί και πότε ο πάροχος της υπηρεσίας.

Εκτιμώ ότι η ερμηνευτική προσέγγιση της κατάσχεσης στην περίπτωση της ιντερνετικής νέφους απαιτεί περαιτέρω προβληματισμό. Αυτό για το οποίο κατηγορείται ο ύποπτος πρέπει να του παρέχεται (προσφέρεται) προς εξέταση και μάλιστα όχι μόνο ως αρχείο αλλά και ως τεχνική διαδικτυακή διαδρομή απόκτησης, ώστε να είναι σε θέση να ανταποδείξει με τους ισχυρισμούς του. Όμως στο παράδειγμα που δώσαμε παραπάνω, τέτοια δυνατότητα δεν υπάρχει.

Θα μπορούσε να αντιλέξει κανείς ότι αν κατά την στιγμή της έρευνας εντοπιστεί διαχείριση αρχείου που *τρέχει* στο νέφος, τότε θα μπορούσε ο ερευνητής να κατεβάσει το αρχείο σε δικό του μέσο αποθήκευσης δεδομένων ώστε να το διατηρήσει. Στην περίπτωση αυτήν η πρώτη ένσταση έχει να κάνει με την ίδια την αρχή της αποφυγής αλλοίωσης των δεδομένων που θα κατασχεθούν. Το αρχείο που θα κατέβει στο μέσο αποθήκευσης του ερευνητή *δεν θα είναι πράξη του κατηγορουμένου* αλλά του ίδιου του ερευνητή. Σαφώς και αλλάζουν τα δεδομένα διότι ενδεχόμενα ο κατηγορούμενος για το αρχείο, που τρέχει στο νέφος, να έχει ισχυρισμό που να επιτρέπει ακόμη και αμφιβολίες περί της γνώση του. Αυτό δεν μπορεί να του το στερήσει ο ερευνητής *προσθέτοντας υλικό* εκεί που δεν υπάρχει. Από την άλλη υπάρχει και μια ένσταση τεχνική καθόσον το κατέβασμα αλλοιώνει τα (μετα-)δεδομένα της στιγμής της έρευνας και φυσικά θα είναι δράση που ενεργείται σε χρόνο που ο ύποπτος δεν έχει την φυσική εξουσίαση του χώρου αλλά είναι ο ερευνητής που είναι

[243] Με όποιους σχετικούς προβληματισμούς έχουμε να αναδείξουμε στην συνέχεια των συλλογισμών μας, αναφορικά με την ερμηνεία της διάταξης του αρ. 265 Κ.Ποιν.Δ., οι οποίοι εκτίθενται σε αυτήν εδώ την θεματική ενότητα.

κυρίαρχος και συνεπώς διακινδυνεύει να τεθεί εν αμφιβόλω ολόκληρη η έρευνα, ήτοι να προκληθεί μεγαλύτερη αποδεικτική ζημία στην έρευνα.

Επόμενος προβληματισμός έχει να κάνει με ζητήματα δωσιδικίας που ανακύπτουν και ειδικότερα με την προβληματική του εφαρμοστέου δικαίου αναφορικά με την νεφοϋπολογιστική. Αυτό λοιπόν που διώκεται ως αξιόποινη δράση στην Ελλάδα ενδεχόμενα να μην είναι αξιόποινο στον τόπο που λειτουργεί ο server. Ο δράστης φυσικά δεν έχει γνώση της επιλογής συνεργασιών του παρόχου, ο οποίος με την σειρά του αναζητά τις προσφορότερες οικονομικά προτάσεις κι ενδέχεται από την τέλεση της πράξης μέχρι την δίωξή της να έχει μεταβληθεί η χώρα φιλοξενίας του server. Εγείρεται λοιπόν η προβληματική της γνώσης του χρήστη (υπόπτου) αναφορικά με το αξιόποινο, από πλευράς ουσιαστικού δικαίου. Κάτι όμως που με την σειρά του φωτίζει τα πράγματα και εστιάζει στο ζήτημα της νομιμοποίησης της έρευνας.

Εν τέλει διατηρούνται ενστάσεις αναφορικά με το κατά πόσο λογικά και τεχνικά, μπορεί να λογίζεται ότι τα ψηφιακά δεδομένα που είναι αποθηκευμένα και προσβάσιμα μέσω συστήματος και υπηρεσιών νεφοϋπολογιστικής (cloud services) μπορούν να θεωρούνται αποθηκευμένα στο σύστημα υπολογιστή στο οποίο έχουν φυσική πρόσβαση οι αρχές, ώστε τελικά η προσέγγιση αυτή να είναι και νομικά ορθολογική και συνεπής. Και σε όλα αυτά θα πρέπει να προσμετρηθούν οι ενστάσεις νομικής παραδοχής, που έχουν να κάνουν με το κατά πόσο το εντοπισθέν ψηφιακό δεδομένο μπορεί να είναι κοινή κτήση ή διάδραση περισσοτέρων προσώπων ή να ανήκει σε κοινό σύνολο αρχείων, όμως με αυτοτελείς και διακριτές δράσεις χρηστών σε έναν κοινό ψηφιακό τόπο. Η κατάσχεση αυτή δεν μπορεί να μην αγγίζει και δικαιώματα τρίτων, ενδεχομένως αμέτοχων της ερευνώμενης αξιόποινης συμπεριφοράς.

vii. Η πρακτική εκδοχή εκτέλεσης της κατάσχεσης και οι ιδιαίτερες απαιτήσεις του αντικειμένου.

Από μόνο του το (ψηφιακό) αντικείμενο της έρευνας έχει δώσει το στίγμα της ιδιαιτερότητας του χαρακτήρα του, τις ιδιαίτερες απαιτήσεις στον χειρισμό του και την δυσκολία ένταξής του στις παραδοσιακές δομές, έννοιες και λειτουργίες που προκρίνει ο Κ.Ποιν.Δ. αναφορικά με την ερευνητική διαδικασία στην προδικασία. Στην *παραδοσιακή* μορφή της κατάσχεσης, δεν δημιουργείται καμιά απαίτηση αναφορικά με τον τρόπο δέσμευσης του αντικειμένου της κατάσχεσης. Η διαδικαστική πρακτική με την οποία

υλοποιείται η κατάσχεση είναι εκείνη του εντοπισμού του υλικού αντικειμένου και της αφαίρεσής του από τον νόμιμο κάτοχό του, ώστε να αποφευχθεί κίνδυνος αλλοίωσης ή απώλειας του υλικού αντικειμένου που δεσμεύθηκε. Η πράξη της αφαίρεσης, πλην συγκεκριμένων περιπτώσεων για λόγους πρακτικής, δεν απαιτεί κάτι ιδιαίτερο και καλύπτεται από την λογική της αποφυγής αλλοίωσης του κατασχεθέντος καθόσον, αν αυτό δεν είναι επικίνδυνο για την δημόσια ασφάλεια, τότε ενδέχεται να επιστραφεί στον κάτοχο από τον οποίον αφαιρέθηκε ή να αιτηθεί, σε ορισμένες περιπτώσεις, την επανάκτησή του ο άσχετος με την αξιόποινη πράξη ιδιοκτήτης του.

Οι ιδιαιτερότητες όμως των ψηφιακών στοιχείων (δεδομένων και πειστηρίων) δεν ήταν δυνατόν να καλυφθούν μέσα από το γενικό φάσμα της διαχείρισης των αντικειμένων της κατάσχεσης. Έτσι, πολύ ορθά και σε συμμόρφωση με τις τεχνικές πρακτικές και λογικές, ο νομοθέτης αξιώνει την χρήση *κατάλληλου εξοπλισμού* από τον ερευνητή. Καίτοι θα ήταν περιπτωσιολογικά εύκολο κι ευχερές να καθοριστούν τα μέσα αυτά σήμερα με επιλογή από τις πολλές προτάσεις που διατίθενται, ωστόσο ορθότατα ο νομοθέτης δεν προχώρησε σε μια τέτοια λογική αλλά καθόρισε τα πλαίσια δίδοντας τα κριτήρια που πρέπει να πληρούνται κατά την ειδική αυτή κατάσχεσης των ψηφιακών δεδομένων. Και τούτο είναι και ορθολογικό καθόσον η αλματώδης εξέλιξη της τεχνολογίας, σαφώς δημιουργεί ολοένα απαιτήσεις για βελτιωμένες ή καινοτόμες επιλογές.

Έτσι στο άρθρο 265 § 2 Κ.Ποιν.Δ. καθόρισε τις απαιτήσεις που πρέπει να καλύπτονται και άφησε την επιλογή των μέσων στον εκάστοτε ερευνητή. Η λογική του πράγματος επιβάλλει βέβαια επιλογές μέσα από τις τεχνικώς παραδεδεγμένες κι αποδεκτές επιλογές από το σύνολο των προτάσεων που υπάρχουν.

Στα πλαίσια αυτά εκείνος, ο οποίος διεξάγει την έρευνα πρέπει να έχει κατάλληλο εξοπλισμό, που να επιτρέπει την αφαίρεση και την κατάσχεση του υλικού φορέα, στο οποίο βρίσκονται αποθηκευμένα τα δεδομένα, την αντιγραφή και την αφαίρεση των αποθηκευμένων ψηφιακών δεδομένων σε μέσο αποθήκευσης δεδομένων, την αναπαραγωγή και την επαλήθευση της αυθεντικότητας και της ακεραιότητας των κατασχεθέντων δεδομένων. Τέτοιος εξοπλισμός αποτελείται τόσο από ειδικές υπολογιστικές μηχανές (Write Blocker, Forensic Combo Dock, Tableau SATA Bridge), ειδικά λογισμικά ανάλυσης και κρυπτογράφησης (autopsy, SHA-1, MD5) αλλά και απλά τεχνικά εργαλεία (κατσαβίδια κοινά και ακριβείας ωρολογοποιών, κινητών, Η/Υ, Am-Tech L0475, πένσα, τσιμπίδα, καρυδάκια).

Στην περίπτωση εκείνη κατά την οποίαν, ο πρώτος αποκριτής δεν διαθέτει τον εξοπλισμό αυτόν (ή αντίστοιχο και αποδεκτό από τις τεχνολογικές κοινότητες) ή τις ειδικές γνώσεις αναφορικά με μια τέτοια ειδική κατάσχεση και τις απαιτήσεις που εγείρονται, επιβάλλεται η ασφάλιση του χώρου, ως πρώτη ενέργεια και η αναμονή ειδικού ερευνητή που να πληρεί γνωστικά και εξοπλιστικά πρότυπα.

Κατωτέρω στην διαδικαστική πρακτική προσέγγιση της δέσμευσης των ψηφιακών πειστηρίων, γίνεται ειδικότερη αναφορά στον εξοπλισμό του ερευνητή αλλά και στην διαδικαστική προσέγγιση και το πλάνο εργασίας στον χώρο, μέχρι και την ασφαλή αποθήκευση του υλικού. Για τον λόγο αυτόν δεν γίνεται περαιτέρω ανάπτυξη στο σημείο αυτό, αλλά παραπέμπουμε στην αντίστοιχη θέση[244] για λεπτομερέστερες καταγραφές.

Αφού λοιπόν υπάρχει ο κατάλληλος εξοπλισμός, διαδικαστικά περιγράφεται στην § 2 η πρακτική δομής της κατάσχεσης, η οποία είναι ανάλογη με το στοιχείο που κατάσχεται. Έτσι, η κατάσχεση εφόσον αναφέρεται σε σύστημα υπολογιστή της α΄ περ. της 1ης παραγράφου γίνεται με την αφαίρεση και την κατάσχεση του υλικού φορέα στον οποίο βρίσκονται αποθηκευμένα τα ενδιαφέροντα δεδομένα. Αν τώρα η κατάσχεση αφορά σε ψηφιακά δεδομένα της β΄ περ. της 1ης παραγράφου, τότε η κατάσχεση λαμβάνει χώρα με την αντιγραφή και την αφαίρεση των αποθηκευμένων ψηφιακών δεδομένων σε μέσο αποθήκευσης δεδομένων. Σε κάθε δε περίπτωση στην ολοκλήρωση της πράξης κατάσχεσης περιλαμβάνεται και η αναπαραγωγή και η επαλήθευση της αυθεντικότητας και της ακεραιότητας των κατασχεθέντων δεδομένων.

Σε μια εντελώς πρακτική προσέγγιση ο ερευνητής θα εισχωρήσει, με τους παραδεδεγμένους τεχνικά τρόπους, στο σύστημα, εντοπίσει το ενδιαφέρον ψηφιακό υλικό, θα το αντιγράψει, χωρίς να το αλλοιώσει, θα το αφαιρέσει και θα το ασφαλίσει με την μορφή κρυπτογράφησης που θα επιτρέπει την επαλήθευση της αυθεντικότητας και της ακεραιότητας (MD-5, SHA-1).

viii. Η ειδική έκθεση της § 3.

Για την έννοια και την σχέση της *έκθεσης*, ως διαδικαστικής δικονομικής ενέργειας, με την προδικασία κατά τον Κ.Ποιν.Δ. έγινε σχετική αναφορά σε προηγούμενη θέση και τούτο για να μην γίνονται αναπτύξεις και εκτενείς αναφορές στο σημείο αυτό, οι οποίες

[244] Βλ. κατωτέρω υπό 10. Πρωτόκολλο έρευνας και διαχείρισης των ψηφιακών πειστηρίων και των ψηφιακών δεδομένων, *στ.στ. Μεταφορά και αποθήκευση των κατασχεθέντων*. σελ. 191 επ.

ενδεχόμενα, καίτοι απαραίτητες για την κατανόηση του κειμένου, θα αποπροσανατόλιζαν την ανάλυση αναφορικά με το κεντρικό ζήτημα της μελέτης. Για την έκθεση λοιπόν ως διαδικαστική πράξη και τις προϋποθέσεις του υποστατού της, κυρίως όμως για την ουσιαστική της αξία στην προδικασία και την αποδεικτική της ισχύ, έγινε αναφορά σε προηγούμενη ενότητα[245] της μελέτης αυτής και φυσικά οι βασικές θέσεις και τα νομικά χαρακτηριστικά της διατηρούν την σημασία και την αξία τους και στην θεματική αυτήν.

Η έκθεση που προβλέπεται ως διαδικαστική πράξη στην § 3 του άρθρου 265 Κ.Ποιν.Δ., είναι *ειδική*. Δεν παύει όμως να ορίζεται ως έκθεση και ως τέτοια συνεπώς πρέπει πρώτα από όλα να πληρεί τα τυπικά στοιχεία του άρθρου 148 επ. Κ.Πολ.Δ.[246] δηλαδή, σε πολύ λακωνική ανάπτυξη, να έχει έγγραφη μορφή, να συντάσσεται από δημόσιο υπάλληλο, ο οποίος έχει σχέση με την συγκεκριμένη ανακριτική διαδικασία, όπως είναι στην περίπτωσή μας ο ανακριτικός υπάλληλος της έρευνας, να διαλαμβάνει τόπο και χρόνο σύνταξης, με την μεγαλύτερη δυνατή ακρίβεια. Η προσοχή μας όμως εστιάζει στο γεγονός ότι η έκθεση αυτή πρέπει να είναι *ειδική*. Και τούτο με την έννοια του να διαλαμβάνει τα ειδικότερα εκείνα στοιχεία που απαιτεί μια παρουσίαση ειδικών απαιτήσεων όταν η αναφορά γίνεται επί ειδικών στοιχείων, όπως είναι τα ψηφιακά. Όπως η έκθεση μαρτυρικής κατάθεσης διαλαμβάνει οτιδήποτε κατέθεσε ο εξετασθείς μάρτυρας και όπως αυτός τα κατέθεσε, έτσι και στην περίπτωση της παρουσίασης της ανακριτικής ενέργειας θα πρέπει να διαλαμβάνονται στην έκθεση όλα τα στοιχεία που έλαβαν χώρα, αλλά με τρόπο που να διατηρεί την μορφή της καταγραφής και όχι της επεξήγησης (που είναι άλλη διεργασία και μας απασχολεί σε άλλο σημείο, εκείνο της *παρουσίασης*).

Κατά τη ρητή νομοθετική επιταγή, η ειδική έκθεση πρέπει να αναφέρει *ειδικώς τις ενέργειες* που πραγματοποιεί εκείνος που διεξάγει την ανάκριση. Ειδικότερα, να αναφέρει τον εντοπισμό ενδιαφερόντων ψηφιακών δεδομένων, την θέση που αυτά βρέθηκαν, την ηλεκτρονική διαδρομή που ακολούθησε ο ανακριτικός υπάλληλος για να τα εντοπίσει, την αφαίρεση και την κατάσχεση του υλικού φορέα, στο οποίο βρίσκονται αποθηκευμένα τα δεδομένα, την αντιγραφή και την αφαίρεση των αποθηκευμένων ψηφιακών δεδομένων σε μέσο αποθήκευσης δεδομένων. Η αναφορά των ενεργειών αυτών πρέπει να είναι συγκεκριμένη, σαφής, εύληπτη και κατανοητή, ώστε να μην καταλείπεται καμιά αμφιβολία αναφορικά με τις ενέργειες του ανακριτικού υπαλλήλου.

[245] Βλ. ανωτέρω υπό 4. Η Σημασία των Ψηφιακών Πειστηρίων στην Ανακριτική Έρευνα, *iii. Η έκθεση ως δομικό στοιχείο στο σχηματισμό της ποινικής δικογραφίας* σελ. 46 επ.
[246] Βλ. ανωτέρω, υπό 4. Η Σημασία των Ψηφιακών Πειστήριων στην Ανακριτική Έρευνα, *iii. Η έκθεση ως δομικό στοιχείο στο σχηματισμό της ποινικής δικογραφίας*, σελ. 46 επ.

Σημαντικό στοιχείο για μια τέτοια καταγραφή είναι το audit trail, η αναφορά (report) ενεργειών του ερευνητή που αναδεικνύει βήμα – βήμα (καταγραφή σε πραγματικό χρόνο με χρονοσήμανση) τις ηλεκτρονικές διεργασίες που επεχείρησε κατά την αναζήτηση, ώστε να μην υπάρχει καμιά αμφιβολία για την μεθοδολογία, τον εντοπισμό, την θέση και τον φυσικό υλικό φορέα του ψηφιακού δεδομένου[247], αλλά και την τήρηση όλων των παραδεδεγμένων τεχνικών αρχών έρευνας. Χωρίς το audit trail εκτιμώ ότι η ειδική αυτή έκθεση δεν δίνει την σημαντική πληροφορία που απαιτείται σε μια υπόθεση κατάσχεσης ψηφιακών δεδομένων, όπου ο κάθε χειρισμός του ερευνητή πρέπει να ελέγχεται και να αξιολογείται καθόσον ενδεχόμενα σφάλματα μπορεί να μεταβάλλουν πλήρως το αποτέλεσμα και συνεπώς την απεικόνιση της αλήθειας.

Η έκθεση αυτή θα είναι το *εισαγωγικό (συνοδευτικό) έγγραφο της ψηφιακής απόδειξης* στην δίκη. Ενδεχόμενος εντοπισμός ψηφιακών στοιχείων στην ποινικής δικογραφία, που δεν διαλαμβάνονται ως καταγραφή και δεν εμπεριέχονται ως παρουσίαση ενεργειών έρευνας στην ειδική έκθεση, δεν μπορούν να γίνουν δεκτά για αποδεικτική αξιοποίηση[248].

Η κρισιμότητα λοιπόν του περιεχομένου της ειδικής έκθεσης αναδεικνύεται μέσα από τις συνέπειες στην περίπτωση που προσβληθεί, οπότε επέρχονται οι δικονομικές συνέπειες όχι τόσο οι τυπικές του άρθρου 153 (ακυρότητα) όσο του άρθρου 152 Κ.Ποιν.Δ., αναφορικά με το ουσιαστικό περιεχόμενό της. Εδώ εγείρονται σημαντικά θέματα καθόσον κατά την ρητή πρόβλεψη του νομοθέτη «*Η έκθεση έχει αποδεικτική δύναμη ωσότου αποδειχθεί το αντίθετο. Για όσα όμως βεβαιώνονται σ` αυτήν ότι έγιναν από δημόσιο υπάλληλο η έκθεση έχει αποδεικτική δύναμη ωσότου προσβληθεί για πλαστότητα. Αυτό δεν εμποδίζει πάντως τον δικαστή να εκτιμήσει το περιεχόμενο της έκθεσης ελεύθερα.*»[249]. Με άλλα λόγια μπορεί να εμφανιστεί στην δίκη ένα αρχείο το οποίο να μην εμπεριέχεται στον κατάλογο των σχετικών καταγραφών του ανακριτικού υπαλλήλου και η έκθεση απλά να *εκτιμηθεί* (βάσει της συγκεκριμένης έλλειψης της έκθεσης) *ελεύθερα* από τον δικαστή; Και αν το αρχείο αυτό είναι εκείνο που θα στηρίξει την καταδίκη; Πότε θα το πληροφορηθεί ο κατηγορούμενος για να ενεργοποιήσει το δικαίωμα που έχει στην υπεράσπισή του βάσει κατηγορίας για την οποία

[247] Για να αποφευχθούν σκέψεις ενδεχόμενης έκνομης συμπεριφοράς ερευνητή, που θα «φυτέψει» παράνομο ψηφιακό δεδομένο κατά την έρευνα. Οι λόγοι που δεν μπορεί να αποκλειστεί ένα τέτοιο ενδεχόμενο δεν είναι θεωρητικοί και αναπτύσσονται σε άλλο σημείο της έρευνας.

[248] Λ.χ. στην περίπτωση που έχει κατασχεθεί κινητό μάρκας Χ με αριθμό ΙΜΕΙ 123456, αλλά κατά την παράδοσή του στον αναλυτή (τμήμα ψηφιακών πειστηρίων), εντοπίζεται μέσα σε αυτό κάρτα SIM που δεν είχε περιληφθεί στην ειδική έκθεση.

[249] Βλ. *Μ. Γεωργιάδου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, τομ. Ι, Νομική Βιβλιοθήκη 2018, σελ. 1590, με τις εκεί παραπομπές σε Π. Καίσαρη, σύμφωνα με την οποία η έκθεση παραμένει έγκυρη ακόμη και αν συντάχθηκε από αναρμόδιο ανακριτικό υπάλληλο.

πληροφορήθηκε εγκαίρως (ώστε να έχει τον απαιτούμενο χρόνο για την προετοιμασία της υπεράσπισής του);

Κατά την εκτίμησή μου η πρόβλεψη του άρθρου 265 § 3 Κ.Ποιν.Δ., δεν μπορεί να ενταχθεί πλήρως στην λογική των λοιπών εκθέσεων των άρθρων 148 επ. Κ.Ποιν.Δ. Ο λόγος της θέσης αυτής δεν είναι μόνο η αναφορά της στο νόμο ως *ειδικής*, αλλά το ουσιαστικό της περιεχόμενο και η βαρύτητά της για την διασφάλιση των δικαιωμάτων του κατηγορουμένου στην ποινική δίκη. Αν μέσα στις σκέψεις αυτές εξειδικεύσουμε το δικαίωμα πληροφόρησης του κατηγορουμένου, άμεσα έχουμε μια βάση για τον προβληματισμό μας. Ο κατηγορούμενος πρέπει να προετοιμαστεί βάσει του υλικού που έχει δεσμευτεί μέχρι και την τελευταία πρόσκλησή του για απολογία, καθόσον κάθε νέα ανακριτική πράξη μετά την απολογία του κατηγορουμένου, επιβάλλει την εκ νέου κλήτευση και ακρόασή του.

Η σημασία λοιπόν της ειδικής έκθεσης αναφέρεται στο στοιχείο της ενημέρωσης και της πληροφόρησης αναφορικά με το υλικό της απόδειξης, το οποίο στηρίζει την πρόοδο της διαδικασίας, κατ' αρχήν in rem αλλά ενδεχομένως και εναντίον συγκεκριμένου κατηγορουμένου (in personam) και είναι ζωτικής σημασίας για την τήρηση της νομιμότητας της διαδικασίας. Αυτό με τη σειρά του ως παραδοχή οδηγεί στο επόμενο ζήτημα, το οποίο έχει να κάνει με το ουσιαστικό περιεχόμενο της ειδικής έκθεσης.

Η προσλαμβάνουσα παράσταση από την μέχρι σήμερα πρακτική εφαρμογή της διάταξης του άρθρου 265 § 3 Κ.Ποιν.Δ. (ομολογουμένως ολιγόμηνη), δεν διαφέρει ιδιαίτερα από τις παραστάσεις στις συνήθεις εκθέσεις κατάσχεσης. Εκείνο, από τα ουσιαστικά ενδιαφέροντα σημεία, που καταγράφεται είναι το αντικείμενο της κατάσχεσης, σαφώς με όλα τα στοιχεία εξατομίκευσής του. Διατηρείται ο λακωνικός χαρακτήρας στην σύνταξη, αλλά σε καμιά περίπτωση δεν υπάρχει η καταγραφή των ενεργειών έρευνας, όπως απαιτεί ο νόμος. Μια περιπτωσιολογική αναφορά ελλείψεων, στην βάση καταγραφών (ομολογουμένως όχι πολλών) που περιήλθαν σε γνώση μου, ίσως θα αδικούσε πρακτικές κι επιλογές καθόσον δεν υπάρχει αξιόλογης έκτασης αριθμός περιπτώσεων, ώστε να εξαχθεί κατά το μάλλον ασφαλές συμπέρασμα.

Εφόσον λοιπόν σκοπός της ειδικής έκθεσης είναι η ασφαλής κατ' έκταση παρουσίαση της έρευνας ως διαδικαστικού γεγονότος, την ύπαρξη του οποίου καλείται να αναδείξει, η ειδική αυτή έκθεση, πέρα από τα βασικά στοιχεία της κοινής έκθεσης, θα πρέπει να διαλαμβάνει:

a. αναφορά των στοιχείων ταυτότητας και του γνωστικού πεδίου του πρώτου αποκριτή (λ.χ. πτυχίο σχολής πληροφορικής),
b. εάν κι εφόσον χρειάστηκε η συνδρομή περαιτέρω εξειδικευμένου ερευνητή, αναφορά των στοιχείων ταυτότητας και του γνωστικού πεδίου του τελευταίου,
c. το είδος του υλισμικού που κατάσχεται, ανά κατηγορίες, ήτοι:
    i. σύστημα υπολογιστή, κινητή μονάδα (laptop), ταμπλέτες (tablets), έξυπνα τηλέφωνα (smartphones), με σαφή καταγραφή ανά εργοστάσιο κατασκευής, τύπο, τεχνικά χαρακτηριστικά προσδιοριστικά του συστήματος, αριθμό ταυτότητας που φέρει κατά την ένδειξη κατασκευής, περιγραφή (λ.χ. διαστάσεις, χρωματισμός) και όποιο άλλο στοιχείο εξαντλεί τα ζητήματα ταυτότητας του αντικειμένου. Σε καθένα στοιχείο θα πρέπει να δίδεται χωριστός αριθμός πειστηρίου κατ' επιλογή του ανακριτικού υπαλλήλου που ενεργεί και την ταξινόμηση, φωτογραφία ενός εκάστου αντικειμένου,
    ii. μέσο αποθήκευσης δεδομένων υπολογιστή στο οποίο υπάρχουν αποθηκευμένα δεδομένα υπολογιστή που κατάσχεται, όπως usb, memory sticks, sd cards (mini και micro), Smart Media (SM), με σαφή καταγραφή ανά εργοστάσιο κατασκευής, τύπο, τεχνικά χαρακτηριστικά προσδιοριστικά του υλικού, αριθμό ταυτότητας που φέρει κατά την ένδειξη κατασκευής, περιγραφή (λ.χ. διαστάσεις, χρωματισμός) και όποιο άλλο στοιχείο εξαντλεί τα ζητήματα ταυτότητας του αντικειμένου. Σε καθένα στοιχείο θα πρέπει να δίδεται χωριστός αριθμός πειστηρίου κατ' επιλογή του ανακριτικού υπαλλήλου που ενεργεί και την ταξινόμηση, φωτογραφία ενός εκάστου αντικειμένου,
    iii. περιφερειακά συστήματα που συλλειτουργούν με τον υπολογιστή με σαφή καταγραφή ανά εργοστάσιο κατασκευής, τύπο, τεχνικά χαρακτηριστικά προσδιοριστικά του υλικού, αριθμό ταυτότητας που φέρει κατά την ένδειξη κατασκευής, περιγραφή (λ.χ. διαστάσεις, χρωματισμός) και όποιο άλλο στοιχείο εξαντλεί τα ζητήματα ταυτότητας του αντικειμένου. Σε καθένα στοιχείο θα πρέπει να δίδεται χωριστός αριθμός πειστηρίου κατ' επιλογή του ανακριτικού υπαλλήλου που ενεργεί και την ταξινόμηση, φωτογραφία ενός εκάστου αντικειμένου,

iv. το λειτουργικό του συστήματος που κατάσχεται και των εφαρμογών που φέρει αυτό εγκατεστημένα κατά την επέμβαση του ανακριτικού υπαλλήλου,

v. το router που εξυπηρετεί ενδεχόμενη διαδικτυακή σύνδεση (εφόσον υπάρχει),

vi. ψηφιακά δεδομένα ως αναφορά γεγονότος που ενδιαφέρει την έρευνα εφόσον εντοπίστηκε σε σύστημα υπολογιστή που λειτουργεί κατά την επέμβαση, λ.χ. κατέβασμα ύποπτου αρχείου με αναφορά των στοιχείων που το εξατομικεύουν (αρχείο .avi, .jpeg κλπ) και τα μεταδεδομένα που δίδονται αναφορικά με το κατέβασμα.

d. εφόσον γίνεται έρευνα σε κατοικία, την παραμονή κι επίβλεψη καθ' όλη την διαδικασία από τον εκπρόσωπο της δικαστικής αρχής,

e. την αναφορά (report) στη βάση της λογικής audit trail,

f. την δικτύωση στον χώρο, με αναφορά τεχνικών δεδομένων, αλλά και οποιαδήποτε άλλη δικτύωση εντοπίζεται στον χώρο και σχετίζεται με την ερευνώμενη IP, λ.χ. τοπικό δίκτυο (LAN), ενσύρματη σύνδεση από router που βρίσκεται σε άλλο χώρο,

g. την ερευνώμενη IP (που θα προκύπτει πάντα από το βούλευμα που επέτρεψε την άρση του απορρήτου ηλεκτρονικών επικοινωνιών),

h. την αναφορά του λογισμικού ανίχνευσης που χρησιμοποιήθηκε για τον εντοπισμό υπόπτων στοιχείων στο ερευνώμενο υλικό,

i. τα στοιχεία του παρόχου υπηρεσιών νεφοϋπολογιστικής (αν βρέθηκε υλικό),

j. τα στοιχεία του παρόχου ηλεκτρονικών υπηρεσιών επικοινωνίας και διαδικτυακής πρόσβασης,

k. την αναφορά περί δημιουργίας (προχείρου) σκαριφήματος για την συνδεσμολογία.

l. την ψηφιακή απεικόνιση της εισόδου στον χώρο, ήτοι λήψη πριν την επέμβαση του ανακριτικού υπαλλήλου και εποπτεία των ερευνών.

m. αναφορά στην ασφαλή δέσμευση και προστασία των κατασχεθέντων με αναφορά στο μέσο που χρησιμοποιήθηκε σε κάθε περίπτωση (λ.χ. σακούλα faraday) με επεξήγηση της επιλογής του υλικού,

n. ενέργειες και λογισμικά που χρησιμοποιούνται και που αφορούν στην αναπαραγωγή και την επαλήθευση της αυθεντικότητας και της ακεραιότητας των κατασχεθέντων δεδομένων.

Η έκθεση υπογραφόμενη από τα πρόσωπα που ορίζει ο νόμος, παρέχει μια ασφαλιστική δικλείδα από τον κίνδυνο μη νόμιμα συλλεγέν ή επιλεγέν υλικό, να προστεθεί εν αγνοία του κατηγορουμένου ή χωρίς την δυνατότητά του να προβάλλει αντιρρήσεις. Μπορεί η ανωτέρω απαρίθμηση να φαντάζει υπερβολική αλλά μπροστά στον κίνδυνο μιας ακυρότητας, η υπερβολή στην καταγραφή, όχι στην κατάσχεση καθεαυτή, είναι αποδεκτή επιβάρυνση του ανακριτικού έργου, αν και από πλευράς δογματικής θέσης, ό,τι εξασφαλίζει την αλήθεια (και την ακρίβεια) δεν είναι ποτέ υπερβολικό.

Στο σημείο αυτό προτείνεται η ψηφιοποίηση της ειδικής έκθεσης ή τουλάχιστον η παράλληλη παρουσία της στην δικογραφία. Ο συνδυασμός ψηφιακής απόδοσης και έγγραφης κατάδειξης των στοιχείων, είναι μέτρο που λειτούργησε με επιτυχία στον χώρο του διοικητικού δικαίου και δη στις ενδικοφανείς προσφυγές του Ν 4174/2013, όπου το σύνολο των σχετικών εγγράφων και στοιχείων που συνοδεύουν την ενδικοφανή προσφυγή του ελεγχομένου, υποβάλλονται τόσο εγγράφως όσο και ψηφιακά, απαίτηση που σχετίζεται με το παραδεκτό της ενδικοφανούς προσφυγής.

Η συγκεκριμένη πρόταση βασίζεται στην προσπάθεια εξεύρεσης μιας εξασφάλισης της αληθινής εικόνας του τόπου και στον χρόνο της έρευνας κάτι που παράλληλα εξυπηρετεί, με την έννοια της εξασφάλισης, τα δικαιώματα του κατηγορουμένου και δη εκείνο που αναφέρεται στην δίκαιη δίκη. Δεν είναι λίγες οι περιπτώσεις που τα αποτελέσματα μιας ανακριτικής έρευνας αμφισβητούνται από τον κατηγορούμενο ή τον νομικό του παραστάτη. Για τα ηλεκτρονικά εγκλήματα, που λογίζονται ως ιδιαίτερα βαριά, το ζήτημα αποκτά ιδιαίτερα βαρύνουσα σημασία καθόσον ατομικά δικαιώματα όπως η ατομική ελευθερία, περιορίζονται ή περιστέλλονται από το αποτέλεσμα μιας έρευνας.

Το γεγονός ότι ο ελεγχόμενος πολίτης ενδεχόμενα δεν έχει ειδικές γνώσεις αναφορικά με τα δικαιώματά του, όπως εκείνο της προσφυγής σε δικηγόρο της επιλογής του, σε συνδυασμό με την αίσθηση ότι η αναζήτηση συνηγόρου υπεράσπισης μπορεί να αξιολογηθεί ως ομολογία ενοχής, αφήνει πολλούς εκτεθειμένους σε υπηρεσιακές υπερβολές ανακριτικών υπαλλήλων.

Θα μπορούσε να αναρωτηθεί κανείς ποιο μπορεί να είναι το συμφέρον της δίωξης να παρανομήσει και πώς μπορεί να αποδίδεται σε αστυνομικό – ανακριτικό υπάλληλο μια τέτοια κατηγορία. Οι σχετικές απαντήσεις σε τέτοια επιχειρήματα, δίδονται κατωτέρω[250]. Για

[250] Βλ. κατωτέρω υπό αρ. 9. Οι Αρχές που Διέπουν την Έρευνα αναφορικά με τα Ψηφιακά Πειστήρια και τα Ψηφιακά Δεδομένα, *ΣΤ) η αρχή της απόδειξης της νόμιμης δράσης της υπεύθυνης Αρχής*, σελ. 167, όπου η σχετική πρόταση για τον καθορισμό των αρχών που διέπουν την ψηφιακή ανακριτική έρευνα.

τις ανάγκες της εδώ αναφοράς, πρέπει να σημειώσω ότι δυστυχώς οι φόβοι επιβεβαιώνονται από την ίδια την πρακτική και τη σειρά από περιπτώσεις κατάχρησης εξουσίας που απασχόλησαν τη νομολογία[251].

Απλή αναφορά στις σειρές υποθέσεων δήθεν εξιχνίασης εγκληματικών οργανώσεων, που μέσα από μια πολυτελή, συνήθως τηλεοπτική, κι εκκωφαντική ενημέρωση του κοινού κατά τις σωρηδόν προσαγωγές, υπό το φως των καμερών και με τις μεγαλόσχημες αποδόσεις συγχαρητηρίων στους διευθυντές σχηματισμών και προϊσταμένους τμημάτων της ΕΛΑΣ, καταλήγουν, μετά από χρόνο και μακριά από τις κάμερες πλέον, στο σύνηθες «φιάσκο» της απαλλαγής των κατηγορουμένων στις δικαστικές αίθουσες. Εδώ το ζήτημα δεν είναι η αποδεικτική υποστήριξη της κατηγορίας αλλά τα οφέλη που, μέχρι την απαλλαγή (και ανεξάρτητα από αυτήν) του κατηγορουμένου, αποκόμισαν αξιωματικοί στις ετήσιες λεγόμενες «κρίσεις». Σαφώς μια εξιχνίαση ενός ηλεκτρονικού εγκλήματος δεν έχει να δώσει πολλά αν δεν καταλήξει σε κατηγορούμενο. Αν όμως αποδοθεί τελικά κατηγορία, τότε «κάποιος» έχει οφέλη. Και δυστυχώς όλα τα ανωτέρω δεν είναι εικασίες, αλλά σαφώς δεν έχουν άμεση σχέση με το αντικείμενο της έρευνας και σταματά εδώ η ανάπτυξη του προβληματισμού.

Όπως καταδεικνύεται και κατωτέρω, όπου η προαναφερομένη παραπομπή, ακόμη και αυτή η παρουσία του αντιπροσώπου της δικαστικής αρχής στις κατ' οίκον έρευνες, δεν εξασφαλίζει την τήρηση της νομικής ορθότητας και αρτιότητας μιας έρευνας την οποία ο δικαστικός λειτουργός (συνήθως βαθμός Ειρηνοδίκη) δεν έχει τις απαραίτητες τεχνικές γνώσεις για να την εποπτεύει, ήτοι να παρέμβει εκεί που εκτιμά ότι κάτι δεν εκτελείται ορθολογικά.

Με απουσία συνεπώς συνηγόρου υπεράσπισης, ή στην καλύτερη εκδοχή τεχνικού συμβούλου, με όλα τα προαναφερόμενα αρνητικά παραδείγματα, με τα οποία μας τροφοδοτεί η νομολογία, εκτιμώ ότι ο πιο ανώδυνος τρόπος για την διασφάλιση της νομιμότητας στην διαδικασία, την πλήρη απόδειξη της τήρησης της νομιμότητας αυτής αλλά και της προστασίας του ίδιου του ανακριτικού υπαλλήλου από κακόβουλες μομφές στα πλαίσια μιας υπερασπιστικής τακτικής από την πλευρά του κατηγορουμένου, η *ψηφιακή καταγραφή* είναι μια καλή (ασφαλής) πρόταση. Κανείς δεν έχει να χάσει κάτι, τουναντίον όλοι έχουν να κερδίσουν, και πάνω από όλους η δικαιοσύνη, από την *ψηφιακή καταγραφή*

[251] Βλ. κατωτέρω υπό αρ. 9. Οι Αρχές που Διέπουν την Έρευνα αναφορικά με τα Ψηφιακά Πειστήρια και τα Ψηφιακά Δεδομένα, *ΣΤ) η αρχή της απόδειξης της νόμιμης δράσης της υπεύθυνης Αρχής*, ο.π., αναφορά σε πραγματικά περιστατικά διαρροών και ενδεχόμενης αλλοίωσης δεδομένων ποινικής δικογραφίας σε περίπτωση ανθρωποκτονίας από πρόθεση.

όλων των ενεργειών από την έναρξη της επέμβασης μέχρι την τελική αποχώρηση των ανακριτικών υπαλλήλων. Η απεικονιστική ψηφιακή καταγραφή *πριν από την είσοδο* και μέχρι και την αποχώρηση και ασφάλιση του χώρου, ως τελευταία πράξη της έρευνας, με την πλήρη ανάπτυξη και κατάδειξη των ανακριτικών ενεργειών (που σαφώς πρέπει να καταγράφονται και στην ειδική έκθεση κατά την ρητή επιταγή του νόμου – αρ. 265 § 3 Κ.Ποιν.Δ.) δεν θα επιτρέψουν καμιά αμφισβήτηση αναφορικά με το τί τελικά εντοπίστηκε, πώς, από ποιόν, πού και πότε.

Αντίθετη επιχειρηματολογία, η οποία θέλει την παράμετρο του κόστους σε μια τέτοια εκδοχή, μάλλον δεν είναι επιχείρημα αλλά υπεκφυγή. Η λήψη σε ψηφιακή μορφή μπορεί να καλυφθεί με την σχετική εφαρμογή καταγραφής εικόνας ήχου ενός έξυπνου τηλεφώνου ή μια ψηφιακής μηχανής που θα αποτελεί ιδιοκτησία της ερευνητικής αρχής. Το προϊόν της καταγραφής (πάντα με χρονοσήμανση λήψης) μπορεί να διατηρηθεί σε υπολογιστική νέφους ή τελικά να αποθηκευτεί σε μέσο αποθήκευσης, το οποίο μπορεί να φιλοξενήσει και άλλες καταγραφές άλλων υποθέσεων, ή να αποτελέσει ψηφιακό τμήμα του digital copy, που θα συσχετισθεί στην δικογραφία. Ουσιαστικά το κόστος είναι μηδενικό, η ωφέλεια για την διαφύλαξη του χαρακτήρα της εκδίκασης ως δικαίας, τεράστια.

ix. Το αντίγραφο των κατασχεθέντων ψηφιακών δεδομένων και η φύλαξη των ψηφιακών πειστηρίων.

Η ιδιαιτερότητα των ψηφιακών δεδομένων και των υλικών φορέων τους, διαμόρφωσε μια ιδιαίτερη κατηγορία στην διαδικασία της κατάσχεσης ακόμη και στο ζήτημα της αποθήκευσής τους. Έτσι δεν ενέταξε την μετά την κατάσχεση διαχείρισή τους στην γενική πρόβλεψη περί φύλαξης και σφράγισης των πραγμάτων που κατασχέθηκαν του αρ. 268 Κ.Ποιν.Δ. Σύμφωνα λοιπόν με την κοινή για την κατάσχεση αντικειμένων, πρόβλεψη του κώδικα, την κατάσχεση ακολουθεί η φύλαξη των κατασχεθέντων στον γραμματέα του δικαστηρίου και αν τούτο δεν είναι εφικτό, για λόγους πρακτικούς (λ.χ. αν αντικείμενο της κατάσχεσης είναι ένα όχημα) διατάσσεται η φύλαξή του σε συγκεκριμένο φύλακα (αρ. 268 § 1 α΄ Κ.Ποιν.Δ.). Ειδική πρόβλεψη υπάρχει αν προκύπτει κίνδυνος συντήρησης του υλικού οπότε κατ' εξαίρεση επιβάλλεται στην περίπτωση αυτήν η εκποίηση ή καταστροφή των κατασχεθέντων. Ο νομοθέτης μερίμνησε ειδικά για την τύχη της αποθήκευσης των ψηφιακών δεδομένων σε ειδικότερη διάταξη, η οποία είναι εκείνη της § 4 του αρ. 265 Κ.Ποιν.Δ.

Σύμφωνα με την διάταξη αυτήν 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. Πρόκειται για *μερική ψηφιοποίηση* της ποινικής δικογραφίας. Όπως αναφέρθηκε αμέσως παραπάνω, ο συνδυασμός ψηφιακής απόδοσης και έγγραφης κατάδειξης των στοιχείων που συνοδεύουν αποδεικτικά ένα εισαγωγικό δικόγραφο, είναι μέτρο που λειτούργησε με επιτυχία στον χώρο του διοικητικού δικαίου και δη στις ενδικοφανείς προσφυγές του Ν 4174/2013.

Το σύνολο λοιπόν των αντληθέντων ψηφιακών δεδομένων συγκεντρώνεται σε ένα και μόνο ένα μέσο αποθήκευσης, το οποίο παραμένει στην δικογραφία ενώ οι υλικοί φορείς παρακολουθούν την διαδικασία αποθήκευσης σε ειδική προστατευτική συνθήκη (συσκευασία), σύμφωνα και με τις παραδεδεγμένες τεχνολογικές μεθόδους διασφάλισης από κινδύνους αλλοίωσης των ψηφιακών δεδομένων από μαγνητικά πεδία και υγρασία[252].

Κρισιμότατη είναι η πρόβλεψη αναφορικά με την εξαγωγή αντιγράφου των αποθηκευμένων ψηφιακών δεδομένων στο μέσο αποθήκευσης που βρίσκεται στην δικογραφία, κατά τα ανωτέρω αναφερόμενα. Πρόκειται για αντίγραφο, το οποίο δημιουργείται *κατά την ώρα της κατάσχεσης*, με βάση τις προσφερόμενες τεχνολογικές μεθόδους, οι οποίες τυγχάνουν αποδοχής από την επιστημονική κοινότητα της πληροφορικής, κι επιτρέπουν την αναπαραγωγή με την μορφή της μεταφοράς, του περιεχομένου του μέσου αποθήκευσης των δεδομένων με τρόπο ασφαλή. Είναι λοιπόν ξεκάθαρο ότι στο αρχείο αυτό συγκεντρώνονται τα ενδιαφέρονται ψηφιακά δεδομένα στα οποία έγινε η κατάσχεση και όχι οτιδήποτε βρέθηκε στον υλικό φορέα που τα φιλοξενούσε.

Η ευμεταβλητότητα και ευαισθησία των ψηφιακών δεδομένων ως ιδιαίτερο χαρακτηριστικό τους, επιβάλλει την ιδιαίτερη προσοχή στην διαχείριση των στοιχείων και ειδικότερα στην αναπαραγωγή τους όταν παραστεί ανάγκη. Τα ειδικότερα ζητήματα αναφορικά με την εξαγωγή των ψηφιακών δεδομένων από τους υλικούς φορείς, που κατασχέθηκαν και στους οποίους φιλοξενούνται, αναπτύσσονται λόγω της τεχνολογικής τους αυτοτέλειας σε διακριτή θεματική, αμέσως κατωτέρω[253], όπου και παραπέμπω προς απόδοση μιας πληρέστερης εικόνας της προβληματικής.

---

[252] Βλ. κατά τα ειδικότερα αναφερόμενα κατωτέρω υπό 10. Πρωτόκολλο Έρευνας και Διαχείρισης των Ψηφιακών Πειστηρίων και των Ψηφιακών Δεδομένων, ν. Η συλλογή αποδεικτικού υλικού, Β) Η τεχνική πλευρά της ερευνητικής προσέγγισης, *στ. Μεταφορά και αποθήκευση των κατασχεθέντων,* σελ. 190.

[253] Βλ. κατωτέρω υπό 8. Η Κατάσχεση των ψηφιακών δεδομένων (Κατ' άρθρο 265 Κ.Ποιν.Δ.), *x. Η άντληση απόδειξης (εξόρυξη) από τα ψηφιακά δεδομένα που εντοπίζονται στα κατασχεθέντα ψηφιακά πειστήρια*, σελ. 138 επ.

Στο σημείο αυτό όμως καταγράφω ότι με την εξαγωγή αντιγράφου διασφαλίζεται η δυνατότητα *ανάκτησης* των δεδομένων που έχουν κατασχεθεί, σε περίπτωση απώλειας ή καταστροφής. Περαιτέρω με τον τρόπο αυτόν αποφεύγεται ο κίνδυνος επέμβασης στο πρωτόλειο ψηφιακό στοιχείο, στον υλικό φορέα, σε συμμόρφωση προς την αρχή της διατήρησης της *ακεραιότητας* (integrity)[254]. Και τούτο καθόσον η ενδεχόμενη ενεργοποίηση του κατασχεθέντος ψηφιακού πειστηρίου (λ.χ. συστήματος υπολογιστή) ή η προσπέλαση του κατασχεθέντος αρχείου, θα δώσει διαφορετικά μεταδεδομένα, ίσως δε αλλοιώσει και το ίδιο το κρίσιμο ψηφιακό δεδομένο (ενδεχόμενα με ενεργοποίηση διαδικασίας αυτόματης διαγραφής λόγω ενεργοποίησης ειδικής εντολής, είτε με την διαγραφή λόγω παρόδου χρονικού διαστήματος που είχε καθοριστεί εξ ορισμού) με αποτέλεσμα το υλικό αυτό πλέον να εγείρει ζητήματα αξιοπιστίας και συνεπώς να καθίσταται μη αξιοποιήσιμο αποδεικτικά στην ποινική δίκη, ιδίως στην περίπτωση που απαιτηθεί η προσπέλαση του αρχείου σε κάποια στάση της δίκης.

Με την επιλογή αυτήν παρέχονται οι κατάλληλες εγγυήσεις φυσικής ασφάλειας και πρόσβασης σε εκείνους μόνο που ασκούν καθήκοντα στην υπόθεση, όπως είναι ο εισαγγελέας, ο ανακριτής, ο υπεύθυνος ανακριτικός υπάλληλος, που είναι επιφορτισμένος με την εποπτεία του ψηφιακού υλικού και ο γραμματέας της ανάκρισης. Η σχετική πρόβλεψη, κατά την ρητή αναφορά της διάταξης ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία.

Η πρόσβαση και η δυνατότητα αναπαραγωγής των ψηφιακών δεδομένων που κατάσχονται επιτρέπεται λοιπόν 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 (ND-5, SHA-1) και η χρήση κωδικών ασφαλείας για την πρόσβαση και αναπαραγωγή των κατασχεμένων ψηφιακών δεδομένων από το υλικό μέσο αποθήκευσης στο οποίο βρίσκονται αποθηκευμένα. Και στην περίπτωση αυτήν η σχετική πρόβλεψη, κατά την ρητή αναφορά της διάταξης ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία.

Ζήτημα φέρεται να εγείρεται αναφορικά με την *μορφή* του αντιγράφου των ψηφιακών δεδομένων που κατασχέθηκαν. Η διατύπωση της διάταξης της § 4 στα κρίσιμα σημεία της, αναφέρει «*4. Τα ψηφιακά δεδομένα που κατάσχονται διατηρούνται αποθηκευμένα …… σε ένα*

[254] Βλ. ανωτέρω υπό αρ. 9. Οι Αρχές που Διέπουν την Έρευνα αναφορικά με τα Ψηφιακά Πειστήρια και τα Ψηφιακά Δεδομένα, *Α) η αρχή ακεραιότητας (integrity)*, σελ. 160.

και μόνο υλικό μέσο αποθήκευσης που περιέχεται στη δικογραφία. Ασφαλές αντίγραφο αυτού …… σχηματίζεται κατά την κατάσχεσή τους και διατηρείται στο γραφείο πειστηρίων του πρωτοδικείου στο οποίο υποβάλλεται η δικογραφία…». Σύμφωνα με τις σχετικές παραγγελίες αρμοδίων εμπλεκομένων αρχών, το «ασφαλές αντίγραφο» είναι μια πανομοιότυπη αναπαραγωγή του ψηφιακού πειστηρίου, δηλαδή του υλικού φορέα που φιλοξενεί τα ψηφιακά δεδομένα. Έτσι για παράδειγμα στην περίπτωση κατασχεθέντος σκληρού δίσκου τύπου Χ, σχηματίζεται πλήρες αντίγραφο αυτού, με την έννοια τόσο του υλικού φορέα όσο και του περιεχομένου του. Εκτιμώ ότι μια τέτοια προσέγγιση δεν λαμβάνει υπόψη της το γράμμα της διάταξης αλλά και πρακτικά το μείζον ζήτημα της νεφοϋπολογιστικής. Αν την παρακολουθήσει κανείς, δεν μπορεί να εφεύρει τρόπο δημιουργίας ενός αντιγράφου του νέφους[255]. Συνεπώς η προσέγγιση αυτή κείται όχι απλώς εκτός γράμματος της διάταξης αλλά κι εκτός πνεύματος αυτής.

Η αναφορά σε «Ασφαλές αντίγραφο *αυτού*», ως αναφορικού συνδέσμου, παραπέμπει άμεσα στο αντικείμενο, που δεν είναι άλλο από το αναφερόμενο στην προηγούμενη περίοδο, ήτοι στο «*ένα και μόνο υλικό μέσο αποθήκευσης*», που περιέχει τα ψηφιακά δεδομένα. Αν λοιπόν γίνεται λόγος για την άντληση των ψηφιακών δεδομένων, και φυσικά γι αυτό γίνεται ο λόγος, τότε όλα τα κατασχεθέντα ψηφιακά δεδομένα, φιλοξενούνται σε «*ένα και μόνο υλικό μέσο αποθήκευσης*». Στο μέσο αποθήκευσης (digital copy) αναφέρεται το «αυτό» του β΄ εδαφίου της 4ης παραγράφου του αρ. 265 και συνεπώς η δημιουργία αντιγράφου του υλικού υποδοχέα (δηλαδή υλικό και δεδομένα σε ενιαίο όλο) δεν βρίσκει έρεισμα στο νόμο. Περαιτέρω η ψηφιακό αντίγραφο, αποτελούμενο από «*ένα και μόνο υλικό μέσο αποθήκευσης*», φιλοξενεί όλα τα ψηφιακά δεδομένα που κατασχέθηκαν και συνεπώς δεν είναι στην λογική της διάταξης η δημιουργία περισσοτέρων υλικών αντιγράφων που θα μείνουν στην δικογραφία.

Η διατύπωση της διάταξης αναφορικά με το ποιος έχει δικαίωμα πρόσβασης στο μέσο αποθήκευσης που τηρείται στην δικογραφία κατά την διάταξη του άρθρου 265 §§ 5 και 6 Κ.Ποιν.Δ. δεν αφήνει κανένα περιθώριο για διασταλτική ερμηνεία. Το σχετικό δικαίωμα για πρόσβαση και αναπαραγωγή (§ 5) φαίνεται ότι διατηρήθηκε για αμιγώς υπηρεσιακούς λόγους, στα πλαίσια της ενδελεχούς αξιολόγησης και αξιοποίησής του κι η σχετική πρόσβαση και δυνατότητα αναπαραγωγής των ψηφιακών δεδομένων που κατάσχονται επιτρέπεται μόνο σε όσους ασκούν δικαστικά, εισαγγελικά και ανακριτικά καθήκοντα στην υπόθεση ή τους γραμματείς. Ζήτημα γεννάται αναφορικά με την επιλογή των όρων

[255] Προφανώς κανείς δεν μπορεί να εννοήσει αναπαραγωγή ενός server.

πρόσβαση και *αναπαραγωγή*. Τί μπορεί να σημαίνει αναπαραγωγή, που μάλιστα μπορεί να την ενεργήσει και ο γραμματέας; Θέαση; Εκτιμώ πως δεν μπορεί να έχει τέτοιες αρμοδιότητες ο γραμματέας. Μπορεί να σημαίνει αντιγραφή; Μα αυτήν ρητά την απαγορεύει σε όλους η διάταξη της § 6 (επιφύλαξη μόνο για μια περίπτωση που δεν αφορά εδώ). Αν όμως σήμαινε απλή πρακτική πρόσβαση (επαφή) στο αρχείο (ουσιαστικά στον αποθηκευτικό φλασάκι), τότε η επανάληψη του όρου σε τι ωφελεί;

Σε κάθε πάντως περίπτωση στα πρόσωπα που προαναφέρθηκαν σίγουρα δεν μπορούμε να εντάξουμε τους διαδίκους καθόσον δεν είναι υπηρεσιακώς εμπλεκόμενα πρόσωπα και αυτό είναι το μοναδικό χαρακτηριστικό των προσώπων στα οποία επιτρέπεται η πρόσβαση. Και όταν αναφερόμαστε σε διαδίκους εννοούνται ο κατηγορούμενος και ο (ενδεχομένως) παραστάς προς υποστήριξη της κατηγορίας, αμέσως παθών ή ζημιωθείς από την πράξη για την οποία η κατηγορία και οι εκπρόσωποι αυτών (λ.χ. νομικός παραστάτης ή/και τεχνικός σύμβουλος).

Προς ενίσχυση των θέσεων αυτών λειτουργεί και η διατύπωση της § 6 σύμφωνα με την οποία «*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». Ο απόλυτος τρόπος διατύπωσης της διάταξης δεν επιδέχεται ερμηνεία. Η απαγόρευση αίρεται μόνο σε μια περίπτωση και αυτή είναι η συσχέτιση σε άλλη δικογραφία.

Από την άλλη όμως στην ποινική δίκη δεν ενδιαφέρει η δίωξη με κάθε κόστος. Το δικαίωμα πληροφόρησης του κατηγορουμένου και της πρόσβασής του στην δικογραφία, είναι ζήτημα κομβικής σημασίας. Λύση στον προβληματισμό δεν φαίνεται να δίνεται μέσα από την διάταξη του άρθρου 267 Κ.Ποιν.Δ., η οποία αναφέρεται σε χορήγηση αντιγράφων *εγγράφων* που κατασχέθηκαν σε εκείνον που τα κατείχε πριν την κατάσχεση. Αναλογική εφαρμογή δεν μπορεί να γίνει καθόσον το μεν η διάταξη αναφέρεται ρητά σε έγγραφα, το δε είναι ενταγμένη στο ειδικό κεφάλαιο για την κατάσχεση ως ανακριτική πράξη και ως τέτοιο συγκρούεται με την ειδικότερη διάταξη του άρθρου 265 §§ 5 και 6 Κ.Ποιν.Δ., που σαφώς ορίζουν διαφορετικά, όπως αναφέρθηκε και παραπάνω[256].

Λύση φαίνεται να χωρεί στην βάση της αναλογικής εφαρμογής των διατάξεων των άρθρων 100 και 147 Κ.Ποιν.Δ. Ειδικότερα, σύμφωνα με την διάταξη του άρθρου 100 § 1

[256] Βλ. ΕΔΔΑ απόφαση της 19/09/2019 (αρ. προσφ. 7268/10), https://www.echrcaselaw.com/category/ apofaseis- edda/page/14/

Κ.Ποιν.Δ., όταν, μετά την κλήτευσή του εμφανισθεί ή οδηγηθεί στον ανακριτή ο κατηγορούμενος για να αιτιολογηθεί, του ανακοινώνεται το περιεχόμενο του κατηγορητηρίου και των εγγράφων της ανάκρισης. Επιτρέπεται στον κατηγορούμενο να μελετήσει ο ίδιος ή ο συνήγορός του το κατηγορητήριο και τα έγγραφα της ανάκρισης, ενώ με γραπτή αίτηση του κατηγορουμένου και με δαπάνη του χορηγούνται σε αυτόν αντίγραφα του κατηγορητηρίου και των εγγράφων της ανάκρισης. Την ίδια υποχρέωση έχει ο ανακριτής, και τα ίδια δικαιώματα ο κατηγορούμενος, όταν κληθεί ξανά σε συμπληρωματική απολογία.

Η διάταξη κάνει λόγο για έγγραφα και κατηγορητήριο (επίσης έγγραφο). Την ίδια στιγμή ο υπέρτιτλος του άρθρου αναφέρεται σχετικά με τον κατηγορούμενο σε «*Δικαίωμα πρόσβασης στο υλικό της δικογραφίας. Ανακοίνωση των εγγράφων της ανάκρισης*». Ολόκληρο όμως το κείμενο της διάταξης πουθενά δεν αναφέρεται σε αποδεικτικό *υλικό* αλλά σε έγγραφα της δικογραφίας, ενώ σημαντικός λόγος γίνεται αναφορικά με το εάν ερμηνευτικά στην έννοια των εγγράφων της δικογραφίας εντάσσονται οι απολογίες των (τυχόν) λοιπών συγκατηγορουμένων του[257]. Δεν υπάρχει σε κανένα σημείο αναφορά σε δικαίωμα πρόσβασης σε *υλικό ή πειστήρια* που συνοδεύουν την δικογραφία, από την επισκόπηση ή τεχνική εξέταση των οποίων μπορεί να αντληθεί υλικό για υπερασπιστική επιχειρηματολογία και αμυντική στρατηγική. Οι διατάξεις αυτές φυσικά ενταγμένες στις βασικές – κοινές διατάξεις του γενικού μέρους του κώδικα περιέχουν τις δογματικές παραμέτρους και αποφεύγουν αναφορές σε ειδικά ζητήματα. Αν όμως τα ψηφιακά δεδομένα λογίζονται (και όντως είναι) ένα ειδικό αποδεικτικό στοιχείο, η έννοια αποδεικτικό υλικό, με τις αναφορές των άρθρων 177 επ. Κ.Ποιν.Δ. σε σειρά μορφών απόδειξης, δεν είναι κάτι το ειδικό. Μια επιχειρηματολογία μπορεί να στηριχθεί στο ότι αν ο νομοθέτης επέλεγε δικαίωμα του κατηγορουμένου στο σύνολο του αποδεικτικού υλικού θα το ξεκαθάριζε. Από την άλλη διασταλτική ερμηνεία προς το συμφέρον του κατηγορουμένου σαφώς και είναι αποδεκτή καθόσον ενισχύει και δεν προσβάλει τα δικαιώματά του. Σε μια τέτοια προσέγγιση όμως εγείρονται ζητήματα αναφορικά με την σύγκρουση διατάξεων και η κρίση στο έδαφος της ειδικότητας δεν άγει σε λύση υπέρ του κατηγορουμένου.

Και εξηγούμαι. Με την όποια διασταλτική προσέγγιση της διάταξης του δικαιώματος του κατηγορουμένου κατ' άρθρου 100 Κ.Ποιν.Δ.[258] δεν λύνεται ο προβληματισμός από την

[257] Βλ. *Θ. Δαλακούρας*, Ο Νέος Κώδικας Ποινικής Δικονομίας, συνοπτική ερμηνεία κατ' άρθρο του Ν 4620/2019, 2η εκδ. Νομική Βιβλ., 2019, σελ. 89.
[258] Βλ. *Γ. Νούσκαλης*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, τομ. Ι, Νομική Βιβλιοθήκη 2018, σελ. 555, με τις εκεί παραπομπές.

ρητή, περιοριστική αναφορά των προσώπων που δικαιούνται πρόσβασης και διαχείρισης του υλικού φορέα, που συμπυκνώνει και εμπεριέχει τα ψηφιακά δεδομένα ως υλικό της δικογραφίας κατά την διατύπωση του άρθρου 265 §§ 5 και 6 Κ.Ποιν.Δ. Διαγιγνώσκοντας κανείς σύγκρουση σε έδαφος διατάξεων κοινού τυπικού νόμου και δη του ιδίου νομοθετήματος, εγείρεται ως μέθοδος επίλυσης της προβληματικής η επιλογή βάσει της αρχής της ειδικότητας και αυτή οδηγεί σε λύση υπέρ του γράμματος του άρθρου 265 §§ 5 και 6 Κ.Ποιν.Δ.

Διαπίστωση κενού νόμου μέσα στο κείμενο της προαναφερομένης διάταξης ή άλλης διάταξης που διεκδικεί συμπλήρωση για κάλυψη του πραγματικού πεδίου, δεν υφίσταται κι έτσι δεν μπορεί να γίνει λόγος για διασταλτική ερμηνευτική προσέγγιση.

Κατά την δογματική μου προσέγγιση η λύση δεν δίδεται με ασφάλεια στο περιβάλλον του Κ.Ποιν.Δ., αλλά δίδεται στη βάσει των διατάξεων των άρθρων 2 § 1 και 5 § 1 του Συντάγματος και 6 § 1 και 3 εδ. α΄, γ΄ και δ΄ ΕΣΔΑ. Είναι διατάξεις οι μεν πρώτες συνταγματικής περιωπής η δε δεύτερη είναι διάταξη αυξημένης τυπικής ως κείμενο διεθνούς συνθήκης. Τα υπέρτερα δικαιώματα του κατηγορουμένου στην αξία του ως προσώπου και του δικαιώματός του στην πληροφόρηση αναφορικά με την κατηγορία που του αποδίδεται και το υλικό που την στοιχειοθετεί, επιβάλλουν την διαμόρφωση μιας συνθήκης που επιτρέπει, αν όχι επιβάλλει, την άντληση πληροφόρησης από τα ψηφιακά δεδομένα που βρίσκονται αποθηκευμένα στο μέσο, το οποίο υπάρχει στην δικογραφία.

χ. Η άντληση απόδειξης (εξόρυξη) από τα ψηφιακά δεδομένα που εντοπίζονται στα κατασχεθέντα ψηφιακά πειστήρια.

Η όλη διαδικασία που δρομολογήθηκε μέσα από την έρευνα, η οποία παρουσιάστηκε παραπάνω, δεν έχει καμιά αποδεικτική αξία *αν δεν άγει σε αξιοποιήσιμα αποδεικτικά μεγέθη* στην ποινική δίκη. Πρόκειται για την διαδικασία που αφορά στην άντληση των ψηφιακών δεδομένων, τα οποία θα επιτρέψουν την συναγωγή κρίσεων και θα εκθέσουν σκέψεις και προβληματισμούς αναφορικά με την ορθολογική συνοχή στη δομή της κατηγορίας και τούτο προκειμένης περιπτώσεως με αρνητικό αποτέλεσμα να μην εκθέσουν προσωπικότητες αλλά και το ίδιο τον θεσμό της δικαιοσύνης σε άσκοπες και ονειδιστικές διώξεις και προσαγωγές, σε περίπτωση δε θετικής απόδοσης κατηγορίας, αυτή να είναι δομημένη και κατανοητή από τους θεσμικούς παράγοντες της ποινικής δίκης.

Τον σκοπό αυτόν εξυπηρετεί η εργασία που ακολουθεί την έρευνα στον χώρο και λαμβάνει χώρα στο εργαστήριο (τμήμα ψηφιακών πειστηρίων) των αρμοδίων υπηρεσιών[259].

Όπως και σε άλλες θέσεις της μελέτης έχει αναφερθεί, σημαντικές παράμετροι στον χειρισμό των υλικών φορέων αφ' ενός είναι η διατήρηση της ακεραιότητας των ψηφιακών δεδομένων, ώστε να μην αλλοιώνεται η αποδεικτική εικόνα, κείθεν δε η ουσιαστική διάσταση της αλήθειας και αφ' ετέρου, η εκλαΐκευση των αποτελεσμάτων της έρευνας με την έννοια της κατανοητής παρουσίασης των αποτελεσμάτων της, ώστε να υπάρχει ευχέρεια διαχείρισης από τον δικαστή. Ιδιαίτερη δε αναφορά στις περιπτώσεις που οι αποδείξεις αυτές άγονται ενώπιον σύνθεσης Μικτού Ορκωτού Δικαστηρίου, όπου οι λειτουργικές γνώσεις των ενόρκων, ως θεσμικές απαιτήσεις για δίκαιη κρίση, δεν μπορεί να είναι αυξημένες.

Τα ζητήματα που αφορούν την διαδικαστική προσέγγιση βήμα – βήμα αναφορικά με την διαχείριση των υλικών φορέων των ψηφιακών δεδομένων στον χώρο της έρευνας, όπως και σε άλλα σημεία έχω αναφέρει, την αναπτύσσουμε σε αυτοτελή ενότητα[260]. Για τις ανάγκες της εδώ αναφοράς τονίζεται, ίσως κουραστικά, η επανάληψη της προσοχής και μέριμνας για την ακεραιότητα των ψηφιακών δεδομένων σε όλη την διαδικασία από τον εντοπισμό (ακολούθως την κατάσχεση, την μεταφορά) έως την εξόρυξη δεδομένων, μέχρι την ενσωμάτωσή τους σε ενιαίο υποδοχέα αποθήκευσης ψηφιακών δεδομένων.

Α. Η διαδικασία εξέτασης βοηθά να καταστήσει τα πειστήρια αισθητά και «ορατά», να καταγράψει διαδρομές στην χρήση και να αναδείξει τη σημασία τους στην αποδεικτική υποβοήθηση της υπόθεσης. Αυτή η διαδικασία πρέπει να τεκμηριώσει το περιεχόμενο και την κατάσταση των στοιχείων στο σύνολό τους. Στη φάση αυτή συμπεριλαμβάνεται και η διαδικασία αναζήτησης των πληροφοριών που μπορούν να είναι κρυμμένες (hide) ή χαμένες[261].

Η άντληση των δεδομένων έχει να κάνει και με την κατηγοριοποίησή τους στην βάση της σειράς ευμεταβλητότητάς τους (order of volatility)[262]. Οι χειριστικές μικρές αλλά ταχύτατες μνήμες, με πρώτους και κύριους του καταχωρητές, βρίσκονται στην κορυφή της

[259] Στην Ελλάδα είναι η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα στην Αθήνα, συνεπικουρούμενη με διακριτή τοπική αρμοδιότητα από την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα στην Θεσσαλονίκη.
[260] Βλ. κατωτέρω υπό 10. Πρωτόκολλο έρευνας και διαχείρισης των ψηφιακών πειστηρίων και των ψηφιακών δεδομένων, σελ. 173 επ.
[261] Βλ. *Δ.Π. Αγγελόπουλος**, Ψηφιακά Πειστήρια, Γενικές Αρχές – Χειρισμός, http://www.elesme.gr /elesmegr /periodika/t16/t16_5.htm, * Εξεταστής Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών του Αρχηγείου ΕΛ.ΑΣ.
[262] Βλ. άλλως σειρά πτητικότητας σε *Β. Κάτος*, Ψηφιακά Πειστήρια σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, Νομ. Βιβλ. 2019, 77.

πυραμίδας, ως γραφήματος που αναπαριστά την σχέση μεταξύ των κατηγοριών. Πολύ κοντά στην κορυφή η Μνήμη L3/L2/L1/Cache[263] μέχρι το κατώτερο επίπεδο που αναφέρεται σε αρχεία κι εκτυπώσεις, όπου η ευμεταβλητότητα του δεδομένου είναι περιορισμένη. Σχηματική παράσταση δίδεται αμέσως κατωτέρω για την καλύτερη κατανόηση στις σχέσεις, που προαναφέρθηκαν.

Η ιδιαίτερα απαιτητική σε πόρους και αντιστρόφως ανάλογα αποδοτική ως προς τις προσδοκίες για άντληση δεδομένων πρακτική, ρίχνει το ενδιαφέρον στην μνήμη Ram και στα κατώτερα επίπεδα ευμεταβλητότητας.

Στην βάση αυτής της λογικής παραμέτρου αλλά και της νομικής επιταγής του άρθρου 265 § 4 εδ. β΄ Κ.Ποιν.Δ. ο αναλυτής μεριμνά για την εξαγωγή *πιστού αντιγράφου* κάνοντας πιστή αντιγραφή των δεδομένων. Για να το πετύχει αυτό συλλέγει τα δεδομένα στην βάση μιας σειράς σταθερών βημάτων με τα οποία προσεγγίζει το αντικείμενο της έρευνας. Σε μια πρώτη ενέργειά του λαμβάνει τα *κατάλληλα τεχνικά και οργανωτικά μέτρα* ώστε να αποφύγει τον κίνδυνο αλλοίωσης (εγγραφή, διαγραφή, μεταβολή) των ψηφιακών δεδομένων με χρήση συστήματος Write Blocker (αναστολέας εγγραφής), που είναι τεχνικός εξοπλισμός που επιτρέπει την άντληση (εξόρυξη) των ψηφιακών δεδομένων και την εγγραφή τους σε μέσο αποθήκευσης, αποτρέποντας όμως ταυτόχρονα (βάσει διπλής συνδεσμολογίας).

[263] Αφορά σε προσωρινή μνήμη υλικού που χρησιμοποιείται από την κεντρική μονάδα επεξεργασίας (CPU) ενός υπολογιστή για τη μείωση του μέσου χρόνου ή ενέργειας για την πρόσβαση σε δεδομένα από την κύρια μνήμη. Η προσωρινή μνήμη είναι μια μικρότερη, ταχύτερη μνήμη, που βρίσκεται πιο κοντά σε έναν πυρήνα επεξεργαστή, ο οποίος αποθηκεύει αντίγραφα των δεδομένων από τις τοποθεσίες της κύριας μνήμης που χρησιμοποιούνται συχνά. Οι περισσότεροι επεξεργαστές έχουν διαφορετικές ανεξάρτητες κρυφές μνήμες, συμπεριλαμβανομένων των εντολών και των δεδομένων, όπου η προσωρινή μνήμη δεδομένων είναι συνήθως οργανωμένη ως ιεραρχία περισσότερων επιπέδων προσωρινής μνήμης (L1, L2, L3, L4, κ.λπ.) https://en.wikipedia.org/wiki/CPU_cache,

Β. Κρίσιμο σημείο στην εργασία της εξέτασης των πειστηρίων και της εξαγωγής των ψηφιακών δεδομένων είναι και η διαδικασία της *διαλογής*. Έτσι, ξεκινά μια εργώδης διαδικασία κατά την οποία απαιτείται ενδελεχής έλεγχος των αρχείων που εντοπίστηκαν προκειμένου να καταστεί δυνατή η διάκριση των στοιχείων εκείνων που συνδέονται με την αξιόποινη πράξη για την οποία γίνεται η έρευνα. Διαχωρίζονται λοιπόν οι ψηφιακές πληροφορίες που ενδιαφέρουν εγκληματολογικά από τις λοιπές που μπορεί να είναι και πολλαπλάσιες σε ψηφιακό μέγεθος ή σε απόλυτο αριθμητικό εύρος. Στην εργασία αυτή μπορεί να λάβει βοήθεια ο ερευνητής από λογισμικά που λειτουργούν ως μηχανές αναζήτησης είτε βάσει του τύπου των ενδιαφερόντων αρχείων (λ.χ. για αρχεία εικόνας .avi, .jpg, .mp4, για αρχεία ήχου .mp3, άλλως και αναφορικά με έγγραφα.doc, .pdf).

Η διαλογή εντάσσεται λογικά στην σπονδυλωτή έρευνα ως στοιχείο της ανάλυσης, που διαφέρει από την εξέταση, δεδομένου ότι εξετάζεται το προϊόν προκειμένου να ανακαλυφθούν αποδεικτικά στοιχεία ενοχής ή αθωότητας[264].

Γ. Η *αντιγραφή* περαιτέρω γίνεται σε *όλη την έκταση και στο σύνολο των ψηφιακών δεδομένων,* τα οποία υπάρχουν ακόμη στο κατασχεθέν σύστημα υπολογιστή και γενικά στους υλικούς φορείς που κατασχέθηκαν. Αυτό με την έννοια του ότι αντιγράφονται ακόμη και αρχεία, που δεν βρίσκονται στο περιβάλλον διάδρασης με τον χρήστη διότι, λόγου χάριν, έχουν διαγραφεί, πλην όμως η όποια διαγραφή δεν σημαίνει και οριστική απώλεια του στοιχείου, το οποίο με κατάλληλη τεχνική προσέγγιση μπόρεσε και το ανέκτησε ο ερευνητής[265]. Πρόκειται για την διαδικασία παραγωγής του αρχείου που θα διαλάβει το σύνολο των αντλούμενων δεδομένων από το κατασχεθέν υλικό. Για την αποφυγή κενών ή ελλειμματική καταγραφή τους, η αντιγραφή στο πεδίο αυτό γίνεται σε επίπεδο δυαδικής ακολουθίας (bitstream)[266] και επιτυγχάνεται με την χρήση ειδικού λογισμικού, που επιτρέπει την συγκεκριμένη διεργασία. Το παραγόμενο ψηφιακό αρχείο αποτελεί το αντίγραφο το οποίο συσχετίζεται και εντάσσεται στο σώμα της ποινικής δικογραφίας κατ' άρθρο 265 παρ. 4 εδ. β΄ Κ.Ποιν.Δ.

---

[264] Βλ.

[265] https://www.google.com/search?client=ms-android-xiaomi-rev1&sxsrf=ALeKk03lwXQY8cqyXhtQya70HpUYkspUlg%3 A1589705969107&ei=8fzAXr6DBt-fjLsPvPKVsAs&q=what+is+tlo&oq=what&gs_lcp=ChNtb2JpbGUtZ3dzLXdpei1zZXJwEAEYADIGCCMQJxATMgIIADICCAAyAggAMgIILjICCAAyAgguMgIILjoHCCMQsAIQJzoECAAQDToGCAAQDRAKOgYIABANEB46BwgjEOoCECc6BwguEOoCECc6CQgjEOoCECcQEzoFCC4QgwE6BQgAEIMBUIl7WLGkAWD_rwFoAXAAeAKAAeABiAHHFZIBBjAuMTEuNJgBAKABAbABDw&sclient=mobile-gws-wiz-serp

[266] Βλ. *B. Yadegari, S. Debray*, Bit-Level Taint Analysis, 2014, https://raptor.cs.arizona.edu/~debray /Publications/ bit-level-taint.pdf.

Το αντίγραφο αυτό, και πιο κυριολεκτικά, τα ψηφιακά δεδομένα που έχουν αποθηκευτεί μετά από την διαδικασία της εξόρυξης, πρέπει να βεβαιώνεται ότι είναι, αλλά και πράγματι να είναι, ακριβή αντίγραφα των ψηφιακών δεδομένων που αντλήθηκαν ως πληροφορία από τα ψηφιακά πειστήρια. Τούτο με την σειρά του σημαίνει ότι επιβάλλεται να μπορεί ανά πάσα στιγμή να αποδεικνύεται η *πιστότητα* και η *ακεραιότητά*[267] τους. Η λύση στην προβληματική αυτήν δίδεται μέσω της κρυπτογραφικής συνάρτησης κατακερματισμού (cryptographic hash function)[268]. Οι κρυπτογραφικές λειτουργίες Hash χρησιμοποιούνται για την επίτευξη ενός αριθμού των στόχων ασφαλείας. Η κρυπτογραφική συνάρτηση κατακερματισμού είναι μια συνάρτηση κατατεμαχισμού (hash function), η οποία είναι σχεδιασμένη για να χρησιμοποιείται στην κρυπτογραφία. Γενικά η συνάρτηση κατατεμαχισμού είναι μια μαθηματική συνάρτηση, που έχοντας ως είσοδο μια αυθαίρετου μεγέθους ομάδα δεδομένων, δίνει έξοδο μια καθορισμένου μεγέθους στοιχειοσειρά (string) (η συμβολοσειρά είναι συνήθως μικρότερη σε μέγεθος από την αρχική είσοδο). Η έξοδος δεν μπορεί με αντιστροφή (με κανένα τρόπο) να μας παράγει την αρχική είσοδο. Η έξοδος αποκαλείται συνήθως *σύνοψη* (digest)[269]. Οι συναρτήσεις κατατεμαχισμού βρίσκουν εφαρμογή στις εφαρμογές ασφάλειας πληροφοριών, ενδεικτικά στις ψηφιακές υπογραφές, Message Authentication Codes (MACs) και άλλες μορφές πιστοποίησης αυθεντικότητας των δεδομένων.

Αφού ολοκληρωθεί η ψηφιακή διαχείριση των δεδομένων και η εξασφάλιση του αντιγράφου που θα χρησιμοποιηθεί στην ποινική δικογραφία, η σχετική ερευνητική πορεία δεν τερματίζεται. Μόνη η συγκέντρωση του ψηφιακού υλικού δεν έχει να προσδώσει στην *αποδεικτική αξιολόγησή* του, όπως προαναφέρθηκε, κάτι ουσιώδες. Μια διάταξη και καταγραφή ψηφιακών αναφορών, δεν μπορεί να αποτελέσει βάση τεκμηρίωσης δικανικής κρίσης καθόσον δεν άγει, πέρα πάσης αμφιβολίας, στην απόδειξη της ενοχής. Θα μπορούσε να αξιολογηθεί η μέχρι το σημείο αυτό ενέργεια ως εξασφάλιση (δικανικά) ακατέργαστου ψηφιακού υλικού (raw digital material). Μια *μετάφραση* του ψηφιακού κόσμου στη νομική γλώσσα, θα είναι ενδεχόμενα μια ακατάληπτη πιστή μετάφραση ξενόγλωσσου υλικού, που σαφώς δεν αποτελεί αξιοποιήσιμο αποδεικτικά μέγεθος για τις ανάγκες της ποινικής δίκης.

[267] Βλ. *Β. Κάτος*, Ψηφιακά Πειστήρια σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, Νομ. Βιβλ. 2019, 77.
[268] Βλ. https://el.wikipedia.org/wiki/Κρυπτογραφική_Συνάρτηση_Κατατεμαχισμού
[269] Βλ. *R. Sobti, G.Geetha*, Cryptographic Hash Functions: A Review, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, March 2012, https://www.researchgate.net/profile/Geetha_Ganesan3/publication/267422045_Cryptographic_Hash_Functions_A_Review/links/549cf6d10cf2b8037138c35c/Cryptographic-Hash-Functions-A-Review.pdf

Η απαραίτητη διεργασία που την ψηφιακή πληροφορία την μετατρέπει σε απόδειξη στο ποινικό περιβάλλον είναι η *ανάλυση* των δεδομένων. Μόνη μια καταχώρηση σε αρχείο λ.χ. excel στοιχείων που θα αναφέρονται ως *μεταδεδομένα* χωρίς την απαραίτητη λεκτική επεξήγηση και λογική τοποθέτηση της συγκεκριμένης πληροφορίας στην αποδεικτική τάξη, ουσιαστικά αλλοιώνει όλο το οικοδόμημα της αναζήτησης.

Έτσι η χρονική τοποθέτηση και οι συσχετισμοί ενός ψηφιακού δεδομένου με άλλα αποδεικτικά στοιχεία, μπορούν να δώσουν αποδεικτική πληροφορία, η οποία σαφώς δεν μπορεί να προκύψει με μόνη την αναφορά του δεδομένου χωρίς τις επεξηγηματικές αναφορές σε αυτό. Σημαντική επίσης πληροφορία προκύπτει και από τα μεταδεδομένα ενός ψηφιακού δεδομένου, τα οποία δίνουν στοιχεία για την σχέση του χρήστη με το αρχείο, λ.χ. προσπέλαση ως ενέργεια, πόσες φορές επιχείρησε να το προσπελάσει ή αν το τροποποίησε ή το διέγραψε ή το διέδωσε κλπ. Τονίζεται η απαίτηση για καταγραφή της ζώνης ώρας σε κάθε σχετική χρονοσήμανση, καθόσον σε αντίθετη περίπτωση είναι πολύ πιθανή η συναγωγή εσφαλμένου συμπεράσματος όσον αφορά τον δράστη.

Προσπαθώντας να δώσω μια σχηματική σχέση στις ανωτέρω καταγραφές, σημειώνω ότι ο εντοπισμός ενός αρχείου που θα δίνει μεταδεδομένο τροποποίησής του νωρίτερα από την ημερομηνία δημιουργίας του, σαφώς και δεν μπορεί να ενταχθεί σε μια κανονικότητα χρήσης, παραπέμποντας σε αναζήτηση ενεργειών αλλοίωσης της πραγματικής εικόνας που αποτυπώνουν τα ευρήματα. Εν τέλει ο ψηφιακός κόσμος είναι τεχνολογικά ακριβής αλλά δεν παύει να είναι *εικονικός*.

Στα ίδια πλαίσια σκέψεων εντάσσεται και η περίπτωση της αναζήτησης αρχείων που είτε αποπειράθηκε ο χρήστης (δράστης) να αποκρύψει, είτε να τα διαγράψει. Έργο του αναλυτή είναι να εντοπίσει αρχεία που έχουν αποκρυβεί και ενέργειες διαγραφής. Όπως αναφέρθηκε σε άλλο σημείο, μια ενέργεια διαγραφής από τον χρήστη δεν σημαίνει και εξαφάνιση του δεδομένου από το σύστημα υπολογιστή. Περίπτωση πραγματικής απώλειας αρχείου προκύπτει σε περίπτωση ενέργειας format (διαμόρφωση), με την οποία ενέργεια αυτό που γίνεται είναι να διαμορφώνει τον δίσκο με έναν συγκεκριμένο τρόπο ούτως ώστε να μπορούν να τροποποιηθούν τα δεδομένα του που θα χαρακτηρίζουν τα αρχεία. Υπάρχουν διάφοροι τύποι διαμόρφωσης εκ των οποίων το πιο δημοφιλές είναι το NTFS των Windows. Άλλες είναι το κλασικό FAT32, το ext3 του Linux κτλ. Με το format χάνονται όλα τα αποθηκευμένα αρχεία στον δίσκο, ενώ η επαναφορά των αρχείων είναι σχεδόν αδύνατη[270].

[270] Βλ. https://el.wikiversity.org/wiki/Format_(%CE%B4%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CE%B1%CF%83%CE%AF%CE%B1)

Παρόλα αυτά, η καταγραφή της προσπάθειας για διαγραφή αρχείου μπορεί να φωτίσει αποδεικτικά την ποινική διαδικασία και να στηρίξει, όχι βέβαια από μόνη της, την απόδειξη της κατηγορίας.

Στοιχεία σημαντικά για αποδεικτική αξιοποίηση μπορούν να αντληθούν και από τις πρώιμες επιλογές του χρήστη αναφορικά με την ανωνυμία του ή με την συγκάλυψη των ιχνών της χρήσης του. Έτσι, λ.χ. ο χρήστης μπορεί να έχει εγκαταστήσει λογισμικό το οποίο να ενεργοποιεί σε περίπτωση έρευνας ή με απομακρυσμένη εντολή, διαγραφή των κρίσιμων (ενοχοποιητικών) αρχείων ή διαδρομών λήψης τους.

Σε άλλη εκδοχή προσπάθειας απόκρυψης ενοχοποιητικών στοιχείων, ο χρήστης μπορεί να προσπαθήσει να αλλοιώσει την μορφή του αρχείου, ώστε αυτό κατ' αρχήν να μην εντοπίζεται στην βασική έρευνα. Έτσι λ.χ. ένα αρχείο .avi, μπορεί να το μετονομάσει σε .docx. Με τον τρόπο αυτό βέβαια το αρχείο δεν θα είναι λειτουργικό για τον χρήση που προορίζεται. Η εικόνα όμως που δίνει κατ' αρχήν είναι μη ύποπτη. Βέβαια για τον εξειδικευμένο ερευνητή τέτοιες ενέργειες δεν αποτελούν ανυπέρβλητο εμπόδιο, αλλά δεν παύουν ως ενέργεια να εντάσσονται στο ερευνώμενο εγκληματικό πεδίο και να το χαρακτηρίζουν, τουλάχιστον σε επίπεδο δόλου που μπορεί να καταλογιστεί στον δράστη.

Σε άλλη περίπτωση ο χρήστης μπορεί το ύποπτο αρχείο να το εμφανίζει στην επιφάνεια εργασίας είτε γιατί το έχει πρόχειρο για συχνή χρήση, είτε γιατί θέλει να δείξει άγνοια της παράνομης υπόστασής του (χρησιμοποιώντας την έλλειψη πράξεων απόκρυψης ως υπερασπιστική γραμμή). Αυτή η χρήση των ψηφιακών στοιχείων, πρέπει να αναπτυχθεί από τον αναλυτή διότι έχει ουσιαστικά επεξηγηματικό χαρακτήρα που διευκολύνει την κατανόηση της ψηφιακής πληροφορίας ως σύνολο.

Για μια ακόμη φορά, ας μην λησμονούμε, ότι πολλές υποθέσεις, οι οποίες έχουν να κάνουν με το ηλεκτρονικό έγκλημα, όπως λ.χ. η παιδική πορνογραφία, ανήκουν στην αρμοδιότητα δικαστικού σχηματισμού Μικτού Ορκωτού Δικαστηρίου, όπου η πλειοψηφία των δικαστών είναι οι ένορκοι (4 ένορκοι και 3 τακτικού δικαστές), που είναι πολύ πιθανόν να μην είναι καθόλου εξοικειωμένοι με την τεχνολογία, όπως αναφέρθηκε και παραπάνω, στην θεματική αυτήν, ως εισαγωγική παρατήρηση.

xi. Η παρουσίαση των ψηφιακών δεδομένων.

Όλη η ανωτέρω έρευνα και οι πράξεις εξόρυξης δεδομένων από τα ψηφιακά στοιχεία που υπέστησαν την ερευνητική διαδικασία, πρέπει να λάβουν μορφή *παρουσίασης* που να

δίνει την εικόνα με την οποία πληροφορεί ο ερευνητής – αναλυτής τον δικαστή. Αυτή και μόνο αυτή είναι η αξιοποίηση των δεδομένων που προέκυψαν. Η παρουσίαση αυτή κατ' αρχήν πρέπει να λάβει την μορφή της έγγραφης απόδοσης της πληροφορίας που προέκυψε. Αυτή η πληροφορία επειδή έχει ιδιαίτερες απαιτήσεις ως προς την συλλογή, άντληση και ανάλυση των δεδομένων, δεν μπορεί παρά να είναι μια τεχνοκρατική καταγραφή. Ουσιαστικά ο λόγος γίνεται για την πραγματογνωμοσύνη, την οποία θα συντάξει ο ερευνητής μετά την εξέταση από το τμήμα πειστηρίων.

Την ίδια όμως στιγμή η χρήση της ενώπιον δικαστηρίου και μάλιστα με την μορφή του κατεξοχήν αποδεικτικού στοιχείου, το οποίο στηρίζει την κατηγορία, πρέπει να παρουσιάζεται με τρόπο κατανοητό και με δομή και διάταξη ύλης, που να καθιστά το πόρισμα του ερευνητή ξεκάθαρο.

Δεν πρέπει να λησμονείται το γεγονός ότι σε όλη αυτήν την διαδικασία το υποκείμενο της ποινικής δίκης, που είναι ο κατηγορούμενος, θα πρέπει να μπορεί να *πληροφορηθεί* το πόρισμα της διαδικασίας που ενεργείται σε βάρος. Η έννοια της πληροφόρησης αυτής είναι ουσιαστική και όχι τυπική. Έτσι δεν αρκεί μόνη η προσθήκη της πραγματογνωμοσύνης στο αποδεικτικό υλικό, αλλά πρέπει αυτή να είναι κατανοητή και ουσιαστική ως πληροφορία. Αυτό το τελευταίο έχει να κάνει με την διαδικασία εκλαΐκευσης του πορίσματος των ερευνών. Για να μπορεί κάποιος να κατανοεί ένα αντικείμενο ποινικής δίωξης, θα πρέπει είτε να έχει ειδικές γνώσεις είτε να έχει την δυνατότητα τουλάχιστον κατανόησης της καταγραφής της αποδιδομένης κατηγορίας. Αντιλαμβάνεται κανείς την άκομψη εκείνη περίπτωση κατά την οποία ένα άρτια γραμμένο κείμενο σε γλώσσα πληροφορικής, ακόμη και με επεξηγηματική απεικόνιση του περιβάλλοντος γλώσσας προγραμματισμού επιπέδου java, C++ δεν μπορεί να γίνει κατανοητό από τον δικαστή, ή την περίπτωση κατά την οποία σε μια βάση δεδομένων, που χρησιμοποιείται ως αποδεικτικό εύρημα στον κατασχεθέντα υπολογιστή, τα τεθέντα ερωτήματα να γράφονται σε γλώσσα SQL (queries). Θα πρόκειται για μια άρτια επιστημονικά καταγραφή, που θα είναι αδύνατο να γίνει κατανοητή από τους παράγοντες της δίκης, μεταξύ των οποίων θα εντάξουμε και τους συνηγόρους, που είναι συλλειτουργοί της δικαιοσύνης.

Η *πραγματογνωμοσύνη* δεν είναι ένα αμιγώς επιστημονικό κείμενο, το οποίο απευθύνεται στην σχετική επιστημονική κοινότητα, αλλά ένα πόνημα λογικής και εργώδους διαδικασίας, που λειτουργεί ως δικανικό εργαλείο, που τελικά απευθύνεται (πολλές φορές) σε μη ειδικούς, με αποτέλεσμα να μην επιτρέπεται η εκτεταμένη και σε βάθος καταγραφή

στην ειδική επιστημονική γλώσσα που καθιστά αδύνατη την παρακολούθηση του συλλογισμού του συντάκτη.

Ως επιστημονικό και λογικό έγγραφο πόνημα όμως, η πραγματογνωμοσύνη πρέπει να έχει την δομή εκείνη που με την απλή παρακολούθηση (στο μέτρο των δυνατοτήτων του αναγνώστη, ή της εκλαϊκευσης που επέτρεψε ο συντάκτης) από τον δικαστή, θα είναι κατανοητή η πορεία του συλλογισμού και λογική η κατάληξη που παρουσιάζεται ως πόρισμα στην εργασία του συντάκτη.

Το τόσο ιδιαίτερο και απαιτητικό αντικείμενο των ψηφιακών δεδομένων, δεν αποκλείεται να καταστήσει αναγκαία και την ανάπτυξη και επεξήγηση της πραγματογνωμοσύνης, με εξέταση του συντάκτη της ή μάρτυρα με ειδικές γνώσεις, ενώπιον του ακροατηρίου.

Από τις προσλαμβάνουσες παραστάσεις της νομολογίας, στην πρακτική της εκδίκασης υποθέσεων κατοχής ψηφιακού υλικού πορνογραφίας ανηλίκων, η αντίληψη που αποκομίζουν οι δικαστές είναι κυρίως από την ανάγνωση του πορίσματος και μόνο. Η ανθρώπινη φύση θέλει να νιώθει κανείς ασφαλής στην κρίση της και την ασφάλεια στην περίπτωση αυτήν την έχει ο δικαστής στηριζόμενος μόνο σε εκείνο που κατανοεί.

Έτσι, μια αναφορά σε μεταφορά πακέτων, σε πρωτόκολλα μεταφοράς, σε κατακερματισμό αρχείων και στον τρόπο συναρμογής τους ώστε να είναι αξιοποιήσιμα στο περιβάλλον ενός υπολογιστή, μπορεί να φαντάζουν απλώς εξειδικευμένες γνώσεις και (το ανησυχητικό) να καταντούν αναξιοποίητες πληροφορίες για την δίκη. Και εν τέλει ο δικαστής να περιοριστεί (ουσιαστικά όμως να παρασυρθεί) στο *«ασφαλές δεδομένο»* ότι α) βρέθηκαν κατακερματισμένα αρχεία λ.χ. του αρχείου Chil_XX.mp4 (έστω ως υπόθεση εργασίας ότι αφορά σε αρχείο παιδικής πορνογραφίας), στον σκληρό δίσκο και β) ότι το αρχείο Chil_XX.mp4 είναι αρχείο που εντοπίστηκε μέσα από τον διαμοιρασμό του ολοκληρωμένο σε άλλη τοποθεσία και είναι στην πλήρη του απόδοση αρχείο επιλήψιμο. Και τελικά η σύνθεση των δύο στοιχείων να οδηγήσει στην κατάφαση της τέλεσης της πράξης, που αναφέρεται στην κατηγορία.

Σε αρκετές περιπτώσεις στην δικαστηριακή πρακτική, η στομφώδης θέση που (αδόκιμα) εκφέρεται από τον διευθύνοντα την συζήτηση, πολλές φορές είναι η αποστομωτική θέση με τη μορφή ερώτησης προς τον κατηγορούμενο ή τον συνήγορό του ή τον μάρτυρα υπεράσπισης «*μα τελικά έστω τα κομμάτια αυτά δεν είναι από το παράνομο αρχείο;*». Μια τέτοια θέση μαρτυρά άγνοια της λειτουργίας των κατακερματισμένων

αρχείων, καθόσον το αρχείο αν δεν συγκροτηθεί σε ένα ενιαίο ψηφιακό στοιχείο μέσα από τη «συρραφή» των κατακερματισμένων δομών του, δεν μπορεί να αναγνωστεί και θα παραμείνει μη χρησιμοποιήσιμο ψηφιακό στοιχείο που δεν παράγει τίποτε, πέρα από τα bits που καταλαμβάνει. Μόνος λοιπόν ο εντοπισμός τέτοιων ατελών τμημάτων δεν άγει σε κατάφαση πράξης κατοχής, αφού δεν υπάρχει καμιά φυσική εξουσίαση προσπέλασης. Κατά την άποψή μου δεν υπάρχει ούτε προπαρασκευαστική πράξη ώστε να μιλάμε για απόπειρα, αλλά η θέση αυτή θέλει περαιτέρω εμβάθυνση και δεν είναι επιστημονικά ικανοποιητική η σύντομη τεκμηρίωση που παρατέθηκε προηγουμένως. Και φυσικά δεν επιτρέπει ιδιαίτερες προσδοκίες για μια τελική δίκαιη κρίση.

Εν κατακλείδι η έρευνα πρέπει να αποδώσει, γραπτά κατά κύριο λόγο αλλά και προφορικά, αν ειδικές εξηγήσεις κριθούν απαραίτητες, με απλό και κατανοητό τρόπο, εγκληματολογικού ενδιαφέροντος θέματα ψηφιακών πειστηρίων, ώστε όλα τα εμπλεκόμενα μέρη να είναι σε θέση να κατανοήσουν την αποδεικτική σε επίπεδο ανάκρισης ή δικαστηρίου αξία του κάθε ψηφιακού ευρήματος.

xii. Μια ακόμη παράμετρος.

Ένα ακόμη ζήτημα έχει να κάνει με την *δυνατότητα ή μη* να επιβληθεί κατάσχεση σε ψηφιακά στοιχεία μετά την έναρξη της κυρίας διαδικασίας, σε κάθε στάση της δίκης ακόμη και μετά το πέρας της. Σύμφωνα με το άρθρο 266 Κ.Ποιν.Δ. ορίζεται ότι «*…1. Αν κατά την πορεία της ανάκρισης δεν έγινε δυνατή ή δεν θεωρήθηκε αναγκαία η κατάσχεση πραγμάτων ή εγγράφων σχετικών με το έγκλημα, η κατάσχεση μπορεί να διαταχθεί από το δικαστήριο σε κάθε στάδιο της δίκης και αυτεπαγγέλτως, οπότε ενεργείται από τον εντελλόμενο γι' αυτήν ανακριτικό υπάλληλο μόλις γίνει δυνατή η διενέργειά της. 2. Σε περίπτωση αμετάκλητης καταδίκης, η κατάσχεση, οποτεδήποτε θεωρηθεί ότι μπορεί να γίνει και ανεξάρτητα αν η ποινή εκτίθηκε ή αποσβέστηκε με άλλον τρόπο, διατάσσεται από τον εισαγγελέα και αυτεπαγγέλτως…*».

Η ρητή αναφορά σε *κατάσχεση πραγμάτων ή εγγράφων σχετικών με το έγκλημα*, δίνει επιχείρημα υπέρ μιας αρνητικής απάντησης στο ερώτημα που τέθηκε. Το γεγονός ότι η προσθήκη του άρθρου 265 Κ.Ποιν.Δ. ήρθε για να επιλύσει την αδυναμία κάλυψης της κατάσχεσης των ψηφιακών δεδομένων από τις γενικές διατάξεις περί κατάσχεσης υλικών αντικειμένων, δίνει το στίγμα της διάθεσης του νομοθέτη. Ο τελευταίος, σε μια λεπτομερή και ενδεχόμενα εξαντλητική διάταξη αναφορικά με την κατάσχεση των ψηφιακών

δεδομένων, έδωσε μια μεθοδική προσέγγιση του ιδιαίτερου και σχετικά ευαίσθητου ζητήματος της διαχείρισης της κατάσχεσης στο ψηφιακό περιβάλλον.

Και ήταν όντως εξαντλητική η καταγραφή στην διάταξη φτάνοντας μέχρι του σημείου της σχετικής αναφοράς στην § 6 του άρθρου 265 Κ.Ποιν.Δ. σχετικά με τη δυνατότητα διατήρησης ή αναπαραγωγής των ψηφιακών δεδομένων, που περιλαμβάνονται στο ψηφιακό αρχείο της δικογραφίας, κάτι που με την σειρά του δεν επιτρέπει σκέψεις αναλογικής εφαρμογής διατάξεων, της θεματικής της κατάσχεσης, τουλάχιστον σε ζητήματα που φέρεται να τα λύνει η ειδική διάταξη. Μάλιστα απόδειξη της επιλογής του νομοθέτη για ειδικότατη ρύθμιση αποτελεί και η αναφορά σε ειδική έκθεση της § 3 του άρθρου 265 Κ.Ποιν.Δ., όταν το σύνολο των ζητημάτων της κατάσχεσης καλύπτεται ως αποδεικτική καταγραφή μέσα από τις γενικές διατάξεις για την έκθεση, ως δικονομική διαδικαστική πράξη. Ακόμη και αν εντόπιζε κάποιος σχετικό νομοθετικό κενό αυτό ερμηνευτικά δεν μπορεί να καλυφθεί με αναλογική, με την έννοια της διασταλτικής, ερμηνεία της διάταξης καθόσον είναι βέβαιο ότι μια τέτοια διασταλτική ερμηνεία λειτουργεί σε βάρος του κατηγορουμένου και των δικαιωμάτων του και σύμφωνα με την βασική δικονομική θέση του σεβασμού και της προστασίας του τεκμηρίου της αθωότητας.

Συνεπώς εκτιμώ ότι δεν χωρεί αναλογική εφαρμογή, με την έννοια της διασταλτικής ερμηνείας της πρόβλεψης της διάταξης του άρθρου 266 Κ.Ποιν.Δ.

xiii. Η τύχη των κατασχεθέντων ψηφιακών δεδομένων.

Η όλη διαδικασία αναφορικά με την άντληση των ψηφιακών δεδομένων κινείται στα πλαίσια του σκοπού που διαγράφεται στο άρθρο 239 Κ.Ποιν.Δ. και αφορά στην εξυπηρέτηση των αποδεικτικών αναγκών της ποινικής δίκης, ως συνολικό φαινόμενο σε όλα του τα στάδια, όπως είναι και αυτό της προδικασίας. Η συγκέντρωση του υλικού αυτή καίτοι παρίσταται ευχερής ως προς την αποθήκευσή της (δεν απαιτεί ιδιαίτερο χώρο), ωστόσο βάσει των κρισίμων στοιχείων που διαλαμβάνει ως απόδειξης αξιόποινης συμπεριφοράς, δεν μπορεί να διατηρείται στο διηνεκές.

Ρητά προβλέπεται στην ειδική πρόβλεψη για την κατάσχεση των ψηφιακών δεδομένων (αρ. 265 § 6) ότι 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. Πρόκειται για περιπτώσεις κατά τις

οποίες η πορεία της υπόθεσης είτε ανέδειξε άλλους δράστες και είναι τεχνικά αδύνατη η συνάντηση των δικών, είτε διότι νέα στοιχεία που δεν μπορούν να αξιολογηθούν στην αρχική δικογραφία, δημιουργούν συνθήκες συσχέτισης. Η συγκεκριμένη πρόβλεψη προσομοιάζει στην περίπτωση της εξαγωγής αντιγράφων από μια δικογραφία για τον σχηματισμό άλλης, διαδικασία που είναι γνωστή στην ποινική δικονομία, ήδη από το προηγούμενο δικονομικό καθεστώς.

Με βάση την πρακτική, αναφορικά με την χρονική διάρκεια μιας ποινικής δίκης κακουργηματικού επιπέδου και μέχρι την αμετάκλητη περάτωσή της, το προσδόκιμο σε πλαίσια λογικά και όχι παρελκυστικά, δεν μπορεί να εκτιμάται μικρότερο της δεκαετίας. Με τούτο ως δεδομένο, ως δεύτερο στοιχείο έρχεται το γεγονός ότι στο μέτρο που στα ψηφιακά δεδομένα που αντλήθηκαν από έναν προσωπικό ηλεκτρονικό υπολογιστή ή από ένα προσωπικό αρχείο συστήματος ηλεκτρονικού υπολογιστή σε έναν επαγγελματικό χώρο, είναι το πλέον πιθανό ότι θα διαλαμβάνουν προσωπικά στοιχεία είτε με τη μορφή των προσωπικών δεδομένων είτε με στοιχεία που δημιουργούν προφίλ ταυτοποίησης του χρήστη. Με βάση τις δύο αυτές παραμέτρους, διατηρώ επιφυλάξεις για το νόμιμο και παραδεκτό της διατήρησης των ψηφιακών δεδομένων για άλλο τόσο (τουλάχιστον) χρονικό διάστημα, εφόσον ενσωματωθούν σε άλλη ποινική δικογραφία. Και στην περίπτωση αυτήν η σχετική δικονομική πρόβλεψη, κατά την ρητή αναφορά της διάταξης ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία.

Εκτιμώ ότι μια τέτοια συνθήκη δεν είναι συμβατή με την ΕΣΔΑ και δη το άρθρο 8. Η ένσταση αφορά και το κατά πόσο είναι εφικτή μια πλήρης αφαίρεση του προσωπικού στίγματος του δράστη πριν την ενσωμάτωση των δεδομένων στην άλλη δικογραφία και μάλιστα χωρίς να αλλοιωθεί η ακεραιότητα των δεδομένων αυτών.

Ιδιαίτερη πρόκληση δημιουργεί στη βάση blockchain το κρυπτονόμισμα (bitcoin) και ιδιαίτερα η τύχη του μετά την κατάσχεση. Όπως προβλέπεται για τα ψηφιακά κατασχεμένα αυτά θα αφαιρεθούν από την κατοχή του υπόπτου και φυσικά σε περίπτωση απαλλαγής του θα πρέπει να του αποδοθούν. Αν όμως συσχετιζόμενες με το υπό δίωξη ηλεκτρονικό έγκλημα είναι μονάδες bitcoin, εύλογα τίθεται το ερώτημα με ποιόν τρόπο αυτά θα αποθηκευτούν; Κατά την τηρούμενη στα ελληνικά δεδομένα πρακτική, τα bitcoins θα αντιμετωπιστούν ως τιμαλφή και η παρακατάθεσή τους θα γίνει στο Ταμείο Παρακαταθηκών και Δανείων. Εκτιμώ ότι είναι πρόχειρη αντιμετώπιση και μη αρμόζουσα στην ειδική φύση του κρυπτονομίσματος, που δεν είναι άλλη από αυτή των ψηφιακών δεδομένων.

Η πρακτική στις ΗΠΑ θέλει την ρευστοποίησή τους σε εγχώριο νόμισμα, την δέσμευσή του και την μετέπειτα απόδοσή του, όταν τερματιστεί υπέρ του κατηγορουμένου η δίκη. Αυτή είναι μια εξίσου προβληματική προσέγγιση. Αν λ.χ. κατά το χρόνο της κατάσχεσης η ισοτιμία του bitcoin είναι λ.χ. 1 προς 6.000 $, ενδέχεται κατά την απόδοση μετά από κάποια έτη να είναι 1 προς 1.000 ή 10.000 $. Στην περίπτωση της αύξησης της αξίας, ποιος θα καλύψει την διαφορά, που για το κράτος μπορεί να συνεπάγεται ένα τεράστιο οικονομικό κόστος;

Λογικότερη φαίνεται η προσέγγιση της δημιουργίας e-wallet στις Εθνικές δομές, όπου θα μεταφέρεται στο λογαριασμό το κατασχεθέν και σε περίπτωση απόδοσης θα επιστρέφεται χωρίς να έχει υποστεί καμιά μετατροπή.

9. ΟΙ ΑΡΧΕΣ ΠΟΥ ΔΙΕΠΟΥΝ ΤΗΝ ΕΡΕΥΝΑ ΑΝΑΦΟΡΙΚΑ ΜΕ ΤΑ ΨΗΦΙΑΚΑ ΠΕΙΣΤΗΡΙΑ ΚΑΙ ΤΑ ΨΗΦΙΑΚΑ ΔΕΔΟΜΕΝΑ

Τα ιδιαίτερα χαρακτηριστικά[271] των ψηφιακών στοιχείων, είτε αναφερόμαστε σε δεδομένα, τα οποία εξάγονται από υλικά ψηφιακά πειστήρια, είτε αναφερόμαστε στο σύνολο του υλικού υποδοχέα ή διαμορφωτή, ως ψηφιακά πειστήρια από τη μια καθώς και η νομική δέσμευση για προστασία των δικαιωμάτων του κατηγορουμένου ή υπόπτου, επιβάλλουν όχι μόνο την ιδιαίτερη προσοχή κατά την έρευνα αλλά και τον τεχνικό καθορισμό πρωτοκόλλου, τουλάχιστον σε επίπεδο αρχών που πρέπει να τηρούνται κατά την εξαγωγή των δεδομένων.

Η απαιτούμενη ιδιαίτερη προσοχή αναφορικά με το ενδιαφέρον για τα δικαιώματα του κατηγορουμένου ή του υπόπτου τέλεσης αξιόποινης πράξης, έχει την βάση της στη νομική δέσμευση από σειρά διατάξεων συνταγματικής περιωπής, όπως εκείνη της προστασίας της αξίας[272] του ανθρώπου, της ισότητας[273] απέναντι στο νόμο αλλά και από διατάξεις υπερνομοθετικής ισχύος, όπως η σύμβαση της Ρώμης για τα δικαιώματα του ανθρώπου και ιδιαίτερα το τεκμήριο αθωότητας[274] αλλά και το δικαίωμα σε δίκαιη δίκη[275].

Οι παράμετροι αυτοί επιβάλλουν συνεπώς την ιδιαίτερη προσοχή στην έρευνα καθόσον τα εξαγόμενα στοιχεία και πορίσματα στα οποία αυτά οδηγούν, μπορεί να έχουν άμεσες και ιδιαίτερα δυσμενείς συνέπειες στην προσωπική ελευθερία ή στην οικονομική τάξη του υποκειμένου (κατηγορουμένου) σε μια ποινική δίκη, πάντα δε ελλοχεύει ο κίνδυνος να αγγίξουν κι εκθέσουν προσωπικά δεδομένα αμέτοχων τρίτων προσώπων. Η έρευνα για την εξιχνίαση ενός ηλεκτρονικού εγκλήματος δεν νοείται να λαμβάνει χώρα *με κάθε κόστος*.

---

[271] Βλ. ανωτέρω υπό 7. Τα Ψηφιακά Δεδομένα, *Γ) τεχνικά χαρακτηριστικά και χαρακτηριστικά περιεχομένου των ψηφιακών δεδομένων*, σελ. 81.

[272] Βλ. άρθρο 2 § 1 Συντάγματος «1. Ο σεβασμός και η προστασία της αξίας του ανθρώπου αποτελούν την πρωταρχική υποχρέωση της Πολιτείας.»

[273] Βλ. άρθρο 4 § 1 Συντάγματος «Οι Έλληνες είναι ίσοι ενώπιον του νόμου»

[274] Βλ. άρθρο 6 § 2 ΕΣΔΑ «Παν πρόσωπον κατηγορούμενον επί αδικήματι τεκμαίρεται ότι είναι αθώον μέχρι της νομίμου αποδείξεως της ενοχής του.», αλλά και άρθρο 178 § 3 Κ.Ποιν.Δ. «*… 3. Οποιαδήποτε αμφιβολία περί της ενοχής είναι προς όφελος του κατηγορουμένου ή του υπόπτου*»

[275] Βλ. άρθρο 6 ΕΣΔΑ «Ειδικότερα, πας κατηγορούμενος έχει δικαίωμα: α) όπως πληροφορηθεί, εν τη βραχυτέρα προθεσμία εις γλώσσαν την οποίαν εννοεί και εν λεπτομερεία την φύσιν και τον λόγον της εναντίον του κατηγορίας, β) όπως διαθέτη τον χρόνον και τας αναγκαίας ευκολίας προς προετοιμασίαν της υπερασπίσεώς του. γ) όπως υπερασπίση ο ίδιος εαυτόν ή αναθέση την υπεράσπισίν του εις συνήγορον της εκλογής του, εν ή δε περιπτώσει δεν διαθέτει τα μέσα να πληρώση συνήγορον της εκλογής του, εν ή δε περιπτώσει δεν διαθέτει τα μέσα να πληρώση συνήγορον να του παρασχεθή τοιούτος δωρεάν, όταν τούτο ενδείκνυται υπό του συμφέροντος της δικαιοσύνης, δ) να εξετάση ή ζητήση όπως εξετασθώσιν οι μάρτυρες κατηγορίας και επιτύχη την πρόσκλησιν και εξέτασιν των μαρτύρων υπερασπίσεως υπό τους αυτούς όρους ως των μαρτύρων κατηγορίας, ε) να τύχη δωρεάν παραστάσεως διερμηνέως, εάν δεν εννοεί ή δεν ομιλεί την χρησιμοποιουμένην εις το δικαστήριον γλώσσαν.»

Η ιδιαίτερη αυτή συνθήκη που μερικές φορές λειτουργεί ως συμπληγάδες για τον ερευνητή – μελετητή μιας σειράς ψηφιακών στοιχείων, οδήγησε τις αρχές παγκοσμίως στον καθορισμό πρωτοκόλλων έρευνας, με την έννοια καθορισμού βασικών αρχών αναφορικά με την έρευνα στο χώρο αλλά και με την προσεκτικότερη δυνατή προσέγγιση κατά την εξαγωγή των δεδομένων που θα χρησιμοποιηθούν σε μια ποινική διαδικασία.

Στις προσπάθειες αυτές θα εντάξουμε την σχετική διάταξη - οδηγό ενεργειών του Κεντρικού Τμήματος δίωξης ηλεκτρονικού εγκλήματος της ένωσης Αξιωματικών Αστυνομικών της Μεγάλης Βρετανίας[276], τον σχετικό οδηγό ερευνών για έρευνα στον τόπο διάπραξης ηλεκτρονικού εγκλήματος του Εθνικού Ινστιτούτου Δικαιοσύνης των Η.Π.Α.[277], τον οδηγό διαχείρισης ηλεκτρονικών αποδείξεων του Ευρωπαϊκού Συμβουλίου[278] αλλά και τον οδηγό για τον πρώτο αποκριτή του Γραφείου για την ασφάλεια στο διαδίκτυο και στην πληροφορία της Ευρωπαϊκής Ένωσης[279].

Πέρα από τις καταγραφές των αρχών αυτών σε εγχειρίδια όπως τα προαναφερόμενα, οι αρχές αυτές αποτελούν την σταθερή διαχείριση της επιμόρφωσης σε όλες τις ανεπτυγμένες κοινωνικές και κρατικές δομές[280]. Οι αρχές αυτές διατηρούνται σε πρώτη γραμμή στους ερευνητικούς οργανισμούς, στην εκπαίδευση σε ακαδημαϊκό επίπεδο τόσο τεχνολογικό όσο και νομικό.

Όλα όμως τα ανωτέρω, δηλαδή η τεχνική διάσταση στην άντληση και αξιοποίηση των ψηφιακών δεδομένων από τη μια και η νομική διάσταση στην εμφάνισή τους στην ποινική δίκη από την άλλη, τελούν υπό την σαφώς ισχύουσα παράλληλα ηθική εκείνη δέσμευση, που θέλει ως πρώτο μέλημα στην έρευνα την αλήθεια, πέρα από σκοπιμότητες και σχεδιασμούς. Ο ερευνητής με την ανάληψη της έρευνας στον χώρο, κυρίως ως πρώτος αποκριτής στο ηλεκτρονικό έγκλημα, αναλαμβάνει ουσιαστικά και ηθικά την *υπεράσπιση της αλήθειας*, της συνθήκης εκείνης που αναδεικνύουν τα ψηφιακά δεδομένα με τα οποία θα

[276] Βλ. Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, 2012, https://www .digital-detective.net/digital-forensics-evidence/ ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.

[277] Βλ. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, «Electronic Crime Scene Investigation, A Guide for First Responders, Second Edition», https://www.ncjrs.gov/pdffiles1/nij/ 219941.pdf

[278] Βλ. Council de Europe, Electronic Evidence Guide, A basic guide for police officers, prosecutors and judges https://rm.coe.int/16803028af

[279] Βλ. European Union Agency for Network and Information Security, Electronic evidence - a basic guide for First Responders, Good practice material for CERT first responders https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders

[280] Βλ. πέρα από τις προαναφερόμενες παραπομπές στην ευρώπη και στις Η.Π.Α., Tetsutaro UEHARA - Academic Center for Computing and Media Studies, Kyoto University Cyber Crime and Digital Forensics in Japan https://www.jst.go.jp/sicp/ws2010_austria/presentation/presentation_07.pdf

ασχοληθεί. Η ακεραιότητα και επανελεγξιμότητά τους είναι ο σταθερός και μόνος προσανατολισμός του για την ανάδειξη της αλήθειας.

i. Η διεθνής πρακτική αναφορικά με τον καθορισμό (ή μη) αρχών που διέπουν την έρευνα αναφορικά με τα ψηφιακά δεδομένα – Συγκριτικές αναφορές.

Με αυτήν την εισαγωγή κι έχοντας πάντοτε υπόψη ότι η παραμετροποίηση των δεδομένων που καθοδηγούν τον ερευνητή είναι η ανάδειξη της αλήθειας, μέσα από τεχνικά ορθόδοξες και παραδεδεγμένες επιχειρήσεις και νομικά μέσα από συνεπείς και πάντα νόμιμες δράσεις, παρατηρείται διεθνώς μια προσέγγιση πλαισίωσης των ερευνητικών μεθόδων αναφορικά με τα ψηφιακά δεδομένα, με τρόπο που επιτρέπει και την διαχείριση των ψηφιακών δεδομένων στα πλαίσια των διακρατικών συνεργασιών. Τονίσαμε και σε άλλο σημείο ότι στα θετικά για την έρευνα στοιχεία – χαρακτηριστικά των ψηφιακών δεδομένων και των ψηφιακών πειστηρίων γενικότερα, εντάσσεται η τεχνολογική ομοιότητα στην δομή, υπόσταση και λειτουργία τους στον ψηφιακό κόσμο, ώστε η διαχείριση του αποδεικτικού υλικού να μην απαιτεί τροποποιήσεις ή μετατροπές στο ενδεχόμενο δικαστικής αξιοποίησής του στην περιοχή αρμοδιότητας άλλου δικαιικού συστήματος.

1. Στα πλαίσια αυτών των ενεργειών εντάσσουμε τη διάταξη - οδηγό του Κεντρικού Τμήματος δίωξης ηλεκτρονικού εγκλήματος της ένωσης Αξιωματικών Αστυνομικών της Μεγάλης Βρετανίας[281], ο οποίος στην πρώτη του εκδοχή διαμορφώθηκε το 1998 και με τροποποιήσεις έλαβε την ισχύουσα μορφή του το 2012. Αναφορικά με την επικαιροποίησή του υπάρχουν ενστάσεις[282], οι οποίες αναφέρονται ειδικότερα και σχολιάζονται σχετικά κατωτέρω σε αυτή την ενότητα.

Κατά την σχετική καταγραφή, που αποτελεί οδηγό ενεργειών, στην ανακριτική έρευνα στα ψηφιακά στοιχεία, για τους αστυνομικούς υπαλλήλους στην Μεγάλη Βρετανία, οι υποδεικνυόμενες αρχές έρευνας είναι οι ακόλουθες (σε ελεύθερη απόδοση από το κείμενο στην αγγλική γλώσσα):

[281] Βλ. Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, 2012, https://www .digital-detective.net/digital-forensics-evidence/ACPO_Good_Practice_Guide_ for_Digital_ Evidence_v5.pdf.

[282] Βλ. *Gr. Horsman*, ACPO principles for digital evidence: Time for an update?, February 2020, Forensic Science International: Reports https://www.sciencedirect.com/science/article/pii/S2665910720300220

α. καμιά ενέργεια η οποία πραγματοποιείται από αρμόδιο άτομο που ερευνά την υπόθεση (εν. που αφορά σε ψηφιακά πειστήρια), δεν θα πρέπει να αλλοιώνει τα δεδομένα, τα οποία μπορεί ακολούθως να χρησιμοποιηθούν σε δικαστήριο[283].

Η αρχή αυτή αναφέρεται στην διασφάλιση της *ακεραιότητας* (integrity) των ψηφιακών στοιχείων που έχει να παρουσιάσει η έρευνα. Σαφώς η υπόδειξη δεν αναφέρεται στο αυτονόητο, ήτοι την αποφυγή εσκεμμένης αλλοίωσης των ψηφιακών πειστηρίων, αλλά στην αλλοίωση εκείνη που είναι προϊόν αμελούς συμπεριφορές του ανακριτικού υπαλλήλου ή είναι αποτέλεσμα επέμβασης προσώπου που δεν διαθέτει την κατάλληλη ενημέρωση για το αντικείμενο. Εδώ θα μπορούσαμε να εντάξουμε και τις περιπτώσεις προσπέλασης αρχείων, αφαίρεσης συστημάτων, συσκευασίας, μεταφοράς και φύλαξης των ψηφιακών πειστηρίων. Έτσι μια προσεκτική και τεχνικά άρτια άντληση ενός ψηφιακού δεδομένου από το υποστηρικτικό μηχάνημα, δεν έχει να δώσει πληροφορία στο δικαστήριο, αν στην συνέχεια υπάρξει αλλοίωση του αποθηκευτικού φορέα λ.χ. λόγω έκθεσής του σε κακή φύλαξη κατά την οποία δέχεται επί μακρόν σημαντικά μαγνητικά φορτία.

Η σημασία και η ερευνητική προσοχή για την διατήρηση της ακεραιότητας του κατασχεθέντος ψηφιακού «υλικού» αποδίδει την συνέχεια στην παραδοχή του χαρακτήρα των ψηφιακών δεδομένων ως ευμετάβλητων. Ουσιαστικά είναι μια άλλη απόδοση της παραδοχής ότι αμελείς ενέργειες όπως λ.χ. η εκκίνηση ή μη ασφαλής αντιγραφή κι αφαίρεση αρχείου από σύστημα ηλεκτρονικού υπολογιστή οδηγεί[284] στην αλλοίωση των ψηφιακών δεδομένων[285] αλλά και των σχετικών μεταδεδομένων, από τα οποία επίσης αντλείται σημαντική πληροφορία, που ενδεχόμενα να έχει και σημαίνουσα σημασία για την έκβαση μιας δίκης. Προς συμμόρφωση στην αρχή αυτήν υποδεικνύεται η πρακτική της δημιουργίας αντιγράφου του κατασχεθέντος πειστηρίου[286].

β. στην περίπτωση που καθίσταται αναγκαία η πρόσβαση στα πρωτότυπα (ψηφιακά) δεδομένα θα πρέπει η πρόσβαση αυτή να ενεργείται από ειδικά κατηρτισμένο πρόσωπο για την

---

[283] Βλ. Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, 2012, ο.π., σελ. 7 υπό 2.1.1.

[284] Βλ. *Γ. Μπουρμάς*, Η νομιμότητα των ερευνών σε ηλεκτρονικά δίκτυα και δεδομένα στις περιπτώσεις εγκλημάτων στον κυβερνοχώρο, ΠοινΔικ 2019, 563 επ., *Β. Κάτος*, Ψηφιακά Πειστήρια, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 71 επ.

[285] Βλ. επεξηγηματική ανάπτυξη υπό την ενότητα 2.2.3. σε Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, 2012, ο.π., σελ. 8.

[286] Βλ. επεξηγηματική ανάπτυξη υπό την ενότητα 2.2.4. και 2.2.5. σε Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, 2012, ο.π., σελ. 8 καθώς και ανωτέρω υπό 9. *ix. Το αντίγραφο των κατασχεθέντων ψηφιακών δεδομένων και η φύλαξη των ψηφιακών πειστηρίων*, σελ. 132 επ.

εργασία αυτήν, το οποίο θα είναι σε θέση να δώσει πειστικές εξηγήσεις αναφορικά με την συνάφεια και τις συνέπειες της πρόσβασης αυτής[287].

Η αρχή αυτή αναφέρεται στην συνθήκη κατά την οποία εντοπίζεται ένα σύστημα σε λειτουργία ή ένα σύστημα πρέπει να ενεργοποιηθεί προκειμένου να καταστεί δυνατή η εξαγωγή δεδομένων[288]. Σύμφωνα με την αρχή αυτή, οι εργασίες αυτές πρέπει να γίνουν από πρόσωπο με ειδικές γνώσεις, το οποίο να έχει τη δυνατότητα να ανταποκριθεί σε κάθε σχετική απαίτηση από την εξέλιξη της εργασίας με στόχο να επιτευχθεί η μικρότερη δυνατή τροποποίηση στα δεδομένα, να αποτραπεί η ενεργοποίηση ενός λογισμικού διαγραφής δεδομένων κλπ. Έτσι και στην περίπτωση τερματισμού της λειτουργίας ενός συστήματος το εξειδικευμένο πρόσωπο θα πρέπει να έχει την κατάλληλη γνώση και δεξιότητες προκειμένου να διατηρήσει αναλλοίωτη τη συνθήκη άλλως να επιφέρει τη μικρότερη δυνατή μεταβολή στα δεδομένα του συστήματος.

Σε κάθε δε περίπτωση να είναι σε θέση, ανά πάσα στιγμή και δη ενώπιον δικαστηρίου, να εξηγήσει, τεκμηριώσει και αιτιολογήσει τόσο τις ενέργειές του (ιδιαίτερα τη σκοπιμότητα στην επέμβαση) όσο και τις τεχνικές συνέπειες που επέφερε η επέμβαση αυτή.

γ. ένα αρχείο καταγραφής (audit trail) ή οποιοδήποτε άλλο αρχείο αποτύπωσης των ενεργειών που αφορούν στα ψηφιακά δεδομένα θα πρέπει να δημιουργείται και να διατηρείται. Ένας ανεξάρτητος τρίτος θα πρέπει να είναι σε θέση να εξετάσει την διαδικασία που τηρήθηκε και να καταλήξει στο ίδιο αποτέλεσμα[289].

Είναι σημαντικό να επιδεικνύεται αντικειμενικότητα σε ένα δικαστήριο, καθώς και η συνέχεια και η ακεραιότητα των αποδεικτικών στοιχείων. Είναι επίσης απαραίτητο να αποδειχθεί πώς ανακτήθηκαν τα αποδεικτικά στοιχεία, δείχνοντας κάθε διαδικασία μέσω της οποίας αποκτήθηκαν τα αποδεικτικά στοιχεία. Τα αποδεικτικά στοιχεία πρέπει να διατηρούνται σε τέτοιο βαθμό που ένα τρίτο μέρος μπορεί να επαναλάβει την ίδια διαδικασία και να καταλήξει στο ίδιο αποτέλεσμα με αυτό που παρουσιάστηκε σε δικαστήριο.

Εδώ γίνεται αναφορά σε κριτήρια που πρέπει να πληρούν τα ψηφιακά πειστήρια ώστε να είναι παραδεκτά. Σύμφωνα με το ISO27037:2012[290] πρόκειται για:

---

[287] Βλ. Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, 2012, ο.π., σελ. 7 υπό 2.1.2.
[288] Βλ. *Β. Κάτος*, Ψηφιακά Πειστήρια, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 72.
[289] Βλ. Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, 2012, ο.π., σελ. 7 υπό 2.1.3.
[290] Βλ. https://www.iso.org/standard/44381.html, *D. Sudyana*, *Yudi Prayudi*, *B. Sugiantoro*, Analysis And Evaluation Digital Forensic Investigation Framework Using ISO 27037:2012, International Journal of Cyber-

αα. την *ελεγξιμότητα* (auditability)[291], που αναφέρεται στην δυνατότητα ελέγχου των ενεργειών όλων των σταδίων και όλων των προσώπων που επεχείρησαν,

ββ. την *επαναληψημότητα* (repeatability), η οποία αναφέρεται διαδικασία εκείνη κατά την οποία με ίδια προεργασία στους ίδιους φορείς και αντικείμενα ανάλυσης όταν αναμένονται τα ίδια αποτελέσματα με εκείνα που απέδωσε η έρευνα,

γγ. την *αναπαραγωγικότητα* (reproducibility), που αφορά στην παραγωγή των ίδιων αποτελεσμάτων με εκείνα που παρήχθησαν αρχικά, ανεξάρτητα από την διαδικασία και τα μέσα που θα χρησιμοποιηθούν και

δδ. την *δικαιολογητικότητα* (justifiability), που σχετίζεται με την απόδειξη από τον ερευνητή – αναλυτή δεδομένων, ότι ενήργησε με τον καλύτερο δυνατό τρόπο, δίνοντας στοιχεία για τον τρόπο δράσης του, με σαφή αναφορά στις μεθόδους και τα μέσα που χρησιμοποιήθηκαν κατά την εξέταση και ανάλυση των ψηφιακών πειστηρίων.

δ. το πρόσωπο που είναι επικεφαλής στην έρευνα έχει την πλήρη ευθύνη για την εφαρμογή του νόμου και την τήρηση των προαναφερομένων αρχών[292].

Εδώ η αναφορά γίνεται στο πρόσωπο το οποίο έχει την ευθύνη της τήρησης της νομιμότητας της όλης διαδικασίας από τη στιγμή της έρευνας, της προόδου των διαδικασιών μέχρι και την παρουσίαση και χρήση των ψηφιακών στοιχείων σε μια ποινική δίκη και δη μέχρι το στάδιο της θεσμικής αποδέσμευσής τους, με την άρση ή την επικύρωση της κατάσχεσής τους και την εντολή ενδεχόμενα για διαγραφή ή καταστροφή.

2. Σχετικό οδηγό ερευνών για έρευνα στον τόπο διάπραξης ηλεκτρονικού εγκλήματος έχει εκδώσει και το Εθνικό Ινστιτούτο Δικαιοσύνης των Η.Π.Α.[293] το έτος 2008.

Εδώ φαίνεται να έχει πρωτεύουσα σημασία η διαφύλαξη του συνολικού αντικειμένου της έρευνας αναλλοίωτου. Με τον οδηγό αυτόν δίνονται σταθερά βήματα ενεργειών, με τη μορφή αλγοριθμικής δομής, θα μπορούσε να υποστηρίξει κανείς, καθόσον δίδονται περισσότερο υποδείξεις για συγκεκριμένες ενέργειες και όχι γενικές αρχές, όπως οι

Security and Digital Forensics (IJCSDF) 8(1): 1-14 The Society of Digital Information and Wireless Communications (SDIWC), 2019 ISSN: 2305-001

[291] Βλ. *Β. Κάτος*, Ψηφιακά Πειστήρια, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 73.

[292] Βλ. Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, 2012, ο.π., σελ. 7 υπό 2.1.4.

[293] Βλ. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, «Electronic Crime Scene Investigation, A Guide for First Responders, Second Edition», https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

γενικές προσεγγίσεις που είδαμε παραπάνω στην διαχείριση του αντικειμένου από την Μ. Βρετανία.

Η πρώτη υπόδειξη έχει να κάνει με την ασφάλιση του χώρου γενικά, όπως είναι ο αποκλεισμός με ειδική ταινία απαγόρευσης προσέγγισης σε μη εξοσιοδοτημένα πρόσωπα, η άμεση φωτογράφιση κάθε σχετικού αντικειμένου που κατάσχεται αναφορικά με την θέση αλλά και την εικόνα που αποδίδει όπως λ.χ. στις περιπτώσεις ενεργούς οθόνης που είναι συνδεμένη σε ηλεκτρονικό υπολογιστή. Στα ίδια πλαίσια περιπτωσιολογικής αναφοράς, δίδεται ενδεικτικός κατάλογος των αντικειμένων στα οποία μπορεί να αναζητηθούν ψηφιακά δεδομένα και με τον τρόπο αυτόν. Η περιπτωσιολογική αυτή καθοδήγηση συνεχίζεται και στα βήματα ενεργειών στον χώρο της έρευνας ανά κατηγορία αντικειμένου (λ.χ. σταθερή μονάδα ηλεκτρονικού υπολογιστή, φορητών ηλεκτρονικών υπολογιστών, κινητών τηλεφώνων, εξωτερικών μονάδων αποθήκευσης ψηφιακών δεδομένων κλπ). Ιδιαίτερη έμφαση δίδεται στην απεικόνιση της συνδεσμολογίας και στην λεπτομερή αναφορά στην δικτύωση καθώς και στο ενδεχόμενο διασύνδεσης με απομακρυσμένο υπολογιστή σε περιβάλλον νεφοϋπολογιστικής.

Η περιπτωσιολογική αυτή αναφορά φαίνεται να δημιουργεί μια ασφυκτική συνθήκη για τον ερευνητή, ενώ την ίδια στιγμή με τα σταθερά βήματα που υποδεικνύει με λεπτομερή αναφορά στις πιθανές συνθήκες που θα αντιμετωπίσει στον χώρο ο ερευνητής (λ.χ. αν η οθόνη είναι ενεργή αλλά κενή και συνδέεται με ενεργό υπολογιστή, αν η οθόνη είναι ενεργή αλλά κενή και συνδέεται με μη ενεργό υπολογιστή, αν η οθόνη είναι ενεργή και έχει προστασία οθόνης και συνδέεται με ενεργό υπολογιστή, αν η οθόνη είναι ενεργή και έχει φωτογραφίες αλλά όχι από την λειτουργία προστασίας οθόνης και συνδέεται με ενεργό υπολογιστή κ.ο.κ.) δημιουργείται η εντύπωση ότι οποιοσδήποτε και όχι απαραίτητα εξειδικευμένο προσωπικό, μπορεί να ολοκληρώσει την διαδικασία κατάσχεσης και ασφαλούς μεταφοράς και αποθήκευσης των ψηφιακών στοιχείων, τα οποία έχουν δεσμευθεί μέσα από την διαδικασία που ενεργήθηκε.

3. στην Ελλάδα δεν υπάρχει σχετικός οδηγός, τουλάχιστον με την δομή των καταγραφών, που παρατηρήσαμε ανωτέρω, προφανώς η συμμόρφωση στις διεθνείς συνεργασίες[294], αλλά και οι οδηγοί στους οποίους αναφερθήκαμε αμέσως παραπάνω, συνθέτουν το σχετικό πλαίσιο στο οποίο κινούνται οι έρευνες στο ηλεκτρονικό έγκλημα και

[294] Βλ. *An. Papathanasiou, Al. Papanikolaou, V. Vlachos, K. Chaikalis, M. Dimou, M. Karadimou and V. Katsoula*, Legal and Social Aspects of Cyber Crime in Greece, ResearchGate 2015, https://www.researchgate.net/publication/260390705.

στη χώρα μας. Αν περαιτέρω γίνεται κάποια συγκεκριμενοποίηση των ερευνητικών διαδικασιών, αυτή γίνεται κυρίως στην βάση των νομικών πλαισίων που διαμορφώνονται από το Ν 2224/1995[295], το ΠΔ 47/2005[296], Ν 3471/2006[297], Ν 4411/2016[298], αλλά και από το ΠΔ 100/2004[299]. Σαφώς και τηρείται πρωτόκολλο ενεργειών και εργασιών κατά την κατάσχεση των ψηφιακών στοιχείων (πειστηρίων και δεδομένων που εξάγονται από αυτό), αλλά δεν προκύπτει κάποια τήρηση δεσμευτικής μεθοδολογίας αναφορικά με την εργασία στον χώρο της έρευνας, πέρα φυσικά από τα όσο επιτάσσει η λογική του αντικειμένου και οι τεχνικώς παραδεδεγμένες, αποδεκτές από τον επιστημονικό κόσμο, πρακτικές.

4. Να σημειωθεί ότι ανάλογες, με διαφοροποιήσεις σε ορισμένα επουσιώδη σημεία, είναι και οι σχετικές διαμορφώσεις εντολών ανταπόκρισης στις περιπτώσεις εντοπισμού διάπραξης ηλεκτρονικού εγκλήματος, προς τους αρμοδίους (αστυνομικούς) υπαλλήλους με βάσει αναλογικές εφαρμογές των προαναφερομένων οδηγών, σε οικείους οδηγούς έρευνας στην INTERPOL[300], στην Αστυνομία της Σκωτίας[301], στην Αστυνομική Ακαδημία[302], στην υπηρεσία Ασφάλειας Πληροφοριών και Διαδικτύου της Ευρωπαϊκής Ένωσης[303].

ii. Οι Αρχές που διέπουν την ανακριτική έρευνα ως ερευνητική προσέγγιση της μελέτης.

Αν κάποιος επιχειρούσε να συμπυκνώσει σε μια πρόταση την ουσία όλων των αρχών, που διεκδικούν εφαρμογή στο πεδίο της ανακριτικής έρευνας που οδηγεί στον εντοπισμό και

[295] Βλ. Ν 2225/1994, (ΦΕΚ Α 121/20.07.1994) «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας»
[296] Βλ. ΠΔ 47/2005 ΦΕΚ Α 64/10.03.2005.
[297] Βλ. Ν 3471/2006, (ΦΕΚ Α 133/28.06.2006) «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν.2472/1997.»
[298] Βλ. Ν 4411/2016, (ΦΕΚ α 142/03.08.2016) «Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών - Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις.»
[299] Βλ. ΠΔ 100/2003, ΦΕΚ 94/Α/22.04.2003.
[300] Βλ. INTERPOL, Global Guidelines for Digital Forensics Laboratories, at: https://www.interpol.int/content/ download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf (Accessed: November 2019).
[301] Βλ. Police Scotland, Digitally Stored Evidence Standard Operating Procedure, at: https://www.scotland. police.uk/assets/pdf/151934/184779/digitally-storedevidence-sop, 2019.
[302] Βλ. The College of Policing, Passive Data Generator, at: https://www.app. college.police.uk/app-content/investigations/investigative-strategies/passive-datagenerators/#computer-based-electronic-evidence, 2019.
[303] Βλ. European Union Agency for Network and Information Security, Electronic Evidence a Basic Guide for First Responders, at: https://www.enisa.europa.eu/ publications/electronic-evidence-a-basic-guide-for-first-responders/at_download/ fullReport (2019)

την ανάκτηση ψηφιακών δεδομένων, οι οποίες αρχές θα αναπτυχθούν στην συνέχεια, θα μπορούσε να την διατυπώσει ως ακολούθως. *Ας διατηρηθούν τα ψηφιακά στοιχεία στην πρωτότυπη μορφή τους και αν πρέπει να γίνει κάποια επέμβαση σε αυτήν, τότε ας διασφαλιστεί ότι επιχειρείται από γνώστη του αντικειμένου, ο οποίος θα καταγράφει όλη την ερευνητική διαδικασία, που ανά πάσα στιγμή μπορεί να επαναληφθεί παράγοντας τα ίδια αποτελέσματα. Αυτός που επιχειρεί στον πυρήνα της έρευνας θα είναι και ο επικεφαλής, που διασφαλίζει παράλληλα και την τήρηση του νόμου*.[304] Στην διατύπωση αυτήν θα μπορούσαμε να συμπυκνώσουμε και συμπεριλάβουμε αρχές όπως η ακεραιότητα, η ελεγξιμότητα και η αναπαραγωγικότητα, που δεν είναι και οι μόνες στις οποίες γίνεται αναφορά κατωτέρω.

Πρέπει να σημειωθεί ότι η εφαρμογή των αρχών δεν αποκλείει μια αναλογική προσέγγιση στην εξέταση ψηφιακών στοιχείων. Όσοι λαμβάνουν αποφάσεις σχετικά με τη διεξαγωγή μιας ψηφιακής έρευνας πρέπει συχνά να λαμβάνουν αποφάσεις σχετικά με το επίκεντρο και το εύρος μιας έρευνας, έχοντας υπόψη τους διαθέσιμους πόρους πληροφοριών και την έρευνα. Αυτό θα περιλαμβάνει συχνά μια εκτίμηση επικινδυνότητας που βασίζεται σε τεχνικούς και μη τεχνικούς παράγοντες, για παράδειγμα τα πιθανά αποδεικτικά στοιχεία που μπορεί να διατηρούνται από έναν συγκεκριμένο τύπο συσκευής ή το προηγούμενο προσβλητικό ιστορικό του υπόπτου. Ενδεχόμενα δε η σχετική διαπίστωση θα απαιτεί περαιτέρω πρωτοβουλίες του ερευνητή για την αντιμετώπιση του ζητήματος που διαπιστώθηκε. Όπου αυτό γίνεται, θα πρέπει να είναι ευκρινής η επιλογή, οι αποφάσεις, οι οποίες λαμβάνονται θα πρέπει να αιτιολογούνται και να καταγράφεται το σκεπτικό του τελικού πορίσματος.

Α) Η αρχή της ***νομιμότητας***.

Η πρώτη αρχή εδράζεται σε δύο βάσεις, άλλως παρουσιάζεται σε μια πιο προσλαμβάνουσα παράσταση, με δύο πτυχές.

Η πρώτη, η οποία φαντάζει και αυτονόητη, είναι ότι όλη η έρευνα πρέπει να κινηθεί μέσα σε ένα πλαίσιο *νομιμότητας*. Καμιά ενέργεια, ακόμη και αν κρίνεται τεχνικά απαραίτητη, αλλά είναι νομικά εκτεθειμένη, λ.χ. μια άμεση επέκταση της έρευνας σε χώρο ή σε αντικείμενο που δεν καλύπτει η εντολή έρευνας στην οποία αναφέρομαι στην συνέχεια, δεν μπορεί να γίνει ανεκτή. Η τήρηση του νόμου και των πλαισίων που θέτει ερμηνευτικά

[304] Βλ. *Β. Κάτος*, Ψηφιακά Πειστήρια, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, σελ. 65.

αναφορικά με την διαχείριση του αποδεικτικού υλικού, πρέπει να αποτελεί το πρώτο μέλημα σε οποιαδήποτε έρευνα που ενεργείται από όργανο που ασκεί κρατική εξουσία.

Η δεύτερη πτυχή, ίσως και με την διάσταση της στενότερης έννοιας της νομιμότητας, είναι η *νομιμοποιητική* βάση της έρευνας. Καμιά έρευνα δεν μπορεί να γίνεται αποδεκτή σε ένα συντεταγμένο δικαιικό σύστημα εφόσον κείται εκτός νόμιμης εντολής που εκδόθηκε από αρμόδια Αρχή. Είναι σαφές ότι μια ανομιμοποίητη έρευνα θα καταπέσει στο μέλλον, προφανώς μέσα από σχετικές ενστάσεις ακυρότητας, ενδεχόμενα και απόλυτης (αρ. 171 Κ.Ποιν.Δ.) τοιαύτης. Στα πλαίσια παραδοχής μιας τέτοιας ένστασης θα έχουμε μια δικονομική ανατροπή και όλο το συλλεγέν αποδεικτικό υλικό, το μεν δεν θα μπορεί να χρησιμοποιηθεί για τον σκοπό για τον οποίον προορίζεται, το δε μπορεί να εγείρει κατά του ενεργήσαντος ανακριτικού υπαλλήλου και της αρχής στην οποία λειτουργεί, ευθύνες ποινικές αλλά και αστικής αποζημίωσης, ιδίως λόγω προσβολής προσωπικών δεδομένων. Ας μην λησμονούμε ότι η αρχή της νόμιμης βάσης ορίζεται ρητά στο άρθρα 5 § 1 περ. α΄ και 6 GDPR και έχει σαφώς ευθεία εφαρμογή στην περίπτωσή μας καθόσον η επεξεργασία προσωπικών δεδομένων και δη ειδικής κατηγορίας (ευαίσθητων), λαμβάνει χώρα και την ερευνώμενη κρατική δράση.

Για την συμμόρφωση στην αρχή της νομιμότητας στην έρευνα θα πρέπει να υπάρχει από την έναρξη, ήτοι πριν την επέμβαση του πρώτου ανταποκριτή, η σχετική εντολή από την Αρχή ποινικής δίωξης (δεν γίνεται λόγος για άσκηση ποινικής δίωξης ακόμη) μετά από μήνυση ή έγκληση (αναλογικά εφαρμοζόμενης της διάταξης του άρθρου 243 § 1 Κ.Ποιν.Δ.) ή εφόσον πρόκειται για κακουργηματική πράξη η εντολή του Ανακριτή αφού λάβει σχετική παραγγελία από τον Εισαγγελέα κι εφόσον δεν συντρέχει λόγος αποχής του (αρ. 246 έως και 248 § 1 Κ.Ποιν.Δ.). Οι αστυνομικοί προανακριτικοί υπάλληλοι εφόσον διαπιστώσουν την τέλεση κακουργηματικής πράξης οφείλουν να ενημερώσουν αμελλητί τον αρμόδιο Εισαγγελικό λειτουργό ο οποίος καλείται να αξιολογήσει την πληροφορία και να ενεργήσει άμεσα με τη σειρά του.

*Β) η αρχή της **ακεραιότητας (integrity)** του ψηφιακού στοιχείου στο οποίο επεβλήθη η κατάσχεση.*

Με αυτήν την εισαγωγή κι έχοντας πάντοτε υπόψη ότι η παραμετροποίηση των δεδομένων που καθοδηγούν τον ερευνητή είναι η ανάδειξη της αλήθειας, μέσα από τεχνικά

ορθόδοξες και παραδεδεγμένες επιχειρήσεις και νομικά μέσα από συνεπείς και πάντα νόμιμες δράσεις, την προσεγγίζουμε ως κύρια αρχή, η οποία είναι η *ακεραιότητα* (integrity).

Η ακεραιότητα αναφέρεται στην διατήρηση του πρωτότυπου συλλεγέντος υλικού ψηφιακών δεδομένων, *αναλλοίωτου*. Σε επίπεδο ψηφιακής έρευνας αυτό περιλαμβάνει τόσο την ψηφιακή στιγμή της κατάληψης όσο και την υλική διάσταση, ως τέτοιας νοουμένης της διατήρησης του φορέα υποδοχής των ψηφιακών δεδομένων αναλλοίωτου. Η αρχή αυτή πρέπει να είναι ο *πυρήνας των παραμέτρων της έρευνας* και σταθερά το κύριο μέλημα του ανακριτικού υπαλλήλου, που επιχειρεί. Καταλαμβάνει κατά βάση την διατήρηση αναλλοίωτου του ψηφιακού δεδομένου που κατασχέθηκε ή κτήθηκε από κατασχεμένο ψηφιακό φορέα και γενικότερα την διαχείριση του ψηφιακού στοιχείου από την αρχική κατάληψη μέχρι και το αμετάκλητο πέρας της ποινικής διαδικασίας τουλάχιστον. Και τούτο διότι και μετά από το αμετάκλητο της διαδικασίας δεν αποκλείεται νέα στοιχεία να απαιτούν την εκ νέου αξιολόγηση του ψηφιακού δεδομένου, δίνοντας πάντα στον κατηγορούμενο (ή στον νέο κατηγορούμενο) την δυνατότητα της επανεξέτασής του.

Ενδιαφέρουν λοιπόν τόσο οι συνθήκες δέσμευσης, εξόρυξης, ασφάλισης, μεταφοράς όσο και φύλαξης του ψηφιακού υλικού αυτού. Σύμφωνα με τις παραδεδεγμένες πρακτικές για την διατήρηση της ακεραιότητας του ψηφιακού υλικού που κατασχέθηκε, πρέπει να αποφεύγεται κάθε μορφή αλλοίωσής του. Προς αυτήν την κατεύθυνση της ικανοποίησης της αρχής αυτής λειτουργούν πρακτικές όπως

αα. η επέμβαση να γίνεται αποκλειστικά και μόνο από άτομο που διαθέτει τις *ειδικές γνώσεις* και μάλιστα σε τέτοιο επίπεδο που σαφώς ξεπερνούν τις αντιλήψεις του μέσου χρήστη ηλεκτρονικών εφαρμογών. Τα σοβαρά ζητήματα που διακυβεύονται από την περαιτέρω δικαστική αξιοποίηση του ψηφιακού υλικού δεν επιτρέπουν, ούτε πειραματισμούς, ούτε απροσεξίες.

ββ. για την οποιαδήποτε εργασία απαιτείται για την ασφαλή αφαίρεση και μεταφορά του ψηφιακού πειστηρίου, θα πρέπει να τηρούνται οι *παραδεδεγμένες τεχνολογικές μέθοδοι* και όχι αόριστα να εξουσιοδοτείται ο ενεργών ερευνητής. Μόνη η κτήση ειδικών γνώσεων, δεν εξασφαλίζει το μέγιστο στην διασφάλιση της ακεραιότητας του κατασχεθέντος υλικού, που είναι και το ζητούμενο.

γγ. η οποιαδήποτε εργασία για την άντληση και ασφάλιση των ψηφιακών δεδομένων από τον κατασχεμένο υλικό φορέα θα πρέπει να επιχειρείται με *κατάλληλα τεχνικά μέσα, ειδικό λογισμικό και εργαλεία*. Ενδεικτικά η αναφορά γίνεται σε λογισμικά όπως SHA-1 και

SHA-256, MD5 – Linux, Red Line (διαθέτει γραφικό περιβάλλον με αυτόματη ανάλυση), Time Line (για χρονική ανάλυση), Autorun, USB device forensics, kookoo (για κακόβουλα αρχεία) κλπ. Πολλά από αυτά είναι ανοικτού κώδικα. Στον απαιτούμενο τεχνικό εξοπλισμό αναφέρονται ενδεικτικά κάμερες (για λήψη φωτογραφίας και βίντεο), χαρτοκιβώτια, ειδικά έντυπα σημειώσεων αυτοκόλλητα (με τρόπο ασφαλή και όχι επιπόλαιο, που θα μπορούσε να οδηγήσει σε σύγχυση αναφορικά με την ταυτότητα του αντικειμένου το οποίο σημαίνει), ελαστικά γάντια μιας χρήσης, αρχεία καταγραφής αποδεικτικών στοιχείων, ταινία αποδεικτικών στοιχείων, ανεξίτηλη γραφίδα, ταινία αποκλεισμού πρόσβασης στον ερευνώμενο χώρο (ως χώρο τέλεσης εγκλήματος) έντονης κι ευδιάκριτης απόχρωσης ή συνδυασμού αποχρώσεων, αντιστατική σακούλα, μη μαγνητικά εργαλεία (κατσαβίδια κοινά, κατσαβίδια ακριβείας ωρολογοποιών, κινητών, H/Y, Am-Tech L0475, πένσα, τσιμπίδα, καρυδάκια).

δδ. σημαντική θέση στην διατήρηση της ακεραιότητας έχει η δημιουργία *ασφαλούς αντιγράφου*[305] του ψηφιακού πειστηρίου ώστε να διασφαλίζεται η δυνατότητα ανάκτησης των δεδομένων που έχουν κατασχεθεί, σε περίπτωση απώλειας ή καταστροφής. Το αντίγραφο αυτό παράγεται κατά την κατάσχεσή τους και διατηρείται στον προβλεπόμενο χώρο φύλαξης των πειστηρίων.

εε. Απαγόρευση μη εξουσιοδοτημένης πρόσβασης στον χώρο της ανακριτικής έρευνας, στα κατασχεθέντα ψηφιακά στοιχεία και στην πληροφορία που εξάγεται από αυτά, που είναι επίσης μια κρίσιμη παράμετρος κατά την προσπάθεια εξασφάλισης της ακεραιότητας του αποδεικτικού υλικού.

Γ) η αρχή της ***έγγραφης απόδειξης, τεκμηρίωσης και χρονοσήμανσης*** *των ανακριτικών εργασιών.*

Ουσιαστικά πρόκειται για την χαρτογράφηση των ανακριτικών - ερευνητικών ενεργειών στον χώρο διάπραξης του ηλεκτρονικού εγκλήματος. Πρόκειται για το *αρχείο καταγραφής* (audit trail) που συναντήσαμε ανωτέρω[306]. Ως καταγραφή στην πρόταση αυτήν διαλαμβάνουμε όχι μόνο τις επεξηγηματικές πληροφορίες και αναγραφές σε μια τεχνική

[305] Για την ειδικότερη πρόβλεψη στον Κ.Ποιν.Δ. βλ. ανωτέρω υπό 8. Η Κατάσχεση των Ψηφιακών Δεδομένων (Κατ' άρθρο 265 Κ.Ποιν.Δ. *ix. Το αντίγραφο των κατασχεθέντων ψηφιακών δεδομένων και η φύλαξη των ψηφιακών πειστηρίων*, σελ. 132 επ.

[306] Βλ. ανωτέρω στην παρούσα ενότητα υπό *i. Η διεθνής πρακτική αναφορικά με τον καθορισμό (ή μη) αρχών που διέπουν την έρευνα αναφορικά με τα ψηφιακά δεδομένα* (σελ. 138) και αφορά στην σχετική αρχή της Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, 2012, ο.π., σελ. 7 υπό 2.1.3.

έκθεση, αλλά και ό,τι έχει συλλεγεί και αποδεικνύει τις ενέργειες του ερευνητή στο χώρο της έρευνας. Συμπεριλαμβάνονται λοιπόν φωτογραφίες που ελήφθησαν σε διάφορα στάδια της έρευνας στον χώρο, οι οποίες αποδεικνύουν την διάταξη των ψηφιακών στοιχείων στον χώρο καθώς και την συνθήκη (ενεργά ή μη) που βρέθηκαν κατά την επέμβαση.

Όπου απαιτείται ενεργοποίηση του σχετικού ψηφιακού πειστηρίου ή απενεργοποίηση ενώ είναι ενεργό, τα δύο στάδια, ήτοι η κατάσταση πριν όσο και μετά την επέμβαση θα πρέπει να αποδεικνύονται με έγγραφη αναφορά και με τεχνική απεικόνιση. Στο σημείο αυτό θα πρέπει να γίνεται σαφής αναφορά και της τεκμηρίωσης όλων των ενεργειών του ερευνητή με σαφή παραπομπή σε εντελώς εξειδικευμένα σημεία στις επιστημονικά αποδεκτές και πρακτικά παραδεδεγμένες μεθόδους που επέλεξε. Αν παρεμπιπτόντως, και αντίθετα προς τα αναφερόμενα στην αρχή για την ακεραιότητα, όπως αυτή αναπτύσσεται ανωτέρω, ο ερευνητής για την επίλυση μιας ιδιάζουσας συνθήκης επιλέξει μια προσέγγιση που δεν ανταποκρίνεται στα συνήθη μοτίβα, θα πρέπει να είναι σε θέση για τεκμηριώσει τεχνικά την προσέγγιση, αναλαμβάνοντας φυσικά την επί πλέον[307] ευθύνη για το ενδεχόμενο πρόκλησης βλάβης στα δεδομένα που προέκυψαν στην συνέχεια.

Με την καταγραφή αυτήν είναι δυνατή η συμμόρφωση στην υποχρέωση για την *ελεγξιμότητα* (auditability), *επαναληψημότητα* (repeatability), *αναπαραγωγικότητα* (reproducibility) και *δικαιολογητικότητα* (justifiability) κατά τις υπαγορεύσεις του προτύπου ISO27037:2012[308]. Στο περιεχόμενο των τεχνικών αυτών όρων έγινε σχετική αναφορά ανωτέρω[309], όπου και παραπέμπω προς αποφυγή άσκοπης επανάληψης.

Δ) η αρχή της ***ευθύνης του επικεφαλής.***

Απαραίτητη προϋπόθεση για την διατήρηση μιας ασφαλούς συνθήκης αναφορικά με τα ζητήματα που ενδέχεται να ανακύψουν από αξιοποίηση των στοιχείων που θα προκύψουν από την έρευνα, είναι η ύπαρξη του προσώπου στο οποίο θα γίνεται αναφορά σε κάθε ζήτημα που θα ανακύπτει. Είναι ξεκάθαρο ότι η ανακριτική έρευνα θα αγγίξει δικαιώματα,

[307] Εννοείται πέραν εκείνης που έχει ο επικεφαλής της επιχείρησης.
[308] Βλ. https://www.iso.org/standard/44381.html και σχετική αναφορά σε *Β. Κάτος*, Ψηφιακά Πειστήρια, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 72, *Ak. Ajijola, P. Zavarsky, R. Ruhl*, A Review and Comparative Evaluation of Forensics, Guidelines of NIS T SP 800-101 Rev. 1:2014 and ISO/IEC 27037:2012.
[309] Βλ. ανωτέρω στην παρούσα ενότητας υπό *i. Η διεθνής πρακτική αναφορικά με τον καθορισμό (ή μη) αρχών που διέπουν την έρευνα αναφορικά με τα ψηφιακά δεδομένα* (σελ. 153) και αφορά στην σχετική αρχή της Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, 2012, ο.π., σελ. 7 υπό 2.1.3, *Β. Κάτος*, Ψηφιακά Πειστήρια, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019, 73.

ατομικές ελευθερίες κι έννομα αγαθά, όπως η ιδιωτικότητα (privacy) προσώπων υποκειμένων ψηφιακών δεδομένων ή/και ιδιοκτητών ψηφιακών πειστηρίων που ερευνώνται, που μπορεί μάλιστα τελικά να είναι και πρόσωπα αμέτοχα στην ερευνώμενη αξιόποινη συμπεριφορά του ηλεκτρονικού περιβάλλοντος.

Το πρόσωπο αυτό θα πρέπει να είναι επιφορτισμένο με την γνώση του ιστορικού της έρευνας από την στιγμή της εντολής επέμβασης μέχρι και την στιγμή της εξαγωγής του πορίσματος το οποίο αποτελεί το αποδεικτικό υλικό στο οποίο στηρίζεται η δίωξη για το συγκεκριμένο ηλεκτρονικό ή ηλεκτρονικά διαπραχθέν έγκλημα. Μονοδιάστατος στόχος του προσώπου αυτού θα είναι η προστασία της ακεραιότητας της έρευνας ως σύνολο, ήτοι νομικό περιβάλλον δράσης (νομιμοποιητική βάση), υλικές ενέργειες και αποτέλεσμα δράσης, σε συνθήκες όμως διαφάνειας. Θα πρέπει να είναι σε θέση να τεκμηριώσει κάθε σημείο της έρευνας, να διαχειριστεί αιτήματα για λήψη στοιχείων που είναι στην διάθεσή του αλλά και να προστατεύει την όλη διαδικασία από παράγοντες που μπορούν να την βάλλουν και να την καταστήσουν μη δεκτική δικαστικής αξιοποίησης.

Φυσικά ο ανακριτικός αυτός υπάλληλος θα πρέπει να συγκεντρώνει στο πρόσωπό του στοιχεία γνώσης του αντικειμένου του ψηφιακού περιβάλλοντος, των παρεδεδεγμένων τεχνικών μεθόδων έρευνας, εξαγωγής δεδομένων, ανάλυσης, αποθήκευσης και φύλαξης των ψηφιακών στοιχείων, ώστε να είναι σε θέση να δώσει απαντήσεις, ει δυνατόν σε πρώτο χρόνο, στα ερωτήματα που θα θέσει ο κατηγορούμενος ή ο ύποπτος τέλεσης της πράξης για την οποία η δίωξη, ο ίδιος, ο πληρεξούσιος δικηγόρος του και ενδεχόμενα ο ορισθείς τεχνικός του σύμβουλος. Είναι λοιπόν ξεκάθαρο ότι η ανάληψη της σχετικής αρμοδιότητας προϋποθέτει συγκέντρωση γνώσεων νομικής, πληροφορικής, ηλεκτρονικών επικοινωνιών. Σαφώς την σχετική επιμέλεια της ανακριτικής πράξης την διατηρεί ο Ανακριτής ως θεσμικώς ορισμένο όργανο.

Ε) η αρχή της ***αναγκαιότητας και της αναλογικότητας***.

Ο ερευνητής πρέπει να αντιλαμβάνεται ορθά τη νομική φύση και τον σκοπό της ψηφιακής έρευνας. Πρέπει να είναι ξεκάθαρος σχετικά με τις αποδεικτικές ανάγκες και τις προτεραιότητες, που τίθενται κατά την εξέταση καθώς στην διαδικασία και την διαδοχή των ενεργειών, είναι πιθανόν να ανακύψουν βασικές πληροφορίες, οι οποίες επιβάλουν να διατηρηθούν στοιχεία που μπορεί να παραπέμπουν αλλού. Αυτό ισχύει ιδιαίτερα στην περίπτωση που σχετίζεται με την ύπαρξη πρόσθετων αποδεικτικών στοιχείων που

παραπέμπουν σε άλλες παραβάσεις σχετιζόμενες, σε πρόσωπα πέραν του αρχικού υπόπτου αλλά και νεοεμφανιζόμενων θυμάτων.

Πολλές φορές δημιουργείται μια αίσθηση υπερβολής όταν υπάρξει εντοπισμός σωρευμένων πηγών πληροφορίας. Στο αντίκρισμα πολλών ηλεκτρονικών υπολογιστών ή μιας ομάδας από οθόνες στον ίδιο χώρο, δημιουργείται μια αίσθηση σύλληψης μιας μεγάλης επιχείρησης συμπεριφοράς σε ψηφιακό περιβάλλον. Δεν αποκλείεται όμως να υπάρχουν στοιχεία εντελώς άσχετα με την υπό δίωξη πράξη και το σημαντικότερο, τα στοιχεία αυτά, ως ψηφιακά δεδομένα να αφορούν αποκλειστικά προσωπικά δεδομένα, χωρίς καμιά παραπέρα παροχή πληροφορίας, ίσως δε μερικά από αυτά να είναι και ευαίσθητα προσωπικά δεδομένα (λ.χ. ένα αρχείο pdf μια ιατρικής γνωμάτευσης, ή ένα πιστοποιητικό οικογενειακής κατάστασης).

Εδώ ανακύπτουν ζητήματα σχετικά με τις αρχές του *αναγκαίου μέτρου* στην κρατική δράση, το κατά πόσο δηλαδή η επέμβαση για την εξιχνίαση της ερευνώμενης πράξης αναγκαία διέρχεται από την εξέταση του συγκεκριμένου πειστηρίου, κατά πόσο το εύρημα δικαιολογεί την κατάσχεσή του και περαιτέρω, κατά πόσο είναι η επιβολή της κατάσχεσης ανάλογη της πληροφόρησης, με την οποία μπορεί αποδεικτικά να ενισχυθεί ο σκοπός της έρευνας.

Ό,τι είναι εκτός σκοπού και ό,τι κρίνεται υπερβολικό, δεν μπορεί να καλύπτεται από την αρχή της νομιμοποιητικής βάσης που βασίζει όλη την έρευνα. Πριν την δέσμευση ενός αντικειμένου, με την δικονομική πράξη της κατάσχεσης, θα πρέπει να γίνεται μια πρώτη αξιολόγηση αναφορικά με το εάν το αντικείμενο είναι πιθανό να περιέχει ενδιαφέροντα για την υπόθεση αποδεικτικά στοιχεία. Έτσι για παράδειγμα θα πρέπει να γίνει μια αξιολόγηση αν το laptop ανήκει στο περιβάλλον του υπόπτου ή σε τρίτον, πριν κατασχεθεί, ακόμη και αν εντοπίστηκε στο χώρο της έρευνας. Δεν είναι ασύνηθες δύο φοιτητές να έχουν στον ίδιο χώρο τα laptops τους χωρίς όμως ο ένας να γνωρίζει την έκνομη δράση του άλλου που επιχειρείται μέσα από το ίδιο router, στο ίδιο διαμέρισμα. Ακόμη και στην περίπτωση που στην οικία του δράστη εντοπιστεί ένα laptop φίλου του, που μπορεί να βρέθηκε εκεί για πολλούς και διαφόρους λόγους (μη αξιόποινους).

Αν πάλι η έρευνα αφορά σε στοιχεία συγκεκριμένης ημεροχρονολογίας, τότε η έρευνα θα πρέπει να περιοριστεί είτε σε κινήσεις και αρχεία με ημερομηνία δημιουργίας μεταγενέστερη, είτε, στην περίπτωση που η έρευνα επεκτείνεται (ελέγχεται η νομιμότητα ή

μη μιας τέτοιας πράξης) θα πρέπει να έχει όρια το χρονικό σημείο της παραγραφής κακουργήματος ή πλημμελήματος ανάλογα με το εύρημα.

Αλλά και αντικείμενα που φέρονται να ανήκουν στον ίδιο τον ύποπτο μπορεί τα ίδια να είναι άσχετα. Δεν υπάρχει λογική για κατάσχεση σε ό,τι ανήκει στον ύποπτο ή σε ό,τι βρεθεί κατά την έρευνα. Αν λοιπόν η μονάδα του ηλεκτρονικού υπολογιστή είναι συνδεμένη με μια τηλεόραση, την οποία χρησιμοποίησε για οθόνη, είναι σαφές ότι πέρα από την απεικόνιση και σήμανση στον χώρο, η τηλεόραση δεν μπορεί να δώσει δεδομένα και συνεπώς δεν θα πρέπει να την καταλάβει η πράξη της κατάσχεσης. Κατά όμοιο τρόπο εμφανώς πεπαλαιωμένες ηλεκτρονικές συσκευές όπως παλιά κινητά και δη χωρίς ενέργεια (που ενδέχεται να μην βρίσκονται σε τρέχουσα χρήση), καθώς ενδέχεται να είναι δυνατά διαφορετικά επίπεδα εξέτασης για αυτά.

Σχετικά και απλώς ενδεικτικά αναφέρεται στο σημείο αυτό η επέμβαση κι έρευνα σε δικηγορικό γραφείο στην Τουρκία, όπου κατασχέθηκε το σύνολο των ηλεκτρονικών φακέλων πελατών και άλλων συλλειτουργούντων δικηγόρων[310].

Να σημειωθεί στο σημείο αυτό ότι ήδη η αρχή της αναλογικότητας πέρα από την ύπαρξή της στον καταστατικό χάρτη της Ελλάδας, ως γενική δικαιική αρχή (βλ. αρ. 25 § 1 Συντ), αποτελεί πλέον θετό δίκαιο σε όλο το πεδίο της ανακριτικής έρευνας, σύμφωνα με την διάταξη του άρθρου 251 § 2 Κ.Ποιν.Δ., όπως αυτή τροποποιήθηκε και ισχύει με το Ν 4637/2019[311]. Όπως εύστοχα παρατηρείται, η τροποποίηση αυτή, που ουσιαστικά καθιστά σαφή την εφαρμογή της αρχής της αναλογικότητας με ρητή αναφορά σε τυπικό νόμο, στόχο δεν έχει μόνο την άμβλυνση των ενστάσεων αναφορικά με την τριτενέργεια της διάταξης του αρ. 25 § 1 Συντ. Η σημασία της είναι ουσιαστική και είναι η σαφής υπόδειξη στον εφαρμοστή του δικαίου να συνειδητοποιήσει την εφαρμογή της αρχής ως όριο των επεμβάσεών του στα ατομικά δικαιώματα και την ελευθερία των υποκειμένων σε έρευνα προσώπων[312].

[310] Βλ. ΕΔΔΑ Kırdök κ.α. κατά Τουρκίας της 03.12.2019 (αριθ. 14704/12), https://hudoc.echr.coe.int/eng#{%22itemid %22:[%22001-198805%22]}

[311] Βλ. αρ. 8 § 12 Ν 4637/2019, ΦΕΚ Α 189/18.11.2019. Βέβαια ο λόγος για τον οποίος η διάταξη του αρ. 251 Κ.Ποιν.Δ. δεν είχε διαλάβει την σχετική διάταξη την 01.07.2019, όταν και πλέον έλαβε χώρα η ριζική αλλαγή και κωδικοποίηση του Κ.Ποι.Δ. και του Π.Κ. αφήνει εύλογες απορίες, με δεδομένο το γεγονός ότι η αντικατάσταση των κωδίκων και οι εργασίες των νομοπαρασκευαστικών επιτροπών σαφώς και λειτουργούσαν (ίσως όχι με την ίδια δομή και προσανατολισμούς) επί σειρά ετών.

[312] Βλ. *Θ. Δαλακούρας*, Νέος Κώδικας Ποινικής Δικονομίας, Συστηματική ερμηνεία κατ' άρθρο του Ν 4620/2019, Νομική Βιβλιοθήκη, 2019, σελ. 199.

*ΣΤ) η αρχή της **απόδειξης της νόμιμης δράσης** της υπεύθυνης Αρχής.*

Είναι σαφές ότι εδώ δεν γίνεται λόγος για την αρχή της νομιμότητας που μας απασχόλησε ανωτέρω αλλά για την απόδειξη της νόμιμης δράσης της αρχής που επελήφθη. Αντί άλλης ανάπτυξης στο σημείο αυτό παρουσιάζω την θέση με ένα παράδειγμα.

Έστω ότι στο διαμέρισμα Α στην Θεσσαλονίκη, το οποίο είναι μισθωμένο σε πρόσωπο που φέρεται με την μίσθωση να εξυπηρέτησε τρίτους αλλά δεν είχε φυσική εξουσίαση του χώρου, επιχειρεί ανακριτικός υπάλληλος ως επικεφαλής ομάδας μετά από σχετική εντολή αρμοδίου ανακριτή. Επιχειρεί η σχετική ομάδα της δίωξης ηλεκτρονικού εγκλήματος την είσοδο στον χώρο και βάσει πρωτοκόλλου ερευνητικών ενεργειών προχωράει στην φωτογράφηση του χώρου και καταγράφει τα ευρήματα κατά είδος, θέση στον χώρο και λειτουργική συνθήκη στην οποία εντοπίζονται και (συνοπτικά αναφερόμενα) προχωράει στην επιβολή της κατάσχεσης των ψηφιακών πειστηρίων, στην καταγραφή των δικτύων, στην δημιουργία πρόχειρου σκαριφήματος, με ενδεδειγμένο δε τρόπο αποθηκεύει όλα τα κατασχεθέντα πειστήρια, μέσα στο οποία φυσικά υπάρχουν και στοιχεία που είναι στο πεδίο της κατάσχεσης όχι όμως κατ' ανάγκη ψηφιακά τοιαύτα. Η διαδικασία φωτογραφήθηκε ή και βιντεοσκοπήθηκε και μετά την ολοκλήρωση της εργασιών στον χώρο ενεργείται η άντληση των ψηφιακών δεδομένων και μετά από σχετική συνδυαστική εργασία η ποινική δίωξη, που ασκήθηκε in rem, συγκεκριμενοποιείται και στρέφεται κατά συγκεκριμένου προσώπου. Έστω βάσει ίχνους DNA (λ.χ. μια τρίχα), που του αποδίδεται μετά από σχετική ταυτοποίηση και το οποίο φέρεται ότι βρέθηκε στον χώρο[313], κρίνεται ότι συντρέχουν στο πρόσωπό του ενδείξεις ενοχής και έτσι κατηγορείται για την πράξη.

Ο πληρεξούσιος δικηγόρος του όσο και ο τεχνικός σύμβουλος που θα ορίσει ο κατηγορούμενος, προσφεύγοντας ενώπιον του υπευθύνου της έρευνας θα μπορούν να έχουν εικόνα και να λάβουν εξηγήσεις αναφορικά με την έρευνα με σημεία αναφοράς που εκκινούν από την είσοδο των ανακριτικών υπαλλήλων στον χώρο και μετά. Είναι όμως αυτά τα στοιχεία αρκετά;

Όπως αναφέρθηκε στην υπόθεση εργασίας, η σύνδεση του κατηγορουμένου με την εγκληματική δράση στηρίζεται στον εντοπισμό DNA που ταυτοποιήθηκε με τον κατηγορούμενο. *Ποιος όμως πιστοποιεί ότι τα υλικά αυτά βρέθηκαν στον τρόπο της έρευνας;*

[313] Για την ανάδειξη της προβληματικής και μόνο και χωρίς περαιτέρω δυνατότητες για περιπτωσιολογικές αναφορές σε ενδεχόμενες καταστάσεις, έστω ότι το κινητό αυτό δεν φέρεται να έχει επικοινωνία από τον συγκεκριμένο χώρο αλλά απλά βρέθηκε εκεί.

Πώς μπορεί να βεβαιωθεί ότι δεν μεταφέρθηκε («φυτεύθηκε» κατά την χρησιμοποιούμενη ορολογία στην αστυνομία) από άλλη έρευνα το σχετικό (ενοχοποιητικό) υλικό;

Επιχειρήματα του τύπου ποιο το συμφέρον της δίωξης να παρανομήσει και πώς μπορεί να αποδίδεται σε αστυνομικό – ανακριτικό υπάλληλο μια τέτοια κατηγορία δυστυχώς καταρρίπτονται από την ίδια την πρακτική και τη σειρά από περιπτώσεις κατάχρησης εξουσίας που απασχόλησαν τη νομολογία. Για τα δε παραγωγικά αίτια της βούλησης που θα οδηγούσε σε μια τέτοια συμπεριφορά, ας μην ανοίξει ο λόγος εδώ διότι πολλά έχουν να ειπωθούν. Όπως προαναφέρθηκε, απλή αναφορά στις σειρές υποθέσεων δήθεν εξιχνίασης εγκληματικών οργανώσεων, που μέσα από μια πολυτελή κι εκκωφαντική ενημέρωση του κοινού κατά τις σωρηδόν προσαγωγές, υπό το φως των καμερών και με τις μεγαλόσχημες αποδόσεις συγχαρητηρίων στους διευθυντές σχηματισμών και προϊσταμένους τμημάτων της ΕΛΑΣ, καταλήγουν, μετά από χρόνο και μακριά από τις κάμερες πλέον, στο σύνηθες «φιάσκο» της απαλλαγής των κατηγορουμένων στις δικαστικές αίθουσες. Σαφώς μια εξιχνίαση ενός ηλεκτρονικού εγκλήματος δεν έχει να δώσει πολλά αν δεν καταλήξει σε κατηγορούμενο και «εντυπωσιακά» ευρήματα. Αν όμως αποδοθεί τελικά κατηγορία για σοβαρής έκτασης αξιόποινη συμπεριφορά, τότε «κάποιος», συνήθως υψηλόβαθμος αξιωματούχος, έχει οφέλη, συνήθως υπηρεσιακής αποτύπωσης, ηθικής υπόστασης, αλλά και μισθολογικής αύξησης.

Θα μπορούσε επίσης να υποστηρίξει κανείς ότι η παρουσία δικαστικού λειτουργού κατά την επιχείρηση στο διαμέρισμα, όπου η είσοδος θα γίνει βάσει εντάλματος που θα εκδώσει ο αρμόδιος Ανακριτής, εξασφαλίζει την τήρηση της νομιμότητας. Μόνη λοιπόν η συνταγματική απαίτηση για παρουσία δικαστικού λειτουργού επιβεβαιώνει τον ενδοιασμό του υπερασπιστή. Αν η αστυνομία δεν υπήρχε καμιά περίπτωση να παρανομήσει, τότε δεν θα είχε κανέναν δικαιοπολιτικό λόγο η συνταγματική επιταγή για παρουσία δικαστικού λειτουργού κατά την κατ' οίκον έρευνα (αρ. 9 § 1 Συντ).

Αυτά λοιπόν δεν είναι σπέκουλα, φαντασίες, σενάρια και κιτρινισμοί[314]. Και το ερώτημα δεν θα έπρεπε να είναι στην βάση του αν έχουν εμφανιστεί ή όχι τέτοια φαινόμενα,

[314] Τηρώντας την δεοντολογία που επιβάλλει η επιστημονική προσέγγιση και η επαγγελματική μου υποχρέωση για εχεμύθεια, αναφέρομαι σε πραγματικό περιστατικό, το οποίο χειρίστηκα ως πληρεξούσιος δικηγόρος του κατηγορουμένου, ήδη από το στάδιο των ερευνών και αναζητήσεων. Μετά από έρευνες και αναζητήσεις εξαφανισθείσας τον Απρίλιο του 2005, κοπέλας 21 ετών, την Πε 11.08.2005 συνελήφθη από το αρμόδιο τμήμα της Αστυνομικής Διεύθυνσης Θεσσαλονίκης, που επεχείρησε μαζί με το Τμήμα Ασφαλείας Βεροίας, άτομο φερόμενο ως υπαίτιο για τέλεση πράξης ανθρωποκτονίας σε βάρος του προαναφερομένου θύματος. Πρόκειται για υπόθεση γνωστή στο πανελλήνιο μέσα από την ειδησιογραφία αλλά και από την εκπομπή «Φως στο τούνελ», που ασχολήθηκε από την πρώτη ημέρα με το περιστατικό ως εξαφάνιση του (μετέπειτα) θύματος. Την Πα 12.08.2005 ο κατηγορούμενος προσήχθη στην αρμόδια Εισαγγελία Πλημμελειοδικών Βέροιας (ως κατά

αλλά τα πώς θα μπορούσε να τα αποκλείσει κανείς ακόμη και αν ο λόγος γινόταν στην βάση της θεωρητικής και μόνο αναζήτησης.

Προς ενίσχυση των ανωτέρω πρέπει να αναφέρω ότι όσο το ίδιο το κράτος έχει αμφιβολίες για την καθαρότητα στις δομές κι υπηρεσίες πρόληψης και καταστολής του εγκλήματος, όσο διατηρεί ενδοϋπηρεσιακά τμήματα εσωτερικών υποθέσεων για την πάταξη της διαφθοράς και της κατάχρησης εξουσίας από ανακριτικούς υπαλλήλους, πιστός στον όρκο μου κατά την ανάληψη του λειτουργήματός μου, ως υπερασπιστής κατηγορουμένου είμαι υποχρεωμένος να εξαντλώ κάθε δυνατότητα για την προάσπιση των δικαιωμάτων του ανθρώπου που μου εμπιστεύθηκε τις τύχες του. Πάνω από όλα αυτά όμως οφείλω να ζητώ και να μάχομαι για την τήρηση του νόμου προς πάσα κατεύθυνση. Δεν υπάρχει τίποτε χειρότερο από το να παρανομεί ο θεματοφύλακας της δικαιοσύνης.

Επειδή όμως στόχος της παρούσας στάσης στην μελέτη είναι η ανάδειξη της αιτίας που επιβάλλει την εισηγούμενη πρόταση, δεν θα προχωρήσω σε περαιτέρω καταγραφές περιστατικών κατάχρησης εξουσίας, ή ακυροτήτων κατά την ανακριτική έρευνα, για τις οποίες υπάρχει υλικό (δεν έχει ιδιαίτερη σημασία αν είναι «πλούσιο») στη νομολογία.

Προτείνω λοιπόν ως πρόσθετο στοιχείο, που θα συμπεριλαμβάνεται στο αρχείο καταγραφής (audit trail), να υπάρχει καταγραφή εικόνας και ήχου από την χρονική στιγμή

τόπο αρμόδιας) με σειρά επεισοδίων έξω από το κτήριο της Εισαγγελίας Πλημμελειοδικών Βέροιας, συνθήκη που παρακολούθησε το πανελλήνιο μέσα από την ζωντανή τηλεοπτική κάλυψη της προσαγωγής από την Α.Δ. Θεσσαλονίκης. Η δικογραφία παραδόθηκε στην Εισαγγελία Πλημμελειοδικών Βεροίας την Πα 12.08.2005 αλλά λόγω της έντασης δεν ελήφθη απολογία του κατηγορουμένου αλλά δόθηκε, μετά από σχετικό «αίτημα» του κατηγορουμένου, 48ωρη προθεσμία. Ο κατηγορούμενος έλαβε για πρώτη φορά αντίγραφο της δικογραφίας, λόγω του όγκου της και λόγω της συγκέντρωσης πλήθους κάτω από τα γραφεία της Εισαγγελίας Πλημμελειοδικών και του γραφείου της Ανακρίτριας Βέροιας, το Σα 13.08.2005, μετά από συνεννόηση εμού, ως πληρεξουσίου συνηγόρου του, με το γραφείο της Ανακρίτριας Βέροιας. Όμως το βράδυ της Πα 12.08.2005, δηλαδή **μια (1) ημέρα ΠΡΙΝ**, απεικονίσεις από μαρτυρικές καταθέσεις και την προανακριτική απολογία του κατηγορουμένου επεδείχθησαν στην έκτακτη εκπομπή «Φως στο τούνελ». Σημειώνεται ότι λόγω και της αργίας της Δε 15.08.2005, παράσταση πολιτικής αγωγής δηλώθηκε μόλις την Τρ 16.08.2005. Είναι λοιπόν σαφές ότι την δικογραφία την είχε στην διάθεσή της μέχρι και το πρωί της 13.08.2005 ΜΟΝΟ η Α.Δ. Θεσσαλονίκης και η Εισαγγελία Πλημμελειοδικών Βέροιας, ενώ σαφώς η πλευρά του κατηγορουμένου ΔΕΝ είχε κανένα λόγο δημοσιοποίησης της προανακριτικής του κατάθεσης, που ομολογουμένως είχε ληφθεί χωρίς παρουσία συνηγόρου και κατά περιεχόμενο δεν τον εξυπηρετούσε, τουναντίον μάλλον προκαλούσε οργή εναντίον του. Επαναλαμβάνω ότι η πολιτική αγωγή έλαβε τη δικογραφία την 16.08.2005, ήτοι πέντε (5) ημέρες ΜΕΤΑ την δημοσιοποίηση. Τα συμπεράσματα είναι προφανή κι επιβεβαιώνουν τις σχετικές ενστάσεις αναφορικά με τη νομική αρτιότητα των αστυνομικών συμπεριφορών. Το τι είχε να κερδίσει η Α.Δ. Θεσσαλονίκης ή ο προϊστάμενός της, σαφώς και το γνωρίζει ο ίδιος καλύτερα. Το γεγονός όμως είναι ότι τα ανωτέρω έγιναν όλα όπως τα καταγράφω, όσο «απίθανα» κι αν φαντάζουν. Η υπόθεση κρίθηκε και από το Ε.Σ.Ρ., ενώ κατά την εκδίκαση της υπόθεσης μετά από ένα έτος (Νοέμβριο 2006) από το Μ.Ο.Δ. Θεσσαλονίκης (αρ. υπόθεσης 138-144/2006, αδημοσίευτη) βρισκόταν στο ακροατήριο (χωρίς κανέναν προφανή λόγο παρουσίας εκεί) ο επικεφαλής της ερευνητικής ομάδας της Α.Δ. Θεσσαλονίκης, ο οποίος όταν αναδείχθηκε υπερασπιστικά το σχετικό χρονικό επεφύλαξε φραστική επίθεση στον πληρεξούσιο δικηγόρο του κατηγορουμένου, την οποία απέτρεψε ζωηρά κατά την συνεδρίαση η Πρόεδρος της σύνθεσης του Μ.Ο.Δ., ενώ στην απόπειρα επανάληψής της επίθεσης από τον ίδιο εναντίον μου κατά την διακοπή, τον σταμάτησαν οι αστυνομικές δυνάμεις που ήταν επιφορτισμένες με την ασφάλεια του χώρου.

ΠΡΙΝ την είσοδο του ανακριτικού υπαλλήλου στον χώρο. Να βιντεοσκοπείται η στιγμή της πρώτης κλήσης για είσοδο στον χώρο, άλλως από την στιγμή πριν την βίαιη είσοδο (όπου αυτό επιβάλλεται), να δίδεται γενικό πλάνο από τον χώρο και να ακολουθείται κατά πόδας στην έρευνά του ο επικεφαλής. Αυτό τουλάχιστον μέχρι το σημείο που γίνονται οι αναγκαίες και νομικά ανεκτές επεμβάσεις οι οποίες πλέον καλύπτονται με φωτογράφηση στα πλαίσια συμμόρφωσης με τις λοιπές αρχές.

Η προτεινόμενη βιντεοληψία αποτρέπει και αποκλείει κάθε σχετική σκέψη ή υπόνοια κατάχρησης, παρέχει δε την σχετική ασφάλεια στον κατηγορούμενο ότι αποκλείεται το ενδεχόμενο είτε μεταφοράς στον χώρο της έρευνας είτε αφαίρεσης από αυτόν, μετά την είσοδο του ανακριτικού υπαλλήλου, υλικού, το οποίο μπορεί στη συνέχεια να χρησιμοποιηθεί αποδεικτικά για στήριξη της κατηγορίας σε βάρος συγκεκριμένου προσώπου. Και όλα αυτά διότι τόσο το αρχείο καταγραφής (audit trail) όσο και η ειδική έκθεση του άρθρου 265 § 3 Κ.Ποιν.Δ., που θα μας απασχολήσει στην συνέχεια, δεν φαίνεται να διαλαμβάνουν και να εξασφαλίζουν την εικόνα του χώρου ΠΡΙΝ την επέμβαση του ανακριτικού υπαλλήλου που είναι επικεφαλής της έρευνας.

Δεν θα μπορούσε να μείνει ασχολίαστη η συνταγματική πρόβλεψη για παρουσία του δικαστικού λειτουργού ως θεματοφύλακα της νομιμότητας κατά την κατ' οίκο έρευνα, σύμφωνα με το αρ. 9 § 1 Συντ. Η πρακτική καταδεικνύει ότι τον ρόλο του εκπροσώπου της δικαστικής αρχής στις περιπτώσεις αυτές επιτελεί συνήθως Ειρηνοδίκης, ο οποίος υπηρετεί στην περιφέρεια όπου λαμβάνει χώρα η έρευνα. Συνήθως οι γνώσεις του είναι ιδιαίτερα περιορισμένες στο ζήτημα των ενεργειών επί των συσκευών ψηφιακού περιβάλλοντος, με αποτέλεσμα η παρουσία του να μην παρέχει ουσιαστικές εγγυήσεις για την διασφάλιση της νομιμότητας. Εξ άλλου γενικότερα το ζήτημα της εξοικείωσης των δικαστών[315], όλων μάλιστα των βαθμίδων, με τις τεχνολογίες πληροφορικής κι επικοινωνιών (εννοείται πέραν εκείνων του απλού χρήστη) είναι ζήτημα προς μελέτη και φυσικά εκφεύγει των αναζητήσεων που γίνονται εδώ.

Πώς είναι λογικά δυνατόν να εποπτεύεις ένα αντικείμενο το οποίο δεν γνωρίζεις; Φυσικά η συνταγματική πρόβλεψη προϋπήρχε των ουσιαστικών ζητημάτων που έχει η εγείρει η εμφάνιση της τεχνολογίας και του ηλεκτρονικού εγκλήματος. Διατηρεί όμως την σημασία της η διάταξη στην βάση του ότι κατά την θέσπισή της θεωρήθηκε ότι κάποιος

[315] Βλ. *Ν. Δαγκλής*, Η αποδεικτική και διαγνωστική ελευθερία του ποινικού δικαστή σε ζητήματα που απαιτούν ειδικές γνώσεις: Εγγύηση ή ανάχωμα στην διερεύνηση του ηλεκτρονικού εγκλήματος σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, Νομική Βιλβλιοθήκη 2019, σελ. 188 επ.

έπρεπε να «συγκρατεί» τις αρχές πάταξης του εγκλήματος από την υπερβολή, έστω με την διακριτική παρουσία του. Αν ο συντακτικός νομοθέτης είχε τις αμφιβολίες του, εγώ τουλάχιστον δεν νομιμοποιούμαι να μην τις έχω.

iii. Μερικές επιπλέον επισημάνσεις.

Υποστηρίζεται ότι το δυνατό σημείο αυτών των αρχών είναι η γενική εφαρμογή τους καθόσον φαίνεται να μπορούν να καλύψουν όλο το φάσμα των ψηφιακών δεδομένων και πειστηρίων. Απλότητα και ευρύτητα στην εφαρμογή τους είναι τα στοιχεία που επιτρέπουν την χρησιμοποίησή τους και πέρα από τα σύνορα της κρατικής οντότητας που τα παρήγαγε.

Η ανάπτυξη όμως της τεχνολογίας και μάλιστα με αλματώδεις ρυθμούς, αλλά και η ευρηματικότητα των δραστών δημιουργεί ανησυχίες και ερωτήματα αναφορικά με την επιμονή στη διατήρηση των συγκεκριμένων προσεγγίσεων στο πλαίσιο του καθορισμού αρχών αναφορικά με την προσέγγιση του ερευνητή. Τα ερωτήματα έχουν να κάνουν με το κατά πόσο οι αρχές αυτές καλύπτουν όλο το φάσμα της εγκληματικής δράσης και συνακόλουθα το κατά πόσο καλύπτουν όλα τα ενδεχόμενα που καλείται να διαχειριστεί ο ανακριτικός υπάλληλος. Οι θεωρητικές ενστάσεις διατηρούνται αναφορικά με την αοριστία στην διατύπωση των αρχών, στην στασιμότητα της δομής τους σε έναν ολοένα ταχύτερα εξελισσόμενο χώρο, όπως αυτός των τεχνολογιών αιχμής (η αναφορά των αρχών αυτών έχει τις ρίζες της στο έτος 1998 και η τελευταία εκδοχή – αναβάθμισή τους, είναι του έτους 2009)[316].

Προτείνεται λοιπόν μια σχετική αναθεώρηση των προαναφερομένων αρχών από τον Gr. Horsman[317], σύμφωνα με την οποία διαμορφώνεται μια νέα βάση με οκτώ (8), πλέον, αρχές, μερικές από τις οποίες ομολογουμένως θα μπορούσαν να συμπτυχθούν στις ήδη υπάρχουσες. Άξιες αναφοράς, ως καινοτόμες οι προτάσεις για α) εποπτεία της έρευνας στη νομική της πλαισίωση από κρατικό λειτουργό, αλλά η τεχνική επιστασία να ανήκει σε ιδιώτη τεχνικό (διαίρεση αρμοδιοτήτων), β) προβολή της αρχής της αναγκαιότητας και του σκοπού, γ) εφαρμογή μόνο τεχνικώς γνωστών κι επιστημονικώς αποδεκτών (παραδεδεγμένων) μεθόδων, δ) έλεγχος της ακρίβειας των δεδομένων (accurancy) μέσα από τεχνικές δοκιμασίες σε όλα τα εξαγόμενα δεδομένα.

[316] Βλ. *Gr. Horsman*, ACPO principles for digital evidence: Time for an update?, February 2020, Forensic Science International: Reports, https://www.sciencedirect.com/science/article/pii/S2665910720300220
[317] Βλ. *Gr. Horsman*, ACPO principles for digital evidence: Time for an update?, ο.π. σελ. 3 επ.

Περαιτέρω θα πρέπει είναι μεν σημαντική η τήρηση σταθερών πρακτικών που είναι αποδεκτές από την επιστημονική κοινότητα, θα πρέπει όμως να υπάρξει και η δυνατότητα πρωτοβουλιών του ερευνητή βάσει τεχνικών ενεργειών σε ιδιόμορφες καταστάσεις, προκειμένου να καταστεί ουσιαστικό το έργο της έρευνας. Η θέση αυτή δεν αντιστρατεύεται σε τίποτε την προηγούμενη σχετική αναφορά. Η ουσία της διατύπωσης εδώ έχει να κάνει με την επιλογή της σταθερής πρακτικής και υποδεικνυόμενης, ως παραδεδεγμένης, τακτικής, στις περιπτώσεις όμως που δεν δίδεται απάντηση – πρόταση ενεργειών βάσει των συνήθων πρακτικών τότε σαφώς η έρευνα δεν θα περιοριστεί αλλά θα ενεργήσει με πρωτοβουλία ο ειδικός ερευνητής. Σε κάθε όμως περίπτωση παραμένει ως υποχρέωσή του η τεκμηρίωση βάσει των παραμέτρων του προτύπου ISO 17025:2017[318] για την Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος και 17020:2012[319] για τα ψηφιακά πειστήρια, πάντα αναφορικά με το παραδεκτό της δικαστικής αξιοποίησης των ψηφιακών δεδομένων που θα αντληθούν.

[318] Βλ. https://www.qlc.gr/?section=1812&language=el_GR
[319] Βλ. http://qic-eg.com/wp-content/uploads/2015/08/ISO-17020-2012.pdf

10. ΠΡΩΤΟΚΟΛΛΟ ΕΡΕΥΝΑΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗΣ ΤΩΝ ΨΗΦΙΑΚΩΝ ΠΕΙΣΤΗΡΙΩΝ ΚΑΙ ΤΩΝ ΨΗΦΙΑΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η παρουσία του ανακριτικού υπαλλήλου στον τόπο της έρευνας αποτελεί ένα πολυσχιδές, πολύπλευρο και πολυσήμαντο δεδομένο, καθοριστικό και χαρακτηριστικό της αξίας του έργου που θα παραχθεί. Η σαφής αλλά και ασφαλής απεικόνιση και απόδοση των όσων εντοπίζει στον χώρο της έρευνας ο πρώτος αποκριτής (επεμβαίνων ερευνητής ανακριτικός υπάλληλος) είναι ιδιαίτερα σημαντική.

Και είναι ιδιαίτερα σημαντική τόσο προς την κατεύθυνση της αναζήτησης όλων των πειστηρίων, με τα οποία εμπλουτίζει την έρευνα ο χώρος, της άντλησης της μεγαλύτερης δυνατής πληροφορίας από αυτά αναφορικά πάντα με την έρευνα αλλά ταυτόχρονα είναι και ο θεματοφύλακας της ακεραιότητας της πληροφορίας και της εξασφάλισης του ότι η πληροφορία αυτά θα παραμείνει αναλλοίωτη, παρέχοντας με την διττή αυτήν λειτουργία του υπηρεσίες στην εξεύρεση της ουσιαστικής αλήθειας αλλά και προστασίας των δικαιωμάτων του κατηγορουμένου ή υπόπτου.

Η κατανόηση της παρούσας ενότητας επιβάλλει την σταθερή υπόμνηση των βασικών αρχών που διέπουν όλη την έρευνα αναφορικά με τα ψηφιακά δεδομένα και ιδιαίτερα τα χαρακτηριστικά[320] τους, αλλά και τις βασικές αρχές έρευνας, οι οποίες εκτέθηκαν στην αμέσως προηγούμενη ενότητα[321].

Είναι ιδιαίτερα σημαντικό λοιπόν το τί αντικρίζει στον χώρο κατά την επέμβασή του ο πρώτος αποκριτής, διότι ακόμη και από την πρώτη διάταξη των πειστηρίων στον χώρο είναι πολύ πιθανό να μπορούν να εξαχθούν συμπεράσματα, όπως λ.χ. αν ο χώρος καταλήφθηκε επ' αυτοφώρω, αν ο δράστης εγκατέλειψε τον χώρο αρκετό καιρό ή λίγο πριν την επέμβαση των αρχών, πράγμα που με την σειρά του μπορεί να δημιουργήσει προϋποθέσεις άντλησης πορισμάτων αναφορικά με το εάν είναι πιθανό το σενάριο εντοπισμού σφαλμάτων του δράστη, λόγω της σπουδής ή, ανάλογα, του επαρκούς χρόνου που είχε στην διάθεσή του για να απομακρυνθεί από τον χώρο και να εξαφανίσει τα ίχνη του.

Φυσικά για να ανταποκριθεί στον ρόλο του αυτόν ο ερευνητής πρώτης επέμβασης και επιτόπιας αναφοράς πρέπει να είναι εξοπλισμένος με τον κατάλληλο τεχνικό εξοπλισμό.

[320] Βλ. ανωτέρω υπό 7. Τα Ψηφιακά Δεδομένα*, Γ) τεχνικά χαρακτηριστικά και χαρακτηριστικά περιεχομένου των ψηφιακών δεδομένων*, σελ. 81 επ..

[321] Βλ. ανωτέρω υπό 9. Οι Αρχές που Διέπουν την Έρευνα αναφορικά με τα Ψηφιακά Πειστήρια και τα Ψηφιακά Δεδομένα, σελ. 151 επ.

Όταν ο λόγος γίνεται για την ανακριτική έρευνα αναφορικά με την εξιχνίαση ηλεκτρονικού εγκλήματος ασφαλώς οι εξοπλιστικές απαιτήσεις διαφέρουν, όπως φυσικά υπάρχουν διαφοροποιήσεις αναφορικά με τα κοινά εγκλήματα, που ανάλογα με την ετερότητα του προσβαλλόμενου εννόμου αγαθού, παρουσιάζουν ειδικότερες ερευνητικές απαιτήσεις. Ο εξοπλισμός αυτός πρέπει να είναι στην διάθεση του ερευνητή από την πρώτη στιγμή της επέμβασης καθόσον θα είναι ζωηρά ανακόλουθο, ίσως κι εγκληματικό για την πορεία της έρευνας, να απαιτείται η απομάκρυνσή του ή η μείωση της ασφάλειας στον χώρο, προκειμένου να αναζητηθεί ο εξοπλισμός μετά την επέμβαση. Βέβαια τέτοια ενδεχόμενα δεν μπορεί να υπάρχουν στις περιπτώσεις οργανωμένων επεμβάσεων από τις αρχές και η αναφορά γίνεται θεωρητικά για την ανάδειξη της σημασίας του ενημερωμένου εξοπλισμού και μόνον για τον λόγο αυτόν. Δυστυχώς άλλα είναι τα στοιχεία, τα οποία πρέπει να τύχουν προσοχής στην ανακριτική δράση αυτήν, ιδίως αναφορικά με την προστασία των δικαιωμάτων του κατηγορουμένου, αλλά σε αυτή την παράμετρο αναφερόμαστε σε άλλο σημείο[322] της μελέτης.

Την όλη διαδικασία, την επιτόπια εμφάνιση και την ανάληψη δράσης στο χώρο (πρέπει να) την καθορίζει μια σταθερή και συνεπής στην εξέλιξή της, αλληλουχία ενεργειών, με επιβλέποντα τον πρώτο αποκριτή. Ουσιαστικά εδώ γίνεται λόγος για την τήρηση ενός πρωτοκόλλου δράσης. Μιας λεπτομερούς καταγραφής αναφορικά με όλες τις πράξεις που γίνονται για την εξυπηρέτηση του σκοπού της έρευνας, ένα σύνολο κανόνων, μια σπονδυλωτή διάταξη ενεργειών, οι οποίες πρέπει να ακολουθούνται, πάντα σε σχέση με την διασφάλιση των αρχών που διέπουν την έρευνα. Διεθνώς έχει αναπτυχθεί μεθοδολογία[323] και με την μορφή οδηγού, εφαρμόζεται η ίδια πρακτική.

Για οικονομία, όπου κατωτέρω γίνεται αναφορά σε έγκλημα ή σε τόπο τέλεσης εγκλήματος, εννοείται ότι αναφερόμαστε πάντα σε ηλεκτρονικό έγκλημα και τα όσα ανάλογα αναμένει να απαντήσει κανείς στον χώρο διάπραξης μιας τέτοιας συμπεριφοράς.

i. Τα αντικείμενα στο ερευνητικό πεδίο των ηλεκτρονικών εγκλημάτων – Το υλισμικό που ενδέχεται να εντοπίσει ο ερευνητής.

[322] Βλ. παρακάτω υπό 11. Κατάσχεση Ψηφιακών Δεδομένων και Δικαιώματα Κατηγορουμένου υπό το Φως των Εγγυήσεων Προστασίας των Ατομικών Δικαιωμάτων και της Νομολογίας του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων Ανθρώπου (ΕΔΔΑ), σελ. 193 επ.

[323] Βλ. λ.χ. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, «Electronic Crime Scene Investigation, A Guide for First Responders, Second Edition». https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

Πρόκειται για οτιδήποτε μπορεί να φιλοξενήσει, επεξεργαστεί, διαχειριστεί και να αποθηκεύσει ψηφιακά δεδομένα ή ακατέργαστα ηλεκτρονικά δεδομένα. Εδώ συγκαταλέγονται πλακέτες κυκλωμάτων, μικροεπεξεργαστές, ο σκληρός δίσκος της υπολογιστικής μηχανής, εξωτερικός σκληρός δίσκος, μνήμες, ελεύθερες ή σε συναρμογή υφιστάμενες και συνδέσεις διασύνδεσης. Υποστηρικτικά εργαλεία για την διαχείριση των ψηφιακών δεδομένων, όπως οθόνη ή συσκευή προβολής αρχείων εικόνας ήχου, πληκτρολόγιο, συσκευή εισόδου (το γνωστό «ποντίκι» - mouse), περιφερειακές ή εξωτερικά συνδεδεμένες μονάδες δίσκου, κινητά τηλέφωνα, ταμπλέτες, συσκευές και εξαρτήματα, όπως μονάδες usb, αφαιρούμενα μέσα κλπ.

Τα αφαιρούμενα μέσα είναι υλικοί υποδοχείς ψηφιακών δεδομένων και συσκευές αποθήκευσης δεδομένων [όπως κάρτες Secure Digital (SD) mini και micro, Smart Media (SM), υποδοχέας Memory Stick)], που συνήθως χρησιμοποιούνται για την αποθήκευση, αρχειοθέτηση, μεταφορά και μεταφορά δεδομένων και άλλων πληροφοριών.

Τα συστήματα υπολογιστών μπορούν να λάβουν πολλές μορφές, όπως φορητούς υπολογιστές, επιτραπέζιους υπολογιστές, συστήματα που βασίζονται σε βιομηχανικούς διακομιστές (rack-servers), μικροϋπολογιστές και κεντρικούς («μεγάλους») υπολογιστές (mainframes). Πρόσθετα εξαρτήματα και περιφερειακές συσκευές περιλαμβάνουν μόντεμ, δρομολογητές, κόμβους (διανομείς) σε δίκτυο υπολογιστών (hubs), εκτυπωτές, σαρωτές και σταθμούς σύνδεσης.

Ένα σύστημα υπολογιστή και τα στοιχεία του μπορεί να αποτελέσουν πολύτιμα στοιχεία σε μια έρευνα. Το υλικό, το λογισμικό, τα έγγραφα, οι φωτογραφίες, τα αρχεία εικόνας, το ηλεκτρονικό ταχυδρομείο και τα συνημμένα, βάσεις δεδομένων, οικονομικές πληροφορίες, ιστορικό περιήγησης στο Διαδίκτυο, αρχεία καταγραφής συνομιλιών, λίστες φίλων, αρχεία καταγραφής συμβάντων, δεδομένα που είναι αποθηκευμένα σε εξωτερικές συσκευές και ταυτοποίηση πληροφοριών που σχετίζονται με το σύστημα του υπολογιστή και τα συστατικά είναι όλα πιθανά στοιχεία.

Οι συσκευές αποθήκευσης ποικίλλουν σε μέγεθος και στον τρόπο με τον οποίο αποθηκεύουν και διατηρούν δεδομένα. Ο προανακριτικός υπάλληλος, ως πρώτος αποκριτής πρέπει να αντιληφθεί και προετοιμαστεί κατάλληλα, σύμφωνα και με τα κατωτέρω αναφερόμενα, καθόσον ανεξάρτητα από το μέγεθος ή τον τύπο τους, αυτές οι συσκευές ενδέχεται να περιέχουν πληροφορίες που είναι πολύτιμες για μια έρευνα ή δίωξη.

Σημαντικό στοιχείο στην έρευνα επιβάλλει η επισήμανση, που έχει να κάνει με την ευμεταβλητότητα των ψηφιακών δεδομένων, σύμφωνα με την οποία ανάλογα με τη συσκευή και τη θέση, από άποψη λειτουργίας, στην οποία θα εντοπιστούν τα ψηφιακά δεδομένα ή ψηφιακά στοιχεία (ηλεκτρονικά ακατέργαστα δεδομένα) ενδέχεται να χαθούν εάν δεν διατηρηθεί η ισχύς. Επίσης σημαντική η επισήμανση ότι ψηφιακά δεδομένα ή ψηφιακά στοιχεία σε ορισμένες συσκευές, όπως κινητά ή έξυπνα τηλέφωνα, μπορεί η μνήμη τους να αντικατασταθεί ή να διαγραφεί ενώ η συσκευή παραμένει ενεργοποιημένη, ενώ σύμφωνα με τεχνικές που υφίστανται μπορεί να υπάρχει διαθέσιμο λογισμικό για κινητά και έξυπνα τηλέφωνα, τα οποία μπορούν να ενεργοποιηθούν εξ αποστάσεως για να καταστήσουν τη συσκευή άχρηστη και να καταστήσουν τα δεδομένα που περιέχουν σε τέτοια συνθήκη ώστε να μην είναι προσβάσιμα εάν το τηλέφωνο χαθεί ή κλαπεί. Αυτό το λογισμικό μπορεί να παράγει παρόμοια αποτελέσματα, ουσιαστικά «κλείδωμα» της συσκευής ή μέρους των εφαρμογών ή του λειτουργικού της στην περίπτωση που η συσκευή κατασχέθηκε στα πλαίσια ανακριτικής έρευνας. Έχοντας αυτά υπόψη ο πρώτος αποκριτής πρέπει να λάβει προφυλάξεις για να αποτρέψει την απώλεια δεδομένων σε συσκευές, οι οποίες κατάσχονται ή καταλαμβάνονται στον τόπο του εγκλήματος ως αποδεικτικά στοιχεία.

Τέλος, ιδιαίτερης προσοχής πρέπει να τύχει το στοιχείο της διασύνδεσης των υπολογιστικών μηχανών, καθόσον η διασύνδεση, ιδίως η ενσύρματη, που είναι ευκολοδιάγνωστη, μπορεί να παραπέμψει σε άλλο τόπο που συνέχεται με εκείνον της πρώτης επέμβασης. Ιδιαίτερα σημαντική η αναφορά στοιχείων σε απομακρυσμένο server στα πλαίσια και στη δομή της νεφοϋπολογιστικής[324]. Οι δικτυωμένοι υπολογιστές και οι συνδεδεμένες συσκευές μπορεί να είναι ως «ενιαία λειτουργικά σύνολα» αποδεικτικά στοιχεία χρήσιμα για την έρευνα ή την δίωξη. Τα δεδομένα που περιέχουν και οι πληροφορίες μέσα από την διασύνδεση, μπορεί επίσης να είναι πολύτιμα στοιχεία και μπορεί να υποδεικνύουν άλλους δράστες στα πλαίσια συναυτουργικής δράσης αλλά και να περιλαμβάνουν λογισμικό, ιστορικό περιήγησης στο διαδίκτυο, μηνύματα ηλεκτρονικού ταχυδρομείου και συνημμένα αρχεία, αρχεία εικόνας, φωτογραφίες, έγγραφα, βάσεις δεδομένων, οικονομικές πληροφορίες, αρχεία καταγραφής, αρχεία καταγραφής συμβάντων και συνομιλιών, λίστες φίλων και δεδομένα αποθηκευμένα ακόμη και σε εξωτερικές συσκευές. Οι λειτουργίες της συσκευής, οι δυνατότητες και οποιεσδήποτε πληροφορίες αναγνώρισης που σχετίζονται με το σύστημα του υπολογιστή. στοιχεία και συνδέσεις,

[324] Εκτεταμένη αναφορά έγινε ανωτέρω 8. Η Κατάσχεση των Ψηφιακών Δεδομένων (κατ' άρθρο 265 Κ.Ποιν.Δ., *vi. Η κατάσχεση των ψηφιακών πειστηρίων και των ψηφιακών δεδομένων στα πλαίσια της ανακριτικής έρευνας, Γ. σε σύστημα και υπηρεσίες νεφοϋπολογιστικής (cloud services)*, σελ. 110 επ.

συμπεριλαμβανομένων διευθύνσεων πρωτοκόλλου Διαδικτύου (IP) και τοπικού δικτύου (LAN), που σχετίζονται με υπολογιστές και συσκευές. ρυθμίσεις εκπομπής και οι διευθύνσεις της κάρτας πρόσβασης πολυμέσων (MAC) ή της κάρτας διασύνδεσης δικτύου (NIC), μπορεί επίσης να είναι χρήσιμες ως αποδεικτικά στοιχεία.

ii. Τεχνική Υποδομή - Τεχνικός Εξοπλισμός του πρώτου αποκριτή – ανακριτικού υπαλλήλου

Όπως ρητά αναφέρεται και στην διάταξη του άρθρου 265 § 2 Κ.Ποιν.Δ., ο ερευνητής πρέπει για τις ενέργειές του να φέρει *κατάλληλο εξοπλισμό*, που θα επιτρέψει τις απαραίτητες ερευνητικές δράσεις, χωρίς όμως να θέτει σε κίνδυνο την ακεραιότητα των υλικών φορέων και των ψηφιακών δεδομένων που θα αντληθούν από αυτούς.

Ο πρώτος λοιπόν αποκριτής (First Responder), που είναι ο επικεφαλής ή ο υποδειχθείς από τον επικεφαλής ανακριτικό υπάλληλο, ο οποίος έχει την αρχική επαφή με τον τόπο όπου φέρεται ότι τελέστηκε εγκληματική ενέργεια, οφείλει να επέμβει με πλήρη σχετικό εξοπλισμό, ώστε πέρα από όλα τα ανωτέρω στοιχεία που μπορεί να συναντήσει στο χώρο, να έχει υπόψη του και τον εντοπισμό των στοιχείων που μπορεί να συναντήσει και σε περιβάλλοντα κοινής (παραδοσιακής) εγκληματικής δράσης. Το γεγονός ότι θα αναζητήσει ψηφιακά ίχνη, δεν ανεξαρτητοποιούν, ή καλύτερα, δεν «απαλλάσσουν» την έρευνά του από τον εντοπισμό και τη σήμανση λοιπών στοιχείων, όπως το υλικό (DNA), δακτυλικά αποτυπώματα, υλικό (μη ηλεκτρονικό), που μπορεί να συνδέουν συγκεκριμένο πρόσωπο με τον χώρο της εγκληματικής δράσης.

Στις περισσότερες περιπτώσεις, αντικείμενα ή συσκευές που περιέχουν ψηφιακά αποδεικτικά στοιχεία μπορούν να συλλεχθούν χρησιμοποιώντας τυπικά εργαλεία και υλικά κατάσχεσης. Ο ανακριτικός υπάλληλος κατά την επαφή του με τον χώρο και τα αντικείμενα, μετά την καταγραφή και φωτογράφισή τους, ως ενδεικνυόμενες μεθόδους για την απεικόνιση της πραγματικότητας στην στιγμή της *πρώτης επαφής*, πρέπει να είναι ιδιαίτερα προσεκτικός προκειμένου να μην γίνει (από αμέλειά του) η αιτία αλλοίωσης του αποδεικτικού υλικού.

Πρέπει να είναι ιδιαίτερα προσεκτικός κατά τον εντοπισμό, την επαφή με το υλικό κατά τη συλλογή, τη συσκευασία ή την αποθήκευση ψηφιακών συσκευών, έτσι ώστε να αποφευχθεί η περίπτωση αλλοίωσης, πρόκλησης ζημίας ή καταστροφής των ψηφιακών στοιχείων. Σημαντική παράμετρος σε όλες αυτές τις ενέργειες είναι η προσπάθεια, την οποία οφείλει να καταβάλλει ο ερευνητής προκειμένου να λειτουργήσει σε ηλεκτρομαγνητικά

ουδέτερο περιβάλλον καθόσον η χρήση μερικών εργαλείων ή υλικών, τα οποία ενδέχεται να παράγουν ή να εκπέμπουν στατικό ηλεκτρισμό ή μαγνητικό πεδίο, θα μπορούσε να προκαλέσει ζημιά ή καταστροφή των στοιχείων.

Εάν η πολυπλοκότητα μιας ηλεκτρονικής σκηνής εγκλήματος υπερβαίνει την εμπειρία ενός πρώτου αποκριτή, αυτός ο ανακριτικός υπάλληλος, αφού ενεργήσει για την ασφάλιση του χώρου με τον αποκλεισμό οποιουδήποτε αναρμοδίου προσώπου, θα πρέπει να ζητήσει άμεσα βοήθεια από ειδικευμένους ερευνητές με προηγμένο εξοπλισμό και εκπαίδευση στη συλλογή ψηφιακών αποδεικτικών στοιχείων. Η έλλειψη ειδικών γνώσεων αναφορικά με το ψηφιακό περιβάλλον μπορεί να οδηγήσει είτε σε αλλοίωση είτε σε καταστροφή αποδείξεων με αποτέλεσμα την απώλεια σημαντικού υλικού για την δικαστική διερεύνηση της υπόθεσης.

Βάσει όλων των προαναφερομένων παραμέτρων, πέρα δε από τον εξοπλισμό για την διαχείριση χώρων τέλεσης κοινής εγκληματικής δράσης, ο ανακριτικός υπάλληλος που είναι επικεφαλής στον τόπο, πρέπει να έχει ειδικό εξοπλισμό στην εργαλειοθήκη συλλογής ψηφιακών αποδεικτικών στοιχείων, όπως είναι κάμερες (για λήψη φωτογραφίας και βίντεο), χαρτοκιβώτια, ειδικά έντυπα σημειώσεων αυτοκόλλητα (με τρόπο ασφαλή και όχι επιπόλαιο, που θα μπορούσε να οδηγήσει σε σύγχυση αναφορικά με την ταυτότητα του αντικειμένου το οποίο σημαίνει), ελαστικά γάντια μιας χρήσης, αρχεία καταγραφής αποδεικτικών στοιχείων, ταινία αποδεικτικών στοιχείων, ανεξίτηλη γραφίδα, ταινία αποκλεισμού πρόσβασης στον ερευνώμενο χώρο (ως χώρο τέλεσης εγκλήματος) έντονης κι ευδιάκριτης απόχρωσης ή συνδυασμού αποχρώσεων, αντιστατική σακούλα, μη μαγνητικά εργαλεία (κατσαβίδια κοινά, κατσαβίδια ακριβείας ωρολογοποιών, κινητών, H/Y, Am-Tech L0475, πένσα, τσιμπίδα, καρυδάκια).

Θα πρέπει επίσης να διαθέτει υλικό θωράκισης ραδιοσυχνοτήτων όπως σακούλες απομόνωσης faraday ή αλουμινόχαρτο για να τυλίγει κινητά τηλέφωνα, έξυπνα τηλέφωνα και άλλες κινητές συσκευές επικοινωνίας μετά την κατάσχεσή τους. Το τύλιγμα των τηλεφώνων σε υλικό προστασίας ραδιοσυχνοτήτων αποτρέπει τα τηλέφωνα από τη λήψη κλήσης, μηνύματος κειμένου ή άλλου σήματος επικοινωνίας που μπορεί να αλλοιώσει την τάξη και τα στοιχεία, τα οποία υφίστανται κατά το χρόνο της επέμβασης.

Έχοντας αυτά στην εργαλειοθήκη του ο ανακριτικός υπάλληλος, κι έχοντας υπόψη του αυτό που ενδέχεται να συναντήσει στον χώρο όπου θα γίνει η επέμβαση, είναι έτοιμος για την είσοδο στον χώρο.

iii. Η πρώτη επέμβαση – είσοδος στον χώρο της έρευνας.

Ο ανακριτικός υπάλληλος που θα επέμβει πρώτος πρέπει να διαθέτει την κατάλληλη εξουσία - όπως παρατήρηση με απλή άποψη, συγκατάθεση ή δικαστική εντολή - για αναζήτηση και συλλογή αποδεικτικών στοιχείων σε σκηνή ηλεκτρονικού εγκλήματος. Απαιτείται λοιπόν να είναι σε θέση να προσδιορίσει την αρχή βάσει της οποίας μπορεί να καταλάβει αποδεικτικά στοιχεία και φυσικά να είναι σε επικοινωνία με εκείνον που έχει διατάξει την έρευνα ή το εκπρόσωπο της δικαστικής αρχής σε κάθε περίπτωση, που θα ανακύψει ζήτημα που χρήζει άμεσης αντιμετώπισης, στα πλαίσια της απόδειξης της νομιμοποίησης της έρευνας.

Πρωταρχικό μέλημα του πρώτου αποκριτή - ανακριτικού υπαλλήλου πρέπει να είναι η εξασφάλιση του χώρου, με την έννοια της διατήρησης αναλλοίωτων των στοιχείων και δεδομένων που υφίστανται στον χώρο κατά την ώρα της επέμβασης. Οι ενέργειες που ακολουθούν βάσει πρωτοκόλλου αλγοριθμικής λογικής, επιβάλλουν να πρυτανεύει σε κάθε ενέργεια η λογική της διασφάλισης της εικόνας αυτής της πρώτης επέμβασης. Ο χώρος πρέπει να αποκλειστεί με την ειδική ταινία και οι συνεργάτες του ανακριτικού υπαλλήλου να είναι πρόσωπα συγκεκριμένα με καθορισμένους ρόλους. Λ.χ. ειδικός λήψης και αποτύπωσης στοιχείων εικόνας (φωτογράφος, εικονολήπτης), αναλυτής DNA, υπάλληλος για τον εντοπισμό και την ασφαλή λήψη δακτυλικών αποτυπωμάτων από επιφάνειες και φυσικά ειδικοί αναφορικά με τον εντοπισμό των ψηφιακών πειστηρίων, την δικτύωση, της περιφερειακές συσκευές, εξωτερικές μνήμες, στοιχεία αποθήκευσης δεδομένων. Βασικό στοιχείο η αποφυγή μετατόπισης στοιχείων ή η προσθήκη ξένων στοιχείων (το κατά πόσο αυτό είναι αυτονόητο αποτελεί βάση διατύπωσης απόψεων και προτάσεων σε άλλη θέση της μελέτης αυτής)[325].

Αφού ασφαλίσει τη σκηνή και όλα τα άτομα στη σκηνή, ο πρώτος αποκριτής θα πρέπει να προσδιορίσει οπτικά όλα τα πιθανά στοιχεία και να διασφαλίσει ότι διατηρείται η ακεραιότητα τόσο των ψηφιακών όσο και των παραδοσιακών στοιχείων. Πάντα θα πρέπει να έχει υπόψη του το ευμετάβλητο των ψηφιακών δεδομένων, ήτοι ότι τα ψηφιακά δεδομένα σε ηλεκτρονικούς υπολογιστές και άλλες ηλεκτρονικές συσκευές[326] μπορούν, με μη ενδεδειγμένη διαχείριση, να οδηγηθούν σε αλλοίωση (τροποποίηση ή ακόμη και διαγραφή η

[325] Βλ. παρακάτω σε αυτή την ενότητα υπό *Β) Η τεχνική πλευρά της ερευνητικής προσέγγισης*, σελ. 185 επ.
[326] Από την πλειάδα των ηλεκτρονικών στοιχείων (υλικών φορέων) φιλοξενίας – αποθήκευσης, που αναφέρθηκαν ανωτέρω στην ενότητα αυτήν, βλ. σελ. 176 επ.

καταστροφή). Ο ανακριτικός υπάλληλος θα πρέπει να αποδίδει με απεικόνιση και να τεκμηριώνει με την φωτογράφηση, το συντομότερο δυνατό στη σκηνή, ώστε με τον τρόπο αυτόν να ελαχιστοποιήσει έως να αποκλείσει τον κίνδυνο από την αμφισβήτηση του έργου του. Απαραίτητα με την είσοδο στον χώρο πρέπει να προβεί σε εντοπισμό, αναγνώριση, κατάσχεση και προστασία όλων των ψηφιακών αποδεικτικών στοιχείων στη σκηνή, αφού προηγουμένως έχει λάβει όλα τα μέσα για την εξασφάλιση του γεγονότος ότι οι καταγραφές του επιβεβαιώνονται από την απεικόνιση ολόκληρης της σκηνής, με την απεικόνιση σε κάθε επί μέρους τοποθεσία των στοιχείων που βρέθηκαν και με τρόπο φωτογράφισης τέτοιο, που να επιτρέπει την ευχερή αναγνώριση της θέσης στον τρίτο που θα αξιολογήσει το τεχνικό πόνημα στο τέλος. Αυτή η συνοχή στην διαδοχή των φωτογραφιών στον χώρο γίνεται με την ειδικότερη σήμανση κάθε στοιχείου, είτε με σταθερό στοιχείο αναφοράς.

Για την απόδοση της αλήθειας στον τόπο του συμβάντος πρέπει να συλλέξει, επισημάνει και διατηρήσει τα ψηφιακά στοιχεία σε συσκευασία και μεταφορά ψηφιακών στοιχείων με ασφαλή τρόπο.

Πριν από τη συλλογή αποδεικτικών στοιχείων σε μια σκηνή εγκλήματος, ο ανακριτικός υπάλληλος πρέπει να διασφαλίσει ότι α) υπάρχει νομική αρχή για την κατάσχεση αποδεικτικών στοιχείων, β) ο χώρος της έρευνας έχει ασφαλιστεί και τεκμηριωθεί και γ) χρησιμοποιείται κατάλληλος εξοπλισμός ατομικής προστασίας.

Από εδώ και μετά οφείλει να ακολουθήσει το πρωτόκολλο ενεργειών έρευνας αλλά πάνω από όλα την λογική, που θα δώσει λύσεις σε ενδεχόμενο συνάντησης ή διαχείρισης μιας καινοφανούς συνθήκης στον χώρο. Η λογική της φύσης της έρευνας θα δώσει την λύση εκεί που δεν υπάρχει πρόταση και αυτό πάντοτε βάσει των κριτηρίων, που αναφέρθηκαν ανωτέρω, για την διασφάλιση της ακεραιότητας των ψηφιακών δεδομένων.

Με επικέντρωση στο έργο της ερευνητικής διαχείρισης των ψηφιακών συσκευών, θα ασφαλίσει αμέσως όλες τις ηλεκτρονικές συσκευές, συμπεριλαμβανομένων προσωπικών ή φορητών συσκευών. Και τούτο με την έννοια ότι δεν μπορεί να υπάρξει, τουλάχιστον στον χώρο, μη εξουσιοδοτημένη και από μη ειδικό, επέμβαση στις ψηφιακές μηχανές.

Στα πλαίσια αυτής της λογικής θα πρέπει να αρνηθεί οποιαδήποτε προσφορά βοήθειας ή τεχνικής βοήθειας από μη εξουσιοδοτημένα άτομα. Αν μάλιστα απαιτείται η πρόσκληση ειδικού, αυτή θα γίνει από τον επί κεφαλής υπάλληλο, βάσει του σχετικού καταλόγου που θα έχει στην διάθεσή του.

Σημαντικότερη παράμετρος αναφορικά με τον πυρήνα της έρευνας είναι η διασφάλιση ότι η λειτουργική κατάσταση οποιασδήποτε ηλεκτρονικής συσκευής δεν έχει μεταβληθεί. Έτσι δεν θα τεθεί σε λειτουργία κανείς ηλεκτρονικός υπολογιστής απενεργοποιημένος εάν είναι ήδη απενεργοποιημένος κατά την επέμβαση, ή αν βρίσκεται ήδη σε λειτουργία δεν θα τερματιστεί αυτή, δεν θα αφαιρεθεί η παροχή ενέργειας ή δεν θα δοθεί κάποια άλλη εντολή στην μηχανή.

Στοιχεία όπως πληκτρολόγιο, ποντίκι, αφαιρούμενα μέσα αποθήκευσης και άλλα αντικείμενα ενδέχεται να περιέχουν λανθάνουσες ενδείξεις όπως δακτυλικά αποτυπώματα, DNA ή άλλα φυσικά στοιχεία που πρέπει να διατηρηθούν. Ο ανακριτικός υπάλληλος πρέπει να λάβει τα κατάλληλα μέτρα για να διασφαλίσει ότι τα φυσικά αποδεικτικά στοιχεία δεν διακυβεύονται κατά την τεκμηρίωση.

Εάν ένας υπολογιστής είναι ενεργοποιημένος ή δεν μπορεί να προσδιοριστεί η κατάσταση ισχύος, ο πρώτος αποκριτής οφείλει να:

- Ερευνήσει, τόσο τεχνικά όσο και εμπειρικά (με την έννοια ακόμη και να αφουγκραστεί) αναζητώντας ενδείξεις ότι ο ηλεκτρονικός υπολογιστής είναι ενεργοποιημένος. Στα πλαίσια αυτά μπορεί να αναζητήσει τον ήχο των ανεμιστήρων σε λειτουργία ή να ελέγξει αν είναι ενεργοποιημένες οι δίοδοι εκπομπής φωτός (LED).
- Ελέγξει την οθόνη για σημάδια ότι τα ψηφιακά στοιχεία καταστρέφονται. Οι λέξεις που πρέπει να προσέξει περιλαμβάνουν όρους όπως «*διαγραφή* (delete)», «*μορφοποίηση* (format)», «*αφαίρεση* (remove)», «*αντιγραφή* (copy)», «*μετακίνηση* (move)», «*αποκοπή* (cut)» ή «*διαγραφή* (wipe)».
- Αναζητήσει ενδείξεις αναφορικά με το εάν η πρόσβαση στον ηλεκτρονικό υπολογιστή γίνεται, ή ακόμη και ενδεχόμενο να μπορεί να επιχειρηθεί, από έναν απομακρυσμένο υπολογιστή ή συσκευή.
- Αναζητήσει ενδείξεις ενεργών ή συνεχιζόμενων επικοινωνιών με άλλους υπολογιστές ή χρήστες, όπως παράθυρα άμεσων μηνυμάτων ή περιοχές (αίθουσες) συνομιλίας (chat rooms).
- Σημειώσει όλες τις κάμερες ή κάμερες Web (Web Cams) και προσδιορίσει εάν είναι ενεργές.

Οι εξελίξεις στην τεχνολογία και η σύγκλιση τεχνολογιών και των δυνατοτήτων επικοινωνίας έχουν συνδέσει τις πιο συμβατικές συσκευές και υπηρεσίες μεταξύ τους, με

υπολογιστές και στο Διαδίκτυο. Αυτό το ταχέως μεταβαλλόμενο περιβάλλον καθιστά απαραίτητο για τον ανακριτικό υπάλληλο να γνωρίζει τις πιθανές ψηφιακές ενδείξεις στα τηλέφωνα, τις ψηφιακές συσκευές εγγραφής βίντεο, άλλες οικιακές συσκευές[327] και τα μηχανοκίνητα οχήματα[328].

Για το ενδεχόμενο είτε άντλησης πληροφορίας αναφορικά με πρόσωπα και καταστάσεις που μπορούν να διαφωτίσουν την ερευνώμενη πράξη (λ.χ. στην επέμβαση στα γραφεία μιας εταιρίας που ασχολείται με χρηματιστηριακά προϊόντα ή με επενδυτικές εν γένει προτάσεις), ο ανακριτικός υπάλληλος πρέπει να διαχωρίσει και να προσδιορίσει όλα τα (ενήλικα) άτομα που εμφανίζονται να έχουν ενδιαφέρον στη σκηνή του εγκλήματος και να καταγράψουν τη θέση τους κατά τη στιγμή της εισόδου στον χώρο. Κάποιοι από αυτούς μπορεί να είναι άτομα που ενδεχόμενα θα αξιοποιηθούν ως μάρτυρες ή εξελικτικά και τελικά υπόπτους αναφορικά με την εξιχνίαση της ερευνώμενης πράξης. Το ενδεχόμενο να έχει προηγηθεί η σύλληψη και απομάκρυνση από τον χώρο του καταγγελθέντος, δεν εξασφαλίζει ότι δεν υπάρχει κάποιος εναλλακτικός σχεδιασμός για καταστροφή ή απόκρυψη στοιχείων, κάτι που μπορεί να γίνει με μια απλή εντολή στον ηλεκτρονικό υπολογιστή. Η άμεση σύλληψη και μετέπειτα ποινική δίωξη (ακόμη και επ' αυτοφώρω) του δράστη αυτού (ενός έμπιστου υπαλλήλου της διοίκησης λ.χ. στην περίπτωση της εταιρίας με την διαχείριση των οικονομικών προϊόντων) δεν θα αποκλείσει την απώλεια στοιχείων που αφορούν την μείζονα δίωξη για την κυρία πράξη που αποτέλεσε και την βάση για την έρευνα.

Έτσι σε κάθε περίπτωση σε κανέναν από αυτά τα πρόσωπα δεν πρέπει να επιτρέπεται η πρόσβαση σε οποιονδήποτε υπολογιστή ή ηλεκτρονική συσκευή. Την ίδια στιγμή οι

[327] Βλ. *M.U. Farooq, M. Waseem, Anj. Khairi, S. Mazhar,* "A Critical Analysis on the Security Concerns of Internet of Things (IoT)", International Journal of Computer Applications (0975 8887), Volume 111 - No. 7, February 2015, *L. D. X. Z. Shancang Li*, «The internet of things: a survey,» Information Systems, Frontiers, p. 243–259, April 2015, *V. A. Memos, K. E. Psannis, Y. Ishibashi, Byung-Gyu Kim, B.B. Gupta*, An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework, Researchgate 2018.

[328] Βλ. *N. Shaukata, S.M. Alia, C.A. Mehmooda, B. Khana, M. Jawadb, U. Farida, Z. Ullaha, S.M. Anwarc, M. Majidd,* A survey on consumers empowerment, communication technologies, and renewable generation penetration within Smart Grid, Renewable and Sustainable Energy Reviews, Volume 81, Part 1, January 2018, Pages 1453-1475, https://www.researchgate.net/profile/Zahid_Ullah2/publication/317621899_A_survey_on_consumers_empowerment_communication_technologies_and_renewable_generation_penetration_within_SSmar_Grid/links/5b9e8dc5a6fdccd3cb5dd08b/A-survey-on-consumers-empowerment-communication-technologies-and-renewable-generation-penetration-within-Smart-Grid.pdf, *L. D. X. Z. Shancang Li*, «The internet of things: a survey,» Information Systems, Frontiers, p. 243–259, April 2015, *V. A. Memos, K. E. Psannis, Y. Ishibashi, Byung-Gyu Kim, B.B. Gupta*, An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework, Researchgate 2018.

ανακριτικοί υπάλληλοι πρέπει να λαμβάνουν όσο το δυνατόν περισσότερες πληροφορίες όπως[329]:

- Ονόματα όλων των χρηστών των υπολογιστών και των συσκευών.
- Όλες οι πληροφορίες χρηστών υπολογιστών και Διαδικτύου.
- Όλα τα ονόματα σύνδεσης και ονόματα λογαριασμών χρήστη.
- Σκοπό και χρήσεις υπολογιστών και συσκευών.
- Όλους τους κωδικούς πρόσβασης.
- Οποιαδήποτε αυτοματοποιημένη εφαρμογή χρησιμοποιείται.
- Τύπο πρόσβασης στο Διαδίκτυο.
- Οποιονδήποτε χώρο εκτός χώρου αποθήκευσης.
- Πάροχο υπηρεσιών Διαδικτύου.
- Εγκατεστημένη τεκμηρίωση λογισμικού.
- Όλους τους λογαριασμούς ηλεκτρονικού ταχυδρομείου (e-mail).
- Ενεργές διατάξεις ασφαλείας (ενδεχόμενα σε χρήση) .
- Πληροφορίες λογαριασμού αλληλογραφίας Ιστού.
- Περιορισμούς πρόσβασης δεδομένων που ισχύουν.
- Ενδεχόμενη ύπαρξη λογισμικού ή συσκευών καταστροφής δεδομένων που χρησιμοποιούνται.
- Πληροφορίες λογαριασμού ιστότοπου κοινωνικής δικτύωσης στο διαδίκτυο
- Οποιεσδήποτε άλλες σχετικές πληροφορίες.

iv. Η καταγραφή του ιστορικού της ανακριτικής έρευνας.

Πρακτικά η απόδειξη της ορθότητας ή μη των ενεργειών που έχουν ακολουθηθεί αναφορικά με την ανακριτική έρευνα στον χώρο, μπορεί να αποδειχθεί αλλά και να είναι αξιοποιήσιμη, μέσα από την καταγραφή των ενεργειών στα πλαίσια δημιουργίας ενός αρχείου για την έρευνα. Στο σημείο αυτό ενδιαφέρει περισσότερο η ιστορική περιεκτικότητα του εγγράφου που θα παραχθεί, ενώ με την νομική διάσταση και αποδεικτική σημασία της έγγραφης κατάδειξης αυτής, κάνουμε αναφορά σε άλλο σημείο της μελέτης[330]. Είναι λοιπόν ιδιαίτερα σημαντικό να γίνει καταγραφή όσο το δυνατόν με ακρίβεια της εικόνας που

[329] Βλ. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, «Electronic Crime Scene Investigation, A Guide for First Responders, Second Edition», https://www.ncjrs.gov/pdffiles1/nij/219941.pdf σελ. 17.

[330] Βλ. ανωτέρω υπό 8. Η Κατάσχεση των Ψηφιακών Δεδομένων (κατ' άρθρο 265 Κ.Ποιν.Δ.), *viii. Η ειδική έκθεση της § 3*, σελ. 124.

αντίκρισε στον χώρο ο ανακριτικός υπάλληλος. Αυτό μπορεί και πρέπει να γίνει περιφραστικά, όχι κατ' ανάγκη με άσκοπες υπερβολές στην περιγραφή, ενώ οι σημερινές δυνατότητες στα αρχεία κειμένου επιτρέπουν την ενσωμάτωση εικόνων στο κείμενο, για ενίσχυση της κατανόησης της καταγραφής. Στο αρχείο αυτό θα πρέπει να αποδίδεται όλη η συνθήκη και ιδιαίτερα αναφορικά με τις ηλεκτρονικές συσκευές η θέση τους στον χώρο της έρευνας, η συνδεσμικότητα των υπολογιστικών μηχανών, η διασύνδεση μεταξύ τους ως τοπικό δίκτυο ή η διαδικτυακή σύνδεσή τους αλλά και η κατάσταση ισχύος αυτών, των μέσων αποθήκευσης, των ασύρματων συσκευών δικτύου, των κινητών τηλεφώνων, των έξυπνων τηλεφώνων και γενικότερα κάθε συσκευής που έχει δυνατότητα διαχείρισης ή/και αποθήκευσης ψηφιακών δεδομένων. Σημαντική επίσης είναι η καταγραφή της δικτύωσης ως πρόσβαση στο διαδίκτυο και στο τοπικό δίκτυο.

Στα πλαίσια της ανακριτικής έρευνας ενδέχεται να απαιτηθεί η μερική, μικρότερη ή ριζικότερη μετακίνηση ενός ηλεκτρονικού υπολογιστή ή άλλης ηλεκτρονικής συσκευή για να αναζητηθούν, εντοπιστούν και καταγραφούν σειριακοί αριθμοί ή άλλα αναγνωριστικά. Όπως πολλές φορές έχει σημειωθεί η μετακίνηση πρέπει να είναι πολύ προσεκτική με διατήρηση της συνδεσμολογίας καθόσον είναι σε λειτουργία, διότι η παραμικρή αλλαγή ενδέχεται να προκαλέσει βλάβη ή τα ψηφιακά στοιχεία που περιέχει. Ο ερευνητικός – τεχνικός κανόνας, στον οποίον έχουμε αναφερθεί και σε άλλη θέση, ότι οι υπολογιστές και άλλες ηλεκτρονικές συσκευές δεν πρέπει να μετακινούνται έως ότου απενεργοποιηθούν διατηρεί την ισχύ και την σημασία του.

Κατά τη διεθνή πρακτική[331] γίνεται εκτενής αναφορά και υπόδειξη στην χρήση μηχανών λήψης εικόνας – ήχου και η σχετική έγγραφη κατάδειξη της ανακριτικής έρευνας υποδεικνύεται να συνοδεύεται από μια λεπτομερή εγγραφή αρχείου εικόνας - ήχου, φωτογραφίες και σκαριφήματα για να είναι νοητή κι εφικτή η αναδημιουργία ή αναπαράσταση της σκηνής αργότερα. Όλες οι δραστηριότητες και οι διαδικασίες στις οθόνες προβολής πρέπει να είναι πλήρως τεκμηριωμένες από τεχνικής και νομικής άποψης.

Πάντοτε θα υπάρχει το ενδεχόμενο, η έρευνα να επεκταθεί σε άλλο χώρο στον οποίο θα παραπέμπει είτε η συνδεσμικότητα είτε άλλα στοιχεία. Για το ενδεχόμενο αυτό ο

[331] Βλ. *Γ. Κωνσταντάς*, Εγκληματολογική εξέταση ψηφιακών πειστηρίων, 2016, https://www.forensicssociates.gr /el/psifiaka-peistiria, *Γ. Κουρβούλης*, Computer & Network, Εύρεση, ανάλυση ψηφιακών πειστηρίων σε υπολογιστές και δίκτυα (computer forensics), 2011 http://doccdn.simplesite.com/d/5e/99/282319406962284894/605fd94f-ab02-4248-823c-0351d371acb1 /KourvoulisGeorgiosMsc2011.pdf, *Β. Α. Μότσιος*, Forensics Analysis for e-Wallet, 2017, http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/10152/Motsios_Vasileios.pdf?sequence=1&isAllowed=y, *Ε. Καρρά – Τανισκίδου*, Δικανική Υπολογιστών (Computer Forensics), 2014, https://core.ac.uk/download/pdf/38466068.pdf,

ανακριτικός υπάλληλος θα πρέπει να αποδώσει με πλήρη πιστότητα τις σχετικές συνδέσεις ενσύρματες ή ασύρματες. Πρέπει λοιπόν να καταγράφονται σημεία δικτύου και ασύρματης πρόσβασης, τα οποία ενδέχεται να είναι παρόντα και ικανά να συνδέουν υπολογιστές και άλλες συσκευές μεταξύ τους στα πλαίσια τοπικού δικτύου αλλά και στο διαδίκτυο. Η ύπαρξη σημείων πρόσβασης δικτύου και ασύρματου δικτύου μπορεί να υποδηλώνει ότι υπάρχουν επιπλέον στοιχεία πέρα από το (αρχικό) ερευνητικό σημείο αναφοράς.

ν. Η συλλογή αποδεικτικού υλικού.

Α. Γενικές αναφορές

Οι ψηφιακές ενδείξεις πρέπει να αντιμετωπίζονται προσεκτικά για τη διατήρηση της ακεραιότητας της φυσικής συσκευής καθώς και των δεδομένων που περιέχει. Ορισμένα ψηφιακά στοιχεία απαιτούν ειδικές τεχνικές συλλογής, συσκευασίας και μεταφοράς. Τα δεδομένα μπορούν να καταστραφούν ή να τροποποιηθούν από ηλεκτρομαγνητικά πεδία, όπως αυτά που παράγονται από στατικό ηλεκτρισμό, μαγνήτες, ραδιοπομπούς και άλλες συσκευές. Οι συσκευές ηλεκτρονικής επικοινωνίας όπως τα κινητά τηλέφωνα, τα έξυπνα τηλέφωνα, οι προσωπικοί ψηφιακοί οδηγοί ή υπολογιστές (personal digital assistant - PDA) και οι τηλεειδοποιητές πρέπει να ασφαλίζονται με τεχνικά αναγνωρισμένο και παραδεδεγμένο τρόπο ώστε να αποτρέπεται η δυνατότητα που αφορά στην λήψη ή τη μετάδοση δεδομένων[332] μόλις αναγνωριστούν και συλλεχθούν ως αποδεικτικά στοιχεία. Ιδιαίτερα σημαντική επισήμανση αφορά στην περίπτωση των κρυπτογραφημένων ψηφιακών δεδομένων. Έτσι, εάν η κρυπτογράφηση δεδομένων χρησιμοποιείται σε υπολογιστή, συσκευή αποθήκευσης δεδομένων ή άλλη ηλεκτρονική συσκευή και απενεργοποιείται ακατάλληλα κατά τη συλλογή ψηφιακών αποδεικτικών στοιχείων, τα δεδομένα που περιέχει ενδέχεται να μην είναι προσβάσιμα.

Β) Η τεχνική πλευρά της ερευνητικής προσέγγισης.

*αα. Ο έλεγχος της **οθόνης** ηλεκτρονικού υπολογιστή.*

Πολύ συνοπτικά μπορούμε να ακολουθήσουμε την παραδεδεγμένη πρακτική στην συλλογή αποδεικτικού υλικού στην περίπτωση της άντλησης στοιχείων από ηλεκτρονικό υπολογιστή, εφαρμόζοντας τις παραμέτρους μου αναφέρθηκαν σε προηγούμενες θέσεις στην

[332] Ενδεικτική η αναφορά σε σακούλες faraday.

ενότητα αυτήν. Η καταγραφή των ενεργειών που παρατίθεται κατωτέρω ομαδοποιεί δράσεις ώστε να μην δημιουργηθεί μια λεπτομερής μεν αλλά δαιδαλώδης, και λογικά μη εύχρηστη, αναπαραγωγή του πρωτοκόλλου έρευνας.

Έχοντας λοιπόν ο ανακριτικός υπάλληλος απέναντί του μια οθόνη[333] συνδεδεμένη με ηλεκτρονικό υπολογιστή έχει λογικά μια συγκεκριμένη και πρακτικά περιορισμένη συνθήκη πιθανών σεναρίων.

Έστω λοιπόν ότι ο ανακριτικός υπάλληλος εντοπίζει μια οθόνη συνδεμένη σε υπολογιστή. Πρώτη ενδεδειγμένη ενέργεια είναι μια κοντινή φωτογράφιση του αντικειμένου πριν από την οποιαδήποτε περαιτέρω ενέργεια. Η οθόνη αυτή είτε θα είναι ενεργοποιημένη είτε θα είναι απενεργοποιημένη.

Έστω τώρα ότι η οθόνη του ηλεκτρονικού υπολογιστή είναι ενεργοποιημένη κι εμφανίζει ένα πρόγραμμα, μια εφαρμογή, ένα προϊόν εργασίας, μια εικόνα, ένα e-mail ή έναν ιστότοπο Internet. Η λογική και το σχετικό πρωτόκολλο επιβάλλουν την φωτογράφιση της οθόνης και την καταγραφή της επεξηγηματικής πληροφορίας *ενεργός* (active). Αν η ενεργοποίηση της οθόνης αφορά σε μια συνθήκη προφύλαξης οθόνης ή μιας απλής εικόνας, τότε η τεχνική υπόδειξη προτείνει να γίνει μετακίνηση στο ποντίκι ελαφρώς χωρίς να πατηθεί κανένα κουμπί ή να γίνει περιστροφή. Ο ανακριτικός υπάλληλος καλείται να σημειώσει οποιαδήποτε δραστηριότητα στην οθόνη που προκαλεί την αλλαγή της σε οθόνη σύνδεσης, προϊόν εργασίας ή άλλη ορατή οθόνη. Το σχετικό πρωτόκολλο επιβάλλει κι εδώ την φωτογράφιση της οθόνης και την καταγραφή της επεξηγηματικής πληροφορίας *ενεργός* (active). Έστω παραπέρα ότι η οθόνη είναι ενεργοποιημένη πραγματικά, ωστόσο δίνει την αίσθηση ότι είναι «κενή», σα να είναι απενεργοποιημένη. Η τεχνική υπόδειξη προτείνει να γίνει μια πρώτη φωτογράφηση και ακολούθως μετακίνηση στο ποντίκι χωρίς να πατηθεί κανένα κουμπί ή να γίνει περιστροφή. Η οθόνη θα αλλάξει από κενή σε οθόνη σύνδεσης, προϊόν εργασίας ή άλλη ορατή οθόνη. Σημειώνεται η αλλαγή στην οθόνη και ακολουθεί φωτογράφιση της οθόνης και καταγραφή της επεξηγηματικής πληροφορίας *ενεργός* (active).

Στην περίπτωση κατά την οποία η οθόνη είναι απενεργοποιημένη, οπότε η οθόνη είναι κενή. Η τεχνική υπόδειξη προτείνει να γίνει μια πρώτη φωτογράφηση και αρχικό χαρακτηρισμό ως επεξήγηση ***ανενεργός*** (inactive). Ακολούθως εάν ο διακόπτης τροφοδοσίας της οθόνης είναι στη θέση απενεργοποίησης, πρέπει να γίνει ενεργοποίηση της οθόνης. Η οθόνη αλλάζει από κενή οθόνη σε οθόνη σύνδεσης, προϊόν εργασίας ή άλλη ορατή οθόνη.

[333] Θα μπορούσε να είναι και μια οθόνη τηλεόρασης συνδεδεμένη με κατάλληλη σύνδεση με ηλεκτρονικό υπολογιστή.

Σημειώνεται η αλλαγή στην οθόνη και ακολουθεί φωτογράφιση της οθόνης και καταγραφή των πληροφοριών που εμφανίζονται. Με τον τρόπο αυτόν καταδεικνύεται η λειτουργικότητα ή μη της συγκεκριμένης οθόνης.

Στην περίπτωση τώρα κατά την οποία η οθόνη είναι απενεργοποιημένη, οπότε η οθόνη είναι κενή. Η τεχνική υπόδειξη προτείνει να γίνει μια πρώτη φωτογράφηση και αρχικό χαρακτηρισμό ως επεξήγηση ***ανενεργός*** (inactive). Ακολούθως εάν ο διακόπτης τροφοδοσίας της οθόνης είναι στη θέση απενεργοποίησης, πρέπει να γίνει ενεργοποίηση της οθόνης. Έστω ότι η οθόνη δεν αλλάζει και παραμένει κενή. Σημειώνεται ότι δεν εμφανίζεται καμία αλλαγή στην οθόνη και γίνεται νέα φωτογράφηση.

Σε άλλη συνθήκη κατά την οποία η οθόνη είναι ενεργοποιημένη, αλλά η οθόνη είναι κενή. Η τεχνική υπόδειξη προτείνει να γίνει μια πρώτη φωτογράφηση και ακολούθως μετακίνηση στο ποντίκι χωρίς να πατηθεί κανένα κουμπί ή να γίνει περιστροφή με αναμονή για ανταπόκριση. Εάν η οθόνη δεν αλλάξει και η οθόνη παραμείνει κενή, ελέγχεται το στοιχείο του εάν παρέχεται τροφοδοσία στην οθόνη. Εάν η οθόνη παραμείνει κενή, ερευνάται η θέση του υπολογιστή για ενεργά φώτα, λειτουργία στους ανεμιστήρες που περιστρέφονται ή άλλες ενδείξεις ότι ο υπολογιστής είναι ενεργοποιημένος. Εάν η οθόνη παραμείνει κενή και η θήκη του υπολογιστή δεν δείχνει καμία ένδειξη ότι το σύστημα είναι ενεργοποιημένο, τότε αυτός εκτιμάται ***απενεργοποιημένος***.

ββ. Η διαχείριση της μονάδας ηλεκτρονικού υπολογιστή όταν είναι ***απενεργοποιημένος.***

Καταγραφή, φωτογράφιση και σχεδίαση σε σκαρίφημα αναφορικά με όλα τα καλώδια και άλλες συσκευές που είναι συνδεδεμένες στον υπολογιστή. Χωριστή σήμανση (με ειδικές ετικέτες) για το καλώδιο τροφοδοσίας και όλα τα καλώδια (όπου και αν οδηγούν) ή μονάδες USB που είναι συνδεδεμένα στον υπολογιστή, καθώς και την αντίστοιχη σύνδεση που κάθε καλώδιο ή μονάδα USB καταλαμβάνει στον υπολογιστή. Ακολουθεί φωτογράφιση των καλωδίων και των μονάδων USB με τις μοναδικές ειδικές ετικέτες και τις αντίστοιχες συνδέσεις με ετικέτες.

Σε επόμενο στάδιο και αφού εξασφαλίστηκε η απόδοση της εικόνας του υλικού που βρέθηκε στον χώρο, γίνεται η αφαίρεση του καλωδίου τροφοδοσίας από το πίσω μέρος του υπολογιστή και από την παροχή ρεύματος, τη λωρίδα τροφοδοσίας ή τη συσκευή δημιουργίας αντιγράφων ασφαλείας της μπαταρίας. Με όμοια πορεία γίνεται και η

αποσύνδεση και ασφάλιση για όλα τα καλώδια και τις μονάδες USB από τον υπολογιστή και σήμανση της συσκευής ή του εξοπλισμού που είναι συνδεδεμένος στο αντίθετο άκρο. Εφόσον εντοπιστεί κάποια δισκέτα ή συνδεόμενος αποθηκευτικός σχηματισμός, τότε η σχετική σήμανση και περιγραφή διαλαμβάνει και την τοποθέτηση ταινίας. Στον χώρο της υποδοχής της μονάδας για την ανάγνωση δίσκων CD ή DVD, προτείνεται η τοποθέτηση ταινίας και σήμανση επ' αυτής προκειμένου να αποκλειστεί η οποιαδήποτε επέμβαση με άνοιγμα σε άλλο χρόνο ή χώρο. Στην ίδια λογική συστήνεται και η τοποθέτηση ταινίας πάνω από το διακόπτη λειτουργίας.

Καταγραφή του εργοστασίου παραγωγής, του τύπου (μοντέλου), των σειριακών αριθμών αλλά και οποιαδήποτε άλλα σήματα ή αναγνωριστικά που εντοπίζονται και ενδέχεται να αναφέρονται ως δηλωτικά του χρήστη.

Την συσκευασία και εξασφάλιση της ακεραιότητας των υλικών που κατάσχονται και θα απομακρυνθούν, εγγυάται η χρήση των ειδικών υλικών συσκευασίας που αναφέρθηκαν ανωτέρω και τα οποία υλικά αποτρέπουν από την υλική φθορά (θραύση κλπ) σε συνδυασμό με την διατήρηση περιβάλλοντος ουδέτερο από ηλεκτρομαγνητικές μεταβολές.

γγ. Η διαχείριση της μονάδας ηλεκτρονικού υπολογιστή όταν είναι ***ενεργοποιημένος.***

Όπως αναφέρθηκε και σε άλλα σημεία η αλλαγή στην λειτουργία του ηλεκτρονικού υπολογιστή μπορεί να οδηγήσει σε απώλεια σημαντικών πληροφοριών. Στην λογική αυτήν δεν συνιστάται άμεση αποσύνδεση ρεύματος όταν:

- Τα δεδομένα φαινομενικής αποδεικτικής αξίας είναι σε απλή προβολή στην οθόνη. Ο ανακριτικός υπάλληλος πρέπει να αναζητήσει προσωπικό που έχει εμπειρία και εκπαίδευση στη σύλληψη και διατήρηση πτητικών δεδομένων πριν προχωρήσει.
- Υπάρχουν ενδείξεις ότι οποιοδήποτε από τα παρακάτω είναι ενεργό ή χρησιμοποιείται:
- Παιδική πορνογραφία.
- Κατέβασμα αρχείων με παράνομες διαδικασίες (λ.χ. κατά παράβαση της νομοθεσίας για τα πνευματικά δικαιώματα).
- Οικονομικά έγγραφα.
- Σελίδες - Παράθυρα μηνυμάτων
- Κρυπτογράφηση δεδομένων

- Περιοχές (δωμάτια) συνομιλίας (chat rooms).
- Ανοικτά έγγραφα κειμένου.
- Εργασίες σε βάση νεφοϋπολογιστικής με απομακρυσμένη αποθήκευση δεδομένων.
- Άλλες προφανείς παράνομες δραστηριότητες.

Σε μερικές όμως περιπτώσεις η άμεση διακοπή της τροφοδοσίας του αντικειμένου της έρευνας είναι επιβεβλημένη, όπως λ.χ. όταν οι πληροφορίες ή η δραστηριότητα στην οθόνη υποδεικνύουν ότι τα δεδομένα διαγράφονται ή αντικαθίστανται, όταν υπάρχει ένδειξη ότι μια *καταστρεπτική διαδικασία* εκτελείται στις συσκευές αποθήκευσης δεδομένων του υπολογιστή. Στην περίπτωση αυτήν μπορούν να διατηρηθούν πληροφορίες σχετικά με τον τελευταίο χρήστη που θα συνδεθεί και σε ποια στιγμή πραγματοποιήθηκε η σύνδεση, τα έγγραφα που χρησιμοποιήθηκαν πιο πρόσφατα, οι εντολές που χρησιμοποιήθηκαν πιο πρόσφατα και άλλες πολύτιμες πληροφορίες.

Προς την αντίθετη κατεύθυνση λειτουργεί και η παραδοχή της επιστημονικής κοινότητας ότι σε ορισμένες περιστάσεις, μπορεί να είναι απαραίτητο ή σκόπιμο οι εγκληματολόγοι ερευνητές να συλλέγουν αποδεικτικά στοιχεία από έναν υπολογιστή ενώ βρίσκεται σε λειτουργία ή σε «ζωντανή» κατάσταση. Αυτή η τεχνική τείνει να γίνει μια κοινή πρακτική καθώς, παρόλο που θα γίνουν κάποιες αλλαγές στα αρχικά αποδεικτικά στοιχεία, αυτή η μέθοδος επιτρέπει συχνά την πρόσβαση σε αποδεικτικά στοιχεία *τα οποία δεν θα ήταν διαθέσιμα εάν η ισχύς αφαιρεθεί από ένα σύστημα*. Για να καταγραφούν πτητικά ψηφιακά δεδομένα σε μια συσκευή, θα πρέπει να υπάρχει η πρόσβαση στη συσκευή. Ως εκ τούτου, οι αλλαγές θα προκληθούν από τον εξεταστή. Ιδιαίτερη προσοχή πρέπει να δοθεί στην αρχή της ακεραιότητας[334], αναφορικά με τις κατευθυντήριες γραμμές, καθώς η διεξαγωγή ζωντανής ψηφιακής πραγματογνωμοσύνης συνεπάγεται πρόσβαση στα αρχικά αποδεικτικά στοιχεία. Κάθε άτομο που το κάνει αυτό πρέπει να είναι ικανό και να έχει πλήρη επίγνωση του αντίκτυπου που έχουν οι ενέργειές του και πρέπει να είναι έτοιμο να εξηγήσει τους λόγους για τους οποίους ακολουθεί αυτή την επιλογή και φυσικά να μπορεί να την τεκμηριώσει τεχνικά στα πλαίσια της αναγκαιότητας, ως νομιμοποιητική βάση της καθώς και στην τεχνική της διάσταση.

[334] Βλ. ανωτέρω υπό 9. Οι Αρχές που Διέπουν την Έρευνα αναφορικά με τα Ψηφιακά Πειστήρια και τα Ψηφιακά Δεδομένα, *ii. Οι Αρχές που διέπουν την ανακριτική έρευνα ως ερευνητική, προσέγγιση της μελέτης, Β) η αρχή της ακεραιότητας (integrity)*, σελ. 160 επ.

δδ. Η διαχείριση των περιφερειακών συστημάτων που εντοπίστηκαν στον χώρο.

Ηλεκτρονικές συσκευές όπως αυτές που αναφέρονται αμέσως παρακάτω ενδέχεται επίσης να περιέχουν πληροφορίες αποδεικτικής αξίας για μια έρευνα. Εκτός από καταστάσεις έκτακτης ανάγκης, τέτοιες συσκευές δεν πρέπει να λειτουργούν και οι πληροφορίες που ενδέχεται να περιέχουν δεν πρέπει να είναι εκτεθειμένες σε άμεση πρόσβαση. Εάν μια συνθήκη που πρέπει να τύχει διαχείρισης δικαιολογεί την άμεση πρόσβαση σε αυτές τις συσκευές και τις πληροφορίες που περιέχουν, όλες οι σχετικές ενέργειες του ερευνητή που πρέπει να ληφθούν, πρέπει να εξηγούνται και να τεκμηριώνονται διεξοδικά. Τα δεδομένα ενδέχεται να χαθούν εάν δεν γίνεται σωστή διαχείριση της συσκευής ή η σωστή πρόσβαση στα δεδομένα της.

Τέτοια παραδείγματα ηλεκτρονικών συσκευών, εξαρτημάτων και περιφερειακών που ενδέχεται να εμπεριέχουν ψηφιακά δεδομένα, χρήσιμα για την έρευνα εντοπίζονται σε συσκευές εγγραφής ήχου, αξεσουάρ GPS, αυτόματους τηλεφωνητές, τσιπ υπολογιστή, ασύρματα σταθερά τηλέφωνα, μηχανές αντιγραφής, κινητά τηλέφωνα, αντιγραφείς σκληρού δίσκου, τηλεομοιοτυπικά μηχανήματα (φαξ), εκτυπωτές, πολυλειτουργικά μηχανήματα (εκτυπωτής, σαρωτής, φωτοαντιγραφικό και φαξ), ασύρματα σημεία πρόσβασης, τροφοδοτικά και αξεσουάρ φορητού υπολογιστή, έξυπνες κάρτες, συσκευές εγγραφής βιντεοκασετών (VCR), σαρωτές, μονάδες αναγνώρισης τηλεφώνου, προσωπικοί ψηφιακοί οδηγοί ή υπολογιστές (personal digital assistant - PDA).

εε. Άλλο αποδεικτικό υλικό σχετιζόμενο.

Πέρα από τα αναμενόμενα στοιχεία σε έναν χώρο ηλεκτρονικού εγκλήματος, είναι απαραίτητη η προσεκτική έρευνα στο περιβάλλον της σκηνής με αναζήτηση που αφορά σε λοιπά στοιχεία που μπορεί να συνδέονται με το έγκλημα, όπως λ.χ. σημειώσεις (ακόμη και πρόχειρες καταγραφές σε αποκόμματα χαρτιού) με πιθανούς κωδικούς πρόσβασης, λοιπές χειρόγραφες σημειώσεις, κενά χαρτιά με εντυπώσεις από προηγούμενα κείμενα (όπου η πίεση από την γραφίδα στην επάνω σελίδα, που λείπει, αναδεικνύουν το μήνυμα που γράφηκε), εγχειρίδια υλικού και λογισμικού, ημερολόγια, βιβλιογραφία και κείμενο ή γραφικό υλικό που εκτυπώθηκε από τον υπολογιστή και μπορεί να αποκαλύψει πληροφορίες σχετικές με την έρευνα. Αυτές οι μορφές αποδεικτικών στοιχείων θα πρέπει επίσης να τεκμηριώνονται και να διατηρούνται σύμφωνα με τη λογική της εξασφάλισης από αλλοιώσεις (φυσικά όχι του προηγουμένου επιπέδου).

στ.στ. Μεταφορά και αποθήκευση των κατασχεθέντων.

Αφού εντοπιστούν τα ψηφιακά πειστήρια, φωτογραφηθούν στον χώρο και συσκευαστούν με ασφάλεια από κινδύνους φθοράς και αλλοίωσης, ιδίως του ψηφιακού περιεχομένου των δεδομένων τους, υπάρχει και πάλι ενδιαφέρον για τον τρόπο μεταφοράς, ανάλογο με εκείνο της εξασφάλισης των δεδομένων μακριά από κινδύνους αλλοίωσης, στο έδαφος της μεταφοράς. Έτσι τα ψηφιακά στοιχεία πρέπει να διατηρούνται, ακόμη και μετά την προσεκτική και ασφαλή συσκευασία τους, μακριά από μαγνητικά πεδία, όπως αυτά που παράγονται από ραδιοπομπούς, μαγνήτες ηχείων κλπ. Κάθε συσκευή ή υλικό, το οποίο που μπορεί να παράγει στατικό ηλεκτρισμό ή να φέρει μαγνητικά φορτία, πρέπει να αποφεύγεται να βρίσκεται στο περιβάλλον της μεταφοράς.

Σημαντική παράμετρος είναι και η μείωση των κραδασμών κατά την μεταφορά, όταν οι κραδασμοί αυτοί μεταφέρονται στο εσωτερικό των συσκευασιών, όπου βρίσκεται το κατασχεθέν υλικό. Μια άλλη παράμετρος είναι η υγρασία και η θέρμανση. Η παραμονή των ψηφιακών στοιχείων υπό συνθήκες μεταφοράς εκτεθειμένες στην έντονη θερμότητα, ή το έντονο ψύχος καθώς και η υγρασία μπορούν να αλλοιώσουν ή να καταστρέψουν τα ψηφιακά στοιχεία.

Κατά την αποθήκευση ψηφιακών στοιχείων, ο ανακριτικός υπάλληλος έχει πανομοιότυπες αγωνίες, με εκείνες που αφορούν την μεταφορά των στοιχείων και για τον λόγο αυτόν, ό,τι αναφέρθηκε ανωτέρω διατηρεί την ισχύ του κι εδώ. Μιλώντας όμως για ψηφιακά στοιχεία μια σημαντική παράμετρος είναι η ενεργειακή φροντίδα τους όσο παραμένουν αποθηκευμένα. Τούτο διότι ενδεχομένως πολύτιμα ψηφιακά στοιχεία, συμπεριλαμβανομένων ημερομηνιών, ωρών και ρυθμίσεων διαμόρφωσης συστήματος, να χαθούν λόγω παρατεταμένης αποθήκευσης, εάν μειωθούν τα φορτία από τις μπαταρίες ή η πηγή τροφοδοσίας που διατηρεί αυτές τις πληροφορίες.

Εάν έχει κατασχεθεί σύστημα περισσοτέρων ηλεκτρονικών υπολογιστών τότε όλοι οι υπολογιστές, τα καλώδια και οι συσκευές που είναι συνδεδεμένες σε αυτά πρέπει να φέρουν κατάλληλη ετικέτα για να διευκολύνεται η επανασυναρμολόγηση, εάν είναι απαραίτητο. Στη συνέχεια, οι κατασχεθέντες υπολογιστές μπορούν να επισημανθούν με αλφαβητική σειρά. Οι αντίστοιχες συνδέσεις και καλώδια μπορούν να επισημανθούν με την ονομασία γραμμάτων

για τον υπολογιστή και έναν μοναδικό αριθμό για να εξασφαλιστεί η σωστή επανασυναρμολόγηση[335].

vi. Η εργαστηριακή εξαγωγή των ψηφιακών δεδομένων - Λογισμικά ανάλυσης

Η αξιοποίηση των κατασχεμένων ψηφιακών πειστηρίων γίνεται στο περιβάλλον εργασίας του ερευνητή – ανακριτικού υπαλλήλου, αφού βεβαίως τηρούνται όλες οι προϋποθέσεις εξασφάλισης της ακεραιότητας του υλικού αντικειμένου που δεσμεύθηκε. Πρόκειται για το στάδιο εκείνο που το κατασχεθέν υλικό παραδίδεται στον ερευνητή του τμήματος ψηφιακών πειστηρίων, για την εξόρυξη δεδομένων.

Βασική αρχή για την εξασφάλιση της ακεραιότητας του κατασχεθέντος ψηφιακού πειστηρίου είναι η δημιουργία αντιγράφου του. Όπως διεξοδικά αναφέρθηκε και σχετικά αναπτύχθηκε ανωτέρω[336], σύμφωνα και με την νεοπαγή διάταξη του Κ.Ποιν.Δ. (αρ. 265 § 4 εδ. β) κατά την κατάσχεση των ψηφιακών στοιχείων σχηματίζεται ασφαλές αντίγραφο ενός εκάστου πειστηρίου ώστε να διασφαλίζεται η δυνατότητα ανάκτησης των δεδομένων που έχουν κατασχεθεί, σε περίπτωση απώλειας ή καταστροφής, το οποίο φυλάσσεται 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.

Έτσι λοιπόν αφού τα υλικά μέσα – φορείς των ψηφιακών δεδομένων αυτά συλλεχθούν, δημιουργείται τεχνικά ένα ακριβές αντίγραφο τους (forensic duplicate) με κατάλληλα εργαλεία υλικού και λογισμικού. Συνήθως χρησιμοποιείται μία συσκευή write-blocking η οποία αποτρέπει τυχόν τροποποιήσεις στα αρχικά δεδομένα. Η διαδικασία αυτή συχνά ονομάζεται και imaging. Να σημειωθεί ότι μέσα στους σκοπούς της πρακτικής αυτής της αντιγραφής είναι η οποιαδήποτε εξέταση να επιχειρείται επί του αντιγράφου και όχι επί του πρωτότυπου πειστηρίου, έτσι ώστε να αποφευχθεί οποιαδήποτε μεταβολή στα αυθεντικά ψηφιακά δεδομένα, η οποία θα καθιστούσε την όλη έρευνα αναξιόπιστη ώστε να σταθεί ως αποδεικτικό στοιχείο σε μια δικαστική διαμάχη.

---

[335] Βλ. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, «Electronic Crime Scene Investigation, A Guide for First Responders, Second Edition», https://www.ncjrs.gov/pdffiles1/nij/219941.pdf σελ. 46.

[336] Βλ. ανωτέρω υπό 8. Η Κατάσχεση των Ψηφιακών Δεδομένων (κατ' άρθρο 265 Κ.Ποιν.Δ.), *ix. Το αντίγραφο των κατασχεθέντων ψηφιακών δεδομένων και η φύλαξη των ψηφιακών πειστηρίων*, σελ. 132 επ.

Στη συνέχεια, το αρχικό ψηφιακό μέσο τοποθετείται σε ένα ασφαλές μέρος ώστε να αποφευχθούν αλλοιώσεις. Τέλος, για το αποκτηθέν αντίγραφο καθώς και για το αρχικό ψηφιακό μέσο, πρέπει να υπολογιστεί μία κρυπτογραφική σύνοψη[337] (με χρήση για παράδειγμα των συναρτήσεων MD5, SHA-1 και SHA-256). Οι δύο τιμές που θα προκύψουν συγκρίνονται ώστε να πιστοποιηθεί ότι το αντίγραφο είναι ακριβές. Σε κρίσιμα σημεία της ανάλυσης, υπολογίζεται πάλι η σύνοψη του ψηφιακού μέσου έτσι ώστε να επιβεβαιωθεί ότι τα δεδομένα δεν έχουν υποστεί αλλοιώσεις.

Άλλες τεχνικές που ενδέχεται να χρησιμοποιήσει ο ανακριτικός υπάλληλος, ειδικός ερευνητής είναι η ανάκτηση δεδομένων, η ανάλυση μνήμης, η χρονική ανάλυση, η ανάλυση συστήματος, η ανάλυση αρχείων[338].

[337] Το MD5 & SHA-1 Checksum Utility της Raymond Lin είναι ένα αυτόνομο δωρεάν λογισμικό που δημιουργεί και επαληθεύει κρυπτογραφικές κατακερματισμούς σε MD5 και SHA-1. Οι κρυπτογραφικές λειτουργίες κατακερματισμού χρησιμοποιούνται συνήθως για την προστασία από κακόβουλες αλλαγές σε προστατευμένα δεδομένα σε μια μεγάλη ποικιλία λογισμικού, διαδικτύου και εφαρμογών ασφαλείας, συμπεριλαμβανομένων των ψηφιακών υπογραφών και άλλων μορφών ελέγχου ταυτότητας. Δύο από τις πιο κοινές συναρτήσεις κρυπτογραφικού κατακερματισμού είναι ο αλγόριθμος Secure Hash (SHA) και ο αλγόριθμος Μηνύματος Digest. Τα βοηθητικά προγράμματα Checksum χρησιμοποιούνται για την επαλήθευση της ακεραιότητας των παραγόμενων κατακερματισμών. Υπάρχουν δύο βασικοί τύποι, εκείνοι που υπολογίζουν τις τιμές αθροίσματος ελέγχου και εκείνοι που τους επικυρώνουν επίσης ελέγχοντάς τους με μια λίστα τιμών για τα προστατευμένα δεδομένα, που είναι ο μόνος τρόπος που μπορεί να γίνει. https://download.cnet.com/MD5-SHA-Checksum-Utility/3000-2092_4-10911445.html

[338] Οι σχετικές ενέργειες και ο σκοπός της αναλυτικής αυτής διείσδυσης αναφέρθηκε ανωτέρω υπό

11. ΚΑΤΑΣΧΕΣΗ ΨΗΦΙΑΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΔΙΚΑΙΩΜΑΤΑ ΚΑΤΗΓΟΡΟΥΜΕΝΟΥ ΥΠΟ ΤΟ ΦΩΣ ΤΩΝ ΕΓΓΥΗΣΕΩΝ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΑΤΟΜΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΚΑΙ ΤΗΣ ΝΟΜΟΛΟΓΙΑΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΔΙΚΑΣΤΗΡΙΟΥ ΔΙΚΑΙΩΜΑΤΩΝ του ΑΝΘΡΩΠΟΥ (ΕΔΔΑ)

Αναπτύχθηκε στις προηγούμενες ενότητες η διαδικασία της κατάσχεσης των ψηφιακών στοιχείων (υλικών φορέων και δεδομένων) ενταγμένη στο δικονομικό στάδιο της προδικασίας, στο οποίο λειτουργεί ως παράγοντας εμπλουτισμού του αποδεικτικού υλικού.

Κατά την παρουσίαση των σπονδυλωτών δομών της διαχείρισης της ειδικής μορφής αυτής κατάσχεσης, δεν ήταν λίγες οι φορές, που την τεχνοκρατική ροή της ανάπτυξης του λόγου, την διέκοπτε λογικά η όποια αναζήτηση ή ένσταση αναφορικά με την συσχέτιση της ερευνώμενης εργασίας με τα δικαιώματα του ατόμου, άλλως η σύγκρουση των ειδικών απαιτήσεων της έρευνας στον ψηφιακό κόσμο από τη μια, με τα δικαιώματα του κατηγορουμένου ή υπόπτου, από την άλλη.

Κατά την καταγραφή των σχετικών δικαιωμάτων στο τμήμα του Κ.Ποιν.Δ., που αναφέρεται στην προδικασία, στα άρθρα 89 επ., αναφέρονται ο διορισμός (και αριθμός) συνηγόρων (αρ. 89 και 99)[339], το δικαίωμα παροχής δωρεάν νομικής βοήθειας (αρ. 91), το δικαίωμα να απευθύνει, ο ίδιος ή ο συνήγορός του, ερωτήσεις (αρ. 94), το δικαίωμα σε ενημέρωση αναφορικά με όλα τα δικαιώματά του (αρ. 95), το δικαίωμα ενημέρωσης προσώπου της επιλογής του κατηγορουμένου σε περίπτωση στέρησης της ελευθερίας (αρ. 97)[340], το δικαίωμα επικοινωνίας με τρίτα πρόσωπα κατά τη διάρκεια της στέρησης της ελευθερίας (αρ. 98), το δικαίωμα πρόσβασης στο υλικό της δικογραφίας (αρ. 100)[341], το δικαίωμα διερμηνείας και μετάφρασης (αρ. 101), το δικαίωμα αίτησης διεξαγωγής αποδείξεων (αρ. 102), το δικαίωμα για λήψη προθεσμίας για την απολογία (αρ. 103), το δικαίωμα σιωπής και μη αυτοενοχοποίησης (αρ. 104).

[339] Βλ. ενδεικτικά *Γ. Νούσκαλης*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, τομ Ι, 2η εκδοση, Νομική Βιβλιοθήκη, 2018, σελ. 530 επ. με την εκεί πλούσια παραπομπή στην θεωρία.
[340] Βλ. αρ, 50 Ν 4478/2017,με το οποίο έγινε ενσωμάτωση της Οδηγίας 2013/48/ΕΕ.
[341] Βλ. ενδεικτικά, *Λ. Μαργαρίτης*, Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου και Ελληνική Ποινική Δίκη, σε «Εμβάθυνση στην Ποινική Δικονομία», τ. Ι, 2006, σελ. 3, *Αργ. Καρράς*, Η υποχρέωση έγγραφης και λεπτομερούς ανακοίνωση της κατηγορίας στον κατηγορούμενο, ΠοινΧρον 2000, σελ. 673.

Τονίζεται ότι τα σχετικά δικαιώματα του κατηγορουμένου, τυγχάνουν και κατοχύρωσης σε νομοθετήματα αυξημένης τυπικής ισχύος[342], όπως είναι η ΕΣΔΑ[343], το αρ. 2 § 1 του 7ου Πρωτοκόλλου της ΕΣΔΑ[344], αλλά και το Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα του ΟΗΕ[345]. Ενταγμένα μέσα στη γενικότερη μέριμνα για κατοχύρωση του δικαιώματος σε δίκαιη δίκη κατ' αρ. 6 της ΕΣΔΑ, τα δικαιώματα του κατηγορουμένου, υφίστανται, ακόμη και αν δεν υπήρχαν οι ρητές προβλέψεις του Κ.Ποιν.Δ. Τούτο στην βάση της αυξημένης τυπικής ισχύος και άρα της νομοθετικής υπεροχής της συγκεκριμένης πρόβλεψης κατ' αρ. 28 § 1 Συντ[346].

Συνεπώς τόσο η ΕΣΔΑ όσο και το ίδιο το Σύνταγμα με τις διατάξεις αναφορικά με τις ατομικές ελευθερίες, καθορίζουν ένα ρυθμιστικό πεδίο προστασίας για τον κατηγορούμενο, το οποίο πρέπει να τυγχάνει σεβασμού και να λαμβάνεται υπόψη σε κάθε περίπτωση που επιλέγεται μέτρο καταναγκασμού, όπως είναι και η περίπτωση της κατάσχεσης των ψηφιακών δεδομένων και των υλικών φορέων τους, που αντιμετωπίζεται ως κυρία θεματική στην μελέτη αυτήν. Μάλιστα ερμηνευτικές λύσεις δίνουν και οι αναγωγές στις ατομικές ελευθερίες, ακόμη και χωρίς αναγκαστική προσφυγή στην τριτενέργεια των σχετικών συνταγματικών δικαιωμάτων.

Αναφορικά με την καταγραφή των δικαιωμάτων του κατηγορουμένου, τόσο ειδικά αναφορικά με το πρόσωπό του, όσο και ενταγμένα στα γενικότερα δικαιώματα των διαδίκων (στους οποίους σαφώς εντάσσεται και αυτός), αυτά αφορούν στο σύνολο των ποινικών υποθέσεων που μπορεί να απασχολήσουν το ποινικό δικαστήριο και την εισαγγελική αρχή. Ειδικότερες αναφορές και δικαιώματα δεν διατυπώνονται στον Κώδικα. Όπως όμως προέκυψε από τις καταγραφές σε διάφορα σημεία της μελέτης, η κατάσχεση των ψηφιακών δεδομένων δημιουργεί ειδικότερες συνθήκες, που σε συγκεκριμένες περιπτώσεις, όπως η περίπτωση της πρόσβασης του κατηγορουμένου στο ψηφιακό αντίγραφο (digital copy) που ενσωματώνεται στην ποινική δικογραφία, δεν φαίνεται να έχουν λύση, τουλάχιστον ξεκάθαρη. Πρόκειται για το ερώτημα που απασχόλησε στην ειδική αναφορά του άρ. 265 § 5 σχετικά με την περιοριστική αρίθμηση των προσώπων που έχουν δικαίωμα πρόσβασης στο

[342] Βλ. ενδεικτικά, *Δ. Ζημιανίτης*, Το πράσινο βιβλίο της Ευρωπαϊκής Επιτροπής για «τις δικονομικές εγγυήσεις υπέρ υπόπτων και κατηγορουμένων σε ποινικές διαδικασίες σε ολόκληρη την ΕΕ», ΠοινΔικ 2003, σελ. 443 επ.
[343] Βλ. *Θ. Δαλακούρας*, Ο νέος Κώδικας Ποινικής Δικονομίας, συνοπτική ερμηνεία κατ' αρ. Ν 4620/2019, εκδ. β, ΝομΒιβλ, σελ. 84.
[344] Που κυρώθηκε με το Ν 1705/1987.
[345] Που κυρώθηκε με το αρ. 14 § 3 Ν 2462/1997
[346] Από την κύρωσή της ΝΔ 53/1974.

ψηφιακό αντίγραφο (digital copy) καθώς και για την αναφορά στην ρητή απαγόρευση δημιουργίας αντιγράφου της § 6[347].

Η ιδιαίτερη αναφορά στα δικαιώματα του κατηγορουμένου, δεν γίνεται μόνο στη βάση της σημειολογίας τους ως ατομικά δικαιώματα, αλλά σε μια δικονομική διάσταση της καταγραφής, δίδεται η απαραίτητη προσοχή και σημασία, που ο ίδιος ο νομοθέτης έχει δώσει σε αυτά, συμμορφούμενος σε όλες τις ανωτέρω νομοθετικές δεσμεύσεις και απόδειξη αυτού αποτελεί η περιχαράκωση της υποχρέωσης για τον σεβασμό των δικαιωμάτων αυτών, με αυστηρές δικονομικές κυρώσεις στην περίπτωση που δεν προστατευθούν. Αναφέρομαι στην ανωτάτη δικονομική κύρωση της απόλυτης ακυρότητας του αρ. 171 § 1 περ. δ Κ.Ποιν.Δ.[348]. Ο σεβασμός λοιπόν των δικαιωμάτων του κατηγορουμένου, σε όλα τα διαδικαστικά στάδια της ποινικής δίκης και συνεπώς και σε αυτό της προδικασίας, που μας απασχολεί, ενισχύεται με την απειλή της δικονομικής κύρωσης της ρήτρας[349] των *απολύτων ακυροτήτων* στην περίπτωση που προσβληθούν τα δικαιώματα αυτά. Μάλιστα η ομολογουμένως πιο ξεκάθαρη[350] διαμόρφωση της *ρήτρας* των απολύτων ακυροτήτων και ειδικότερα εκείνης της προστασίας των υπερασπιστικών δικαιωμάτων του κατηγορουμένου,

Στην θεματική αυτή της συσχέτισης με τα δικαιώματα του κατηγορουμένου, πρέπει να ελεγχθεί η διάταξη του άρθρου 265 § 5 Κ.Ποιν.Δ. η οποία κατά την διατύπωσή της καθορίζει περιοριστικά τον αριθμό των προσώπων που νομιμοποιούνται να έχουν πρόσβαση στο ψηφιακό αντίγραφο (digital copy). Η διατύπωση λοιπόν ότι «*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 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*

[347] Βλ. ανωτέρω υπό 8. Η Κατάσχεση των Ψηφιακών Δεδομένων (κατ' άρθρο 265 Κ.Ποιν.Δ.), *ix. Το αντίγραφο των κατασχεθέντων ψηφιακών δεδομένων και η φύλαξη των ψηφιακών πειστηρίων,* σελ. 132 επ.

[348] Αρ. 171 § 1 «*Απόλυτη ακυρότητα υπάρχει: 1. Αν δεν τηρηθούν οι διατάξεις που καθορίζουν: α) ……, β) ……, γ) ……, δ) την εμφάνιση, την εκπροσώπηση και την υπεράσπιση του κατηγορουμένου ή του προσώπου στο οποίο αποδίδεται η πράξη κατά την προκαταρκτική εξέταση και την άσκηση των δικαιωμάτων που τους παρέχονται από το νόμο, την Ευρωπαϊκή Σύμβαση για την προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών, το Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα και τον Χάρτη Θεμελιωδών Ελευθεριών της Ε.Ε. 2. Αν ο κατηγορούμενος ζήτησε να ασκήσει δικαίωμα που του παρέχεται από τον νόμο και το δικαστήριο του το αρνήθηκε ή παρέλειψε να αποφανθεί για την σχετική αίτηση. 3. Αν ο υποστηρίζων την κατηγορία παρέστη παράνομα στην διαδικασία του ακροατηρίου.*»

[349] Βλ. *Θ. Δαλακούρας*, Οι ακυρότητες στο ποινικοδικονομικό μας σύστημα, σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη 2019, σελ. 29.

[350] Στην προηγούμενη εκδοχή του Κ.Ποιν.Δ. υπήρχε μια σχετική σύγχυση με την αναφορά της απαγόρευσης άσκησης των δικαιωμάτων του κατηγορουμένου τόσο στις σχετικές ακυρότητες όσο και στις απόλυτες.

αποθηκευμένα. Η παρούσα ισχύει αναλόγως και τα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία.» εγείρει ερωτήματα.

Το *επιτρέπεται μόνο*, που χρησιμοποίησε ο νομοθέτης προφανώς και δεν φαίνεται να επιδέχεται ερμηνευτικής προσέγγισης πέραν της γραμματικής καθόσον δεν καταλείπεται αμφιβολία αναφορικά με την επιλογή και την βούληση του νομοθέτη, να προστατεύσει το κρίσιμο, μάλλον κεντρικό και ίσως μοναδικό, αποδεικτικό στοιχείο, το οποίο στηρίζει την αποδιδομένη κατηγορία. Και η διατύπωση είναι σαφής καθόσον στον κατάλογο των προσώπων που επιτρέπεται να έχουν πρόσβαση στο ψηφιακό αντίγραφο, μνημονεύονται μόνον εκείνοι που ασκούν δικαστικά, εισαγγελικά και ανακριτικά καθήκοντα στην υπόθεση ή οι γραμματείς τους.

Στις προσεγγίσεις της προβληματικής αυτής, πρέπει να συνυπολογιστεί και η άποψη, που επικράτησε στη θεωρία[351] αναφορικά με τις ακυρότητες και δη τις απόλυτες που σχετίζονται με την προστασία των δικαιωμάτων του κατηγορουμένου, ότι η προστασία των υπερασπιστικών δικαιωμάτων του κατηγορουμένου, τυγχάνει τέτοιας προσοχής ώστε ο δικαστής να έχει την υποχρέωση να εξασφαλίζει όλες εκείνες τις προϋποθέσεις που καθιστούν δυνατή την άσκηση των δικαιωμάτων του κατηγορουμένου, ακόμη και χωρίς την υποβολή σχετικής αίτησης από τον τελευταίο[352].

Σταθερά η συγκρουσιακή σχέση παραμένει μεταξύ δύο πόλων. Της αξίωσης για δημόσια ασφάλεια και πρόληψη του εγκλήματος από τη μια και της προστασίας των ατομικών ελευθεριών, τουλάχιστον στο επίπεδο του σκληρού πυρήνα τους.

1. Μια πρώτη συνθήκη που μας απασχολεί είναι η περίπτωση της προληπτικής κατάσχεσης, άλλως οι περιπτώσεις εκείνες όπου η μετέπειτα δίωξη στηρίχθηκε σε αξιοποίηση μη νόμιμης ή μη νομιμοποιημένης αστυνομικής δράσης.

Κρίσιμη από την πρόσφατη διεθνή και θεσμικά υψηλού επιπέδου, από πλευράς διαβάθμισης, νομολογία, είναι η απόφαση του ΕΔΔΑ αναφορικά με την έλλειψη των προϋποθέσεων νόμιμης έρευνας που οδηγεί στην κατάσχεση ψηφιακών δεδομένων, στην υπόθεση *Trabajo Rueda κατά Ισπανίας* της 30-5-2017 (αριθμ. προσφ. 32600/12)[353]. Ο προσφεύγων, Carlos Trabajo Rueda, είναι Ισπανός υπήκοος, ο οποίος γεννήθηκε το 1976 και

[351] Βλ. *Ν. Ανδρουλάκης*, Θεμελιώσεις έννοιες της ποινικής δίκης, 2007, σελ. 522, *Αργ. Καρράς*, Η αρχή της δικαστικής ακρόασης, 1989, σελ. 320 επ.
[352] Έτσι και η *Π. Παπανδρέου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, τομ Ι, 2η έκδοση, Νομική Βιβλιοθήκη, 2018, σελ. 989.
[353] Βλ. Trabajo Rueda κατά Ισπανίας της 30-5-2017 (αριθμ. προσφ. 32600/12), https://hudoc.echr.coe.int/eng #{%22itemid%22:[%22001-173787%22]}

ζει στη Σεβίλλη (Ισπανία). Στις 17.12.2007 ο κ. Trabajo Rueda πήγε τον υπολογιστή του σε κατάστημα ηλεκτρονικών υπολογιστών για να αντικαταστήσει έναν ελαττωματικό καταγραφέα δεδομένων. Ο τεχνικός αντικατέστησε σωστά το εν λόγω εξάρτημα και το δοκίμασε ανοίγοντας ορισμένα αρχεία, οπότε και παρατήρησε ότι περιείχαν υλικό παιδικής πορνογραφίας. Στις 18.12.2007 ανέφερε τα γεγονότα στις αρχές και παρέδωσε τον υπολογιστή στις αστυνομικές αρχές, οι οποίες δέσμευσαν και εξέτασαν το περιεχόμενό του και τον διαβίβασαν στους εμπειρογνώμονες της αστυνομίας. Ο δικαστής ενημερώθηκε σχετικά με τις τρέχουσες αστυνομικές έρευνες. Στις 20.12.2007 ο προσφεύγων συνελήφθη στο δρόμο προς το ηλεκτρονικό κατάστημα για να παραλάβει τον υπολογιστή του. Τον Μάιο του 2008 καταδικάστηκε σε φυλάκιση τεσσάρων ετών από το Δικαστήριο της Σεβίλλης για κατοχή και κυκλοφορία πορνογραφικών εικόνων ανηλίκων. Ο κ. Trabajo Rueda υπέβαλε ένσταση στο δικαστήριο για να κηρύξει τα αποδεικτικά στοιχεία άκυρα με το σκεπτικό ότι είχε παραβιαστεί το δικαίωμα σεβασμού της *ιδιωτικής του ζωής* καθώς και ότι οι αστυνομικές αρχές είχαν πρόσβαση στο περιεχόμενο και στα αρχεία του υπολογιστή του, αλλά το αίτημά του απορρίφθηκε. Ο προσφεύγων άσκησε όλα τα ένδικα μέσα αλλά απορρίφθηκαν αμετάκλητα. Αρχικά, το ΕΔΔΑ έκρινε ότι η πρόσβαση σε αρχεία στον προσωπικό υπολογιστή του κ. Trabajo Rueda και στη συνέχεια, η καταδίκη του, ισοδυναμούσε με παρέμβαση των αρχών στο δικαίωμα <u>σεβασμού της ιδιωτικής ζωής</u> του προσφεύγοντος, επισημαίνοντας ότι η παρέμβαση αυτή κατοχυρώνετο και στο εσωτερικό δίκαιο, δηλαδή από τα νομικά κείμενα σε συνδυασμό με την ερμηνευτική νομολογία του Συνταγματικού Δικαστηρίου, το οποίο θέσπισε τον κανόνα σύμφωνα με τον οποίο απαιτείται *προηγούμενη δικαστική εξουσιοδότηση*[354] σε περίπτωση που η ιδιωτική ζωή ενός ατόμου πιθανόν θα παραβιαστεί, εξαιρουμένου των καταστάσεων έκτακτης ανάγκης, οπότε απαιτείται μεταγενέστερος δικαστικός έλεγχος.

Δεύτερον, το Δικαστήριο σημείωσε ότι η επίμαχη παρέμβαση είχε επιδιώξει τον θεμιτό σκοπό της «πρόληψης του εγκλήματος» και της «προστασίας των δικαιωμάτων τρίτων», υπογραμμίζοντας ότι «η σεξουαλική κακοποίηση είναι αναμφισβήτητα ένα απεχθές είδος αδικίας, με εξουθενωτικές επιπτώσεις στα θύματά του» και ότι «τα παιδιά και τα υπόλοιπα ευάλωτα άτομα έχουν δικαίωμα στην προστασία του κράτους, με τη μορφή της αποτελεσματικής αποτροπής, από τέτοιους σοβαρούς τύπους παρεμβολών σε βασικές πτυχές της ιδιωτικής τους ζωής».

[354] Σε αντιστοιχία με το Ν 2225/1994 του Ελληνικού Δικαίου.

Τρίτον, το Στρασβούργο διαπίστωσε ότι η κατάσχεση και η επιθεώρηση όλων των αρχείων ηλεκτρονικού υπολογιστή από την αστυνομία στη προκειμένη περίπτωση, ήταν *δυσανάλογη* προς τους επιδιωκόμενους νόμιμους σκοπούς και δεν ήταν επομένως «απαραίτητη σε μια δημοκρατική κοινωνία». Το Δικαστήριο επεσήμανε ότι ήταν δύσκολο στη προκειμένη περίπτωση, να εκτιμήσει τον επείγοντα χαρακτήρα της κατάστασης όπου απαιτεί από την αστυνομία να συλλέξει τα αρχεία από τον προσωπικό υπολογιστή του κ. Trabajo Rueda και να αποκτήσει πρόσβαση στο περιεχόμενό τους, παρακάμπτοντας την προϋπόθεση του προηγούμενου εντάλματος έρευνας. Επομένως, το Δικαστήριο δεν κατάλαβε γιατί η αναμονή για ένα σχετικά σύντομο χρονικό διάστημα, έως ότου να εξασφαλίσει προηγούμενη δικαστική εξουσιοδότηση πριν ελεγχθεί ο υπολογιστής του κ. Trabajo Rueda, θα εμπόδιζε την αστυνομική έρευνα ως προς τα προσβληθέντα γεγονότα. Κατά συνέπεια, το Δικαστήριο διαπίστωσε παραβίαση του άρθρου 8 της Σύμβασης.

2. Σχετικοί προβληματισμοί αναφορικά με την επιλογή στα μέτρα δικονομικού καταναγκασμού, συνδυασμένα με τις κρατικές επιλογές αναφορικά με την πρόληψη εγκληματικής δράσης, απασχόλησαν το ΕΔΔΑ, στην βάση της αναλογικότητας και της επιλογής ανάμεσα σε ηπιότερα μέτρα. Στην υπόθεση *Apostolovi κατά Βουλγαρίας* της 07.11.2019 (αριθ. προσφ. 32644/09)[355], το ΕΔΔΑ καθόρισε τα κριτήρια αναφορικά με την έκταση των μέτρων δικονομικού καταναγκασμού σε σχέση με το ατομικό δικαίωμα του κατηγορουμένου στην περιουσία του.

Στην περίπτωση εκείνη, οι προσφεύγοντες υπέστησαν δέσμευση όλων των περιουσιακών τους στοιχείων λόγω εκκρεμούσας ποινικής διαδικασίας κατά του πρώτου προσφεύγοντος για τραπεζικό αδίκημα. Στο πρωτόδικο Δικαστήριο ζήτησαν την αποδέσμευση κάποιων λογαριασμών για την ανάληψη των εξόδων λόγω προβλημάτων υγείας του γιού τους. Ο πρώτος προσφεύγων παρέλειψε να προτείνει τον ισχυρισμό στο δευτεροβάθμιο δικαστήριο, πλην όμως αναφέρθηκε στα στοιχεία της πρωτόδικης αίτησης. Τα δικαστήρια απέρριψαν το αίτημα του.

Το κύριο ζήτημα που απασχόλησε το ΕΔΔΑ είναι αν υπήρχε *εύλογη σχέση αναλογικότητας μεταξύ του σκοπού και των μέσων* που χρησιμοποιήθηκαν για την επίτευξη αυτού του στόχου.

[355] Βλ. Apostolovi κατά Βουλγαρίας της 07.11.2019 (αριθ. προσφ. 32644/09), https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%2232644/09%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-197266%22]}

Το Δικαστήριο, διαπίστωσε ότι η εγχώρια νομοθεσία της Βουλγαρίας επιτρέπει την επιβολή δέσμευσης περιουσιακών στοιχείων ως παρεπόμενη ποινή, κρίνει όμως ότι το καθήκον των εθνικών δικαστηρίων ήταν να βεβαιωθούν ότι η δήμευση των περιουσιακών στοιχείων του πρώτου προσφεύγοντα δεν θα του προκαλέσει περισσότερη ζημία από εκείνη που αναπόφευκτα απορρέει από τα μέτρα αυτά[356]. Κατά το ΕΔΔΑ τα εγχώρια Δικαστήρια παρέλειψαν να διαπιστώσουν αν η πραγματική ζημία που υπέστησαν οι θιγόμενοι ήταν εκτενέστερη από εκείνη που είναι αναπόφευκτη, διαπιστώνοντας τελικά παραβίαση του άρθρου 1 του Πρώτου Πρωτοκόλλου της ΕΣΔΑ.

3. Η χωρίς πλαίσια και κριτήρια ευρεία παροχή εξουσίας στην αστυνομική αρχή κατά το στάδιο της προδικασίας, απασχόλησε το ΕΔΔΑ στην υπόθεση *Μοδέστου κατά Ελλάδας* της 16-3-2017 (αριθμ. προσφ. 51693/13)[357]. Και στην περίπτωση αυτήν το θέμα που εξετάσθηκε από το ΕΔΔΑ αγγίζει, μεταξύ άλλων τις υπερβολικές ενέργειες των εξουσιαστικών δομών, που κινούνται μακριά από την αρχή της αναλογικότητας και τους σχετικούς περιορισμούς που θέτει η αρχή αυτή στη σχέση μεταξύ σκοπού και μέσου που τελικά επιλέγεται.

Στην κριθείσα περίπτωση ο προσφεύγων είναι Κύπριος επιχειρηματίας, ο οποίος ζει στην Αθήνα. Με εντολή εισαγγελέα στο πλαίσιο προκαταρκτικής εξέτασης έγινε έρευνα στο σπίτι του, χωρίς να είναι ο ίδιος παρών, κατά τη διάρκεια της οποίας *κατασχέθηκαν υπολογιστές και έγγραφα*. Στη συνέχεια ο εισαγγελέας άσκησε εναντίον του ποινική δίωξη για εγκληματική οργάνωση. Το Δικαστήριο παρατήρησε ότι το ένταλμα έρευνας είχε συνταχθεί με γενικούς όρους. Ο εισαγγελέας δεν είχε συμπεριλάβει οποιαδήποτε πληροφορία σχετικά με την εν λόγω έρευνα και τα αντικείμενα που έπρεπε να κατασχεθούν, πράγμα που σήμαινε ότι παρείχε *ευρεία εξουσία* στον αστυνομικό. Το Δικαστήριο επισήμανε, ωστόσο, ότι η έρευνα συνοδεύονταν από ορισμένες διαδικαστικές δικλείδες. Το ΕΔΔΑ έκρινε ότι οι εθνικές αρχές δεν είχαν εκπληρώσει την υποχρέωσή τους σχετικά με τη παροχή σχετικών και επαρκών λόγων, οι οποίοι θα δικαιολογούν την έκδοση του εντάλματος έρευνας.

Ειδικότερα, τον Σεπτέμβριο του 2010 ο Εισαγγελέας του Εφετείου Αθηνών διέταξε την αστυνομία να διεξάγει έρευνες σε 15 κατοικίες και επαγγελματικούς χώρους, συμπεριλαμβανομένου της οικίας του προσφεύγοντος, στο πλαίσιο προκαταρκτικής έρευνας. Ένας αστυνομικός, συνοδευόμενος από τον αναπληρωτή εισαγγελέα, άνοιξε με τη

[356] Σχετική αναφορικά με την μείζονα σκέψη και η ΕΔΔΑ Mindek κατά Κροατίας της 11.09.2018 (αρ. προσφ. 6169/13), https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-186047%22]}

[357] Βλ. https://www.echrcaselaw.com/category/apofaseis-edda/kat-arthro/arthro-8/page/20/

βοήθεια κλειδαρά τη μπροστινή πόρτα και έψαξε το σπίτι του κ. Μοδέστου, κατάσχοντας έναν αριθμό αντικειμένων – δύο υπολογιστές και εκατοντάδες έγγραφα – παρουσία μάρτυρα. Τον Μάιο του 2012, ο εισαγγελέας κίνησε ποινικές διαδικασίες κατά κάποιων ατόμων, μεταξύ των οποίων και ο προσφεύγων, για συμμετοχή σε εγκληματική οργάνωση. Στις 8.11.2012 ο κ. Μοδέστος προσέφυγε στο Δικαστήριο ζητώντας η εντολή κατάσχεσης και η έρευνα να κηρυχθούν άκυρες και να επιστραφούν τα κατασχεθέντα αντικείμενα. Το Δικαστήριο απέρριψε την προσφυγή. Παρατήρησε ότι η προκαταρκτική έρευνα της αστυνομίας και η επακόλουθη προδικαστική έρευνα είχαν από κοινού ως στόχο την «διερεύνηση της αλήθειας», το τελευταίο αναφορικά με τον κατηγορούμενο και το πρώτο αναφορικά με «τον ύποπτο», ο οποίος, υποστήριξε, ότι απολάμβανε όλα τα δικαιώματα που παρέχονταν στον κατηγορούμενο. Το Δικαστήριο παρατήρησε ότι η προκαταρκτική έρευνα της αστυνομίας ήταν δικαστικής και όχι διοικητικής φύσεως και αποτέλεσε στάδιο της ποινικής διαδικασίας, αναγνωρίζοντάς της με τον τρόπο αυτόν νομιμοποιητική βάση.

4. Αναφορικά με τα δικαιώματα του κατηγορουμένου και ειδικότερο το της δυνατότητας πρόσβασης στην δικογραφία που αφορά την κατηγορία που του αποδίδεται, το ΕΔΔΑ ασχολήθηκε στην υπόθεση *Akif Hasanov κατά Αζερμπαϊτζάν* της 19/09/2019 (αρ. προσφ. 7268/10)[358].

Σύμφωνα με τα πραγματικά περιστατικά ο προσφεύγων είχε καταδικαστεί πρωτοδίκως σε ποινή κράτησης 5 ημερών για χουλιγκανισμό. Άσκησε έφεση κατά της απόφασης του πρωτοβάθμιου δικαστηρίου στις 26 Νοεμβρίου 2007, αλλά δεν ήταν παρών κατά την επ' ακροατηρίω συζήτηση σχετικά με την έφεσή του και δεν υπάρχει καμία απόδειξη ότι ο προσφεύγων έλαβε αυτοπροσώπως αντίγραφο της απόφασης του Εφετείου Μπακού της 12ης Δεκεμβρίου 2007, όπως είχε το δικαίωμα, εντός της προθεσμίας που ορίζει το άρθρο 437 του CAO. Το Δικαστήριο σημειώνει τον ισχυρισμό του προσφεύγοντα ότι είχε διαμαρτυρηθεί επίμονα σε διάφορες εγχώριες δικαστικές και εκτελεστικές αρχές σχετικά με την αποτυχία του Εφετείου του Μπακού να εξετάσει την έφεσή του και να εκδώσει την αντίστοιχη απόφαση και ότι δεν ακολούθησε καμία απάντηση από τις αρχές. Ο προσφεύγων υποστήριξε ότι μόλις στις 24 Αυγούστου 2009 έλαβε αντίγραφο της απόφασης που εξέδωσε το Εφετείο του Μπακού στις 12 Δεκεμβρίου 2007. Με τηλεομοιοτυπία της 28ης Αυγούστου 2014 ο δικηγόρος του προσφεύγοντος υπέβαλε νέα καταγγελία εξ ονόματος του

[358] Βλ. https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%227268/10%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-195852%22]}

προσφεύγοντος προβάλλοντας ότι η κατάσχεση από το γραφείο του ολόκληρου του φακέλου της υποθέσεως που αφορούσε την εκκρεμούσα, ενώπιον του Δικαστηρίου, υπόθεση του προσφεύγοντος αποτελούσε εμπόδιο στην άσκηση του δικαιώματος του προσφεύγοντος να υποβάλει μεμονωμένη προσφυγή δυνάμει του άρθρου 34 της Σύμβασης.

Κατά το Δικαστήριο, η αδυναμία πρόσβασης του προσφεύγοντος και του δικηγόρου του στα αντίγραφα του φακέλου της υπόθεσης, συνιστά αδικαιολόγητη παρέμβαση και σοβαρό εμπόδιο στην αποτελεσματική άσκηση του δικαιώματος ατομικής προσφυγής, και συνεπώς διαπίστωσε παραβίαση του άρθρου 34 της σύμβασης.

5. Έτερο ζήτημα αφορά στην διαχείριση του δικαιώματος του κατηγορουμένου να εξετάσει μάρτυρες υπεράσπισης, ιδίως μάρτυρες με ειδικές γνώσεις, που θα μπορούσαν, ιδίως στο αντικείμενο της έρευνας της παρούσης μελέτης, να φωτίσουν δύσβατα μονοπάτια σε ουσιαστικά ζητήματα αναφορικά με τον τρόπο λειτουργίας του διαμοιρασμού ηλεκτρονικών αρχείων αλλά και των ηλεκτρονικών ιχνών που συνδέουν μια συμπεριφορά με ένα αξιόποινο αποτέλεσμα, τόσο στο στάδιο της ολοκληρωμένης δράσης όσο και της απόπειρας (σχετικά με τα κατακερματισμένα ηλεκτρονικά αρχεία), που απαιτούν εξειδικευμένες γνώσεις πληροφορικής.

Το ΕΔΔΑ ασχολήθηκε με το ζήτημα της απαγόρευσης εξέτασης μαρτύρων υπεράσπισης στην προδικασία στην υπόθεση *Kartvelishvili κατά Γεωργίας* της 07.06.2018 (αριθ. προσφ. 17716/08)[359]. Το Δικαστήριο έκρινε ότι το αίτημα του κ. Kartvelishvili να εξετάσει μάρτυρες υπεράσπισης ενώπιον των εθνικών δικαστηρίων αποτέλεσε απολύτως εύλογη προσπάθεια να αμφισβητηθεί την υπόθεση ότι είχε στην κατοχή του ένα παράνομο αντικείμενο στο κελί του. Αυτό οφείλεται ιδιαίτερα στις ασυνέπειες στο σύνολο των διαδικασιών. Στην σε βάρος του προσφεύγοντος δίκη *αξιοποιήθηκε βίντεο* που ανέδειξε μια αντίφαση μεταξύ των καταθέσεων των μαρτύρων κατηγορίας. Παρά τις ασυνέπειες αυτές, τα Δικαστήρια αρνήθηκαν να εξετάσουν τους μάρτυρες υπεράσπισής του γιατί τους θεώρησαν αναξιόπιστους, ισχυρισμοί τους οποίους το ΕΔΔΑ έκρινε ανεπαρκείς. Πράγματι, μια τέτοια δικαιολογία αποτελούσε άρνηση καθήκοντος του ποινικού δικαστηρίου να διεξάγει δίκη χωρίς προκαταλήψεις σχετικά με την ενοχή του κατηγορούμενου και, σε περίπτωση αμφιβολίας, να αποφασίζει πάντα υπέρ του κατηγορουμένου. Ο κ. Kartvelishvili αποκλείστηκε έτσι από τη μοναδική ευκαιρία να αμφισβητήσει αποτελεσματικά τον πυρήνα της κατηγορίας που διατυπώθηκε εναντίον του. Τα υπόλοιπα στοιχεία, το βίντεο και η

[359] Βλ. https://www.echrcaselaw.com/apofaseis-edda/kat-arthro/arthro-6/prokatalipsi-dikastwn-se-varos-katigoroymenoy-arnisi-na-eksetasoun-martires-iperaspisis/

αναφορά της έρευνας και της κατάσχεσης, δεν προσκόμισαν πρόσθετα, αυτόνομα αποδεικτικά στοιχεία που να αποδεικνύουν την ενοχή του κ. Kartvelishvili.

Η άρνηση των εγχώριων δικαστηρίων να εξετάσουν τους μάρτυρες υπεράσπισης, χωρίς να ληφθεί υπόψη η πιθανή συνάφεια της μαρτυρίας τους, καθιστούσε ως εκ τούτου τη δίκη στο σύνολό της άδικη, κατά παραβίαση του άρθρου 6 § 1 και 3 (δ).

6. Η σύγκρουση του δικαιώματος στο απόρρητο της επικοινωνίας από τη μια και η αποδεικτικές δυσχέρειες μια ιδιάζουσας αξιόποινης συμπεριφοράς, όπως είναι η δωροδοκία, απασχόλησαν το ΕΔΔΑ στην υπόθεση *Oleynik κατά Ρωσίας* της 21.06.2016 (αριθ. προσφ. 23559/07)[360]. Εκείνο που αποτέλεσε κυρίως αντικείμενο της δικανικής κρίσης ήταν η έλλειψη ειδικής νομοθετικής πρόβλεψης που να καθορίζει τα πλαίσια μια νομιμοποιημένης διάρρηξης του δικαιώματος στο σχετικό αυτό απόρρητο υπέρ καθορισμένων λόγων, πάντα με σεβασμό στην αρχή της αναλογικότητας και της αναγκαιότητας.

Ο προσφεύγων, Aleksey Nikolayevich Oley nik, είναι Ρώσος υπήκοος ο οποίος γεννήθηκε το 1974 και ζει στην Rtishchevo (περιοχή Saratov, Ρωσία). Σύμφωνα με τους ισχυρισμούς του, υπό την ιδιότητά του ως αξιωματικός της αστυνομίας, φέρεται να έχει δωροδοκηθεί από ένα άτομο (V), ο οποίος στην συνέχεια τον κατήγγειλε στην Ομοσπονδιακή Υπηρεσία Ασφαλείας (FSB) και ο οποίος κατέγραψε τις συνομιλίες τους, χρησιμοποιώντας ένα μαγνητόφωνο κρυμμένο πάνω του. Η πρώτη ηχογράφηση έγινε με τη πρωτοβουλία του V. και οι μεταγενέστερες εγγραφές σύμφωνα με τις οδηγίες της FSB.

Στις 03.02.2006, ο κ. Oleynik συνελήφθη από αξιωματικούς της FSB στο δημόσιο σχολείο όπου εργάζεται η σύζυγός του, την στιγμή που ο V. θα του παρέδιδε τα χρήματα. Αρκετοί άλλοι άνθρωποι ήταν παρόντες στη στιγμή εκείνη. Σύμφωνα με τα λεγόμενα του προσφεύγοντος, κρατήθηκε για ένα μεγάλο μέρος της νύχτας στις εγκαταστάσεις της FSB χωρίς να του παρουσιάσουν κάποιο έγγραφο που να νομιμοποιεί την κράτησή του, και ήταν σοβαρά κτυπημένος από τη προσπάθεια των αστυνομικών αρχών να του αποσπάσουν μια ομολογία.

Στις 6.10.2006 ο κ. Oleynik καταδικάστηκε σε φυλάκιση δύο ετών. Το δικαστήριο βάσισε την απόφασή του, μεταξύ άλλων παραγόντων, στις δηλώσεις του V. και ορισμένων μαρτύρων, στις εκθέσεις σχετικά με την κατάσχεση των χρημάτων και στις ηχογραφημένες συνομιλίες μεταξύ του προσφεύγοντος και του V. Μετά τη προσφυγή επί νομικών

[360] Βλ. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-163807%22]}

ζητημάτων, το Περιφερειακό Δικαστήριο του Saratov έκανε δεκτή την απόφαση της 26ης Δεκεμβρίου 2006.

Το ΕΔΔΑ διαπίστωσε ότι η *καταγραφή των συνομιλιών* του κ. Oleynik αποτελούσε *παρεμβολή στο δικαίωμα άσκησης του δικαιώματος του σεβασμού της ιδιωτικής και οικογενειακής ζωής του*. Προκειμένου να διαπιστωθεί κατά πόσον η παρέμβαση ήταν σύμφωνα με το νόμο, κατά την έννοια του άρθρου 8 § 2 της ΕΣΔΑ, το Δικαστήριο αναφέρθηκε στην απόφασή του από την υπόθεση Bykov[361], στην οποία διαπίστωσε ότι «*η απουσία συγκεκριμένων και λεπτομερών ρυθμίσεων, έχει ως αποτέλεσμα η χρήση αυτής της τεχνικής επιτήρησης ως μέρος ενός λειτουργικού πειράματος να μη συνοδεύεται από επαρκείς εγγυήσεις για τη πρόληψη καταχρήσεων. Συνεπώς, η χρήση της υπόκειτο σε αυθαιρεσίες και ήταν ασυμβίβαστη με τη νομιμότητα.*»

Το Δικαστήριο επισήμανε ότι, μετά την έκδοση της αποφάσεως αυτής οι αρχές δεν προέβησαν σε καμία νομοθετική τροποποίηση έτσι ώστε η χρήση αυτής της τεχνικής επιτήρησης να περιστοιχίζεται από επαρκείς εγγυήσεις και δικλείδες ασφαλείας έναντι διαφόρων πιθανών καταχρηστικών ενεργειών. Ως εκ τούτου, το Δικαστήριο έκρινε ότι η παρέμβαση στην παρούσα υπόθεση δεν ήταν «σύμφωνη με το νόμο», κατά το έννοια του άρθρου 8 § 2 της Σύμβασης, και ότι υπήρξε παραβίαση του Άρθρου 8.

7. Η <u>αόριστη διατήρηση δεδομένων</u> που συνδέουν τον κατηγορούμενο με την πράξη, τα οποία δίνουν προσωποποιημένη πληροφόρηση μετά την αμετάκλητη καταδίκη του, στα πλαίσια προστασίας της δημόσιας ασφάλειας, συγκρούεται με το δικαίωμά του σ την ιδιωτική του ζωή.

Σχετική η απόφαση του ΕΔΔΑ στην υπόθεση *Gaughran κατά Ηνωμένου Βασιλείου* της 13.02.2020 (αριθ. 45245/15)[362]. Ο προσφεύγων Fergus Gaughran, είναι βρετανός υπήκοος, ο οποίος γεννήθηκε το 1972 και ζει στο Newry (Βόρεια Ιρλανδία). Συνελήφθη τον Οκτώβριο του 2008 για οδήγηση υπό την επήρεια αλκοόλ. Μεταφέρθηκε στο αστυνομικό τμήμα όπου υπεβλήθη σε αλκοτέστ μέσω αναπνοής το οποίο κατέληξε θετικό. Η αστυνομία πήρε επίσης τη φωτογραφία του, τα δακτυλικά του αποτυπώματα και δείγμα DNA. Αργότερα κρίθηκε ένοχος, του επιβλήθηκε πρόστιμο και απαγόρευση να οδηγεί για 12 μήνες. Η καταδίκη του εκτίθηκε το 2013. Το δείγμα DNA του καταστράφηκε το 2015

[361] Βλ. Case of Bykov v. Russia (Application no. 4378/02) https://hudoc.echr.coe.int/fre# {%22itemid%22:[%22001-91704%22]}

[362] Βλ. https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%2245245/15%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-200817%22]}

κατόπιν αιτήσεώς του. Η αστυνομική υπηρεσία της Βόρειας Ιρλανδίας («PSNI») εξακολουθεί να διατηρεί για αόριστο χρόνο το προφίλ DNA (*ψηφιακά δεδομένα*) που εξήχθη από το δικό του δείγμα DNA, τα δακτυλικά αποτυπώματα και τη φωτογραφία του. Ο προσφεύγων αμφισβήτησε ανεπιτυχώς τη συνεχιζόμενη διατήρηση των δεδομένων του PSNI ενώπιον των εθνικών δικαστηρίων.

Το Δικαστήριο διαπίστωσε ότι η διατήρηση του προφίλ DNA, των δακτυλικών αποτυπωμάτων και της φωτογραφίας του προσφεύγοντος, με τη μορφή ψηφιακών δεδομένων, συνιστούσε *προσβολή της ιδιωτικής ζωής του*, η οποία είχε *ολοκληρώσει τον νόμιμο σκοπό* της ανίχνευσης και επομένως την πρόληψη του εγκλήματος. Υπογράμμισε τη σπουδαιότητα της εξέτασης των δικαιωμάτων ιδιωτικού απορρήτου όπου οι εξουσίες που εμπίπτουν στις αρμοδιότητες του κράτους ήταν *ασαφείς και η διαθέσιμη τεχνολογία εξελίσσεται συνεχώς*. Παραδείγματος χάριν, η τεχνολογία που αφορά τις φωτογραφίες και τη χαρτογράφηση του προσώπου είχε ήδη προχωρήσει από τη στιγμή που η υπόθεση είχε εξεταστεί από τα εθνικά δικαστήρια. Στη συνέχεια εξέτασε αν η παρέμβαση στα δικαιώματα του προσφεύγοντος για την προστασία της ιδιωτικής ζωής ήταν δικαιολογημένη, επαναλαμβάνοντας ότι οι εθνικές αρχές έπρεπε να διαθέτουν «*περιθώριο εκτίμησης*» κατά την αξιολόγηση αυτή. Μια ισχυρή συναίνεση στην προσέγγιση των κρατών μελών όσον αφορά τη διατήρηση δεδομένων όσων καταδικάστηκαν για αδίκημα θα περιορίσουν αυτό το περιθώριο εκτίμησης. Το Δικαστήριο έκρινε ότι η πλειοψηφία των κρατών μελών είχαν καθεστώτα που έθεταν χρονικό περιορισμό διατήρησης των βιομετρικών δεδομένων των καταδικασθέντων, δηλαδή τα δακτυλικά τους αποτυπώματα και τα προφίλ DNA. Το Ηνωμένο Βασίλειο ήταν ένα από τα λίγα κράτη του Συμβουλίου της Ευρώπης που επιτρέπει την *αόριστη* διατήρηση των προφίλ DNA. Το περιθώριο εκτίμησης, ιδίως όσον αφορά τα προφίλ DNA, ήταν περιορισμένο συνεπώς για την ανωτέρω αιτία. Περαιτέρω το ΕΔΔΑ υπογράμμισε ωστόσο ότι η διάρκεια της διατήρησης δεν ήταν καθοριστική για την εκτίμηση κατά πόσο ένα κράτος είχε υπερβεί το αποδεκτό περιθώριο εκτίμησης για να καθορίσει το καθεστώς συλλογής και διατήρησης δεδομένων. Δεν υπήρχε ο ίδιος κίνδυνος στιγματισμού στη διατήρηση των δεδομένων όπως στην υπόθεση S. και Marper κατά Ηνωμένου Βασιλείου, η οποία αφορούσε άτομα που ήταν ύποπτα για αδικήματα αλλά όχι καταδικασθέντα.

Αυτό που ήταν καθοριστικό ήταν η ύπαρξη και η λειτουργία διασφαλίσεων. Αφού επέλεξε το κράτος την αόριστη διατήρηση και συλλογή δεδομένων, το κράτος βρισκόταν στο όριο του περιθωρίου εκτίμησης. Επομένως, έπρεπε να διασφαλίσει ότι υπήρχαν ορισμένες

διασφαλίσεις και ήταν αποτελεσματικές για τον προσφεύγοντα. Εντούτοις, τα βιομετρικά δεδομένα και οι φωτογραφίες του προσφεύγοντος διατηρήθηκαν χωρίς να γίνει αναφορά στη σοβαρότητα του αδικήματός του και ανεξάρτητα από τη διαρκή ανάγκη διατήρησης των δεδομένων αυτών επ' αόριστον. Επιπλέον, η αστυνομία στη Βόρεια Ιρλανδία ήταν εξουσιοδοτημένη να διαγράψει βιομετρικά στοιχεία, δεδομένα και φωτογραφίες μόνο σε εξαιρετικές περιπτώσεις. Επομένως, ο προσφεύγων δεν μπορούσε να ζητήσει επανεξέταση της διατήρησης των δεδομένων του, δεδομένου ότι δεν υπήρχε διάταξη που να επιτρέπει τη διαγραφή εάν κριθεί ότι τα δεδομένα δεν ήταν πλέον απαραίτητα λόγω της φύσης του αδικήματος, της ηλικίας του ή του χρόνου που είχε παρέλθει και της σημερινής του προσωπικότητας. Το Δικαστήριο διαπίστωσε ότι η φύση των εξουσιών αυτών δεν επέτρεψε την επίτευξη δίκαιης ισορροπίας μεταξύ των ανταγωνιστικών δημόσιων και ιδιωτικών συμφερόντων. Κατά συνέπεια, το εναγόμενο κράτος υπερέβη το αποδεκτό περιθώριο εκτίμησης και η επίδικη διατήρηση συνιστούσε δυσανάλογη προσβολή του δικαιώματος του προσφεύγοντος στο σεβασμό της ιδιωτικής ζωής, η οποία δεν μπορούσε να θεωρηθεί αναγκαία σε μια δημοκρατική κοινωνία. Κατά συνέπεια, υπήρξε παραβίαση του δικαιώματος της ιδιωτικής ζωής (άρθρο 8 της Σύμβασης).

8. Η προβληματική της πρακτικής εφαρμογής της *αρχής της αναλογικότητας και της αρχής του σκοπού*, απασχόλησε το ΕΔΔΑ αναφορικά με το επαγγελματικό απόρρητο και ειδικότερα με την επιβολή κατάσχεσης στα αρχεία δικηγορικού γραφείου και τούτο όχι για πρώτη φορά. Η πλέον πρόσφατη είναι η περίπτωση της υπόθεσης *Kırdök κ.α. κατά Τουρκίας* της 03.12.2019 (αριθ. 14704/12)[363].

Οι προσφεύγοντες, Mehmet Ali Kırdök, Mihriban Kırdök και Meral Hanbayat, είναι Τούρκοι υπήκοοι οι οποίοι γεννήθηκαν το 1954, 1958 και 1980 αντίστοιχα και ζουν στην Κωνσταντινούπολη. Είναι όλοι δικηγόροι, διαμαρτυρήθηκαν για την κατάσχεση των ηλεκτρονικών τους δεδομένων από τις δικαστικές αρχές για την άσκηση ποινικής δίωξης κατά άλλου δικηγόρου (Ü.S.), ο οποίος μοιράζονταν το γραφείο τους.

Το 2011 το γραφείο του Εισαγγελέα της Κωνσταντινούπολης ξεκίνησε έρευνα για τον εντοπισμό και την έκθεση των κρυφών διαύλων επικοινωνίας που δημιουργήθηκαν μεταξύ του Abdullah Öcalan και της πρώην οργάνωσής του (το PKK – το Κόμμα των Εργαζομένων του Κουρδιστάν, – και το KCK). Δικαστής στο Κακουργιοδικείο της Κωνσταντινούπολης εξέδωσε ένταλμα για τις δραστηριότητες του Ü.S., ο οποίος συνελήφθη

[363] Βλ. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-198805%22]}

την επόμενη μέρα στο σπίτι του. Η αστυνομία διεξήγαγε έρευνες στο γραφείο που μοιράζονταν με τους προσφεύγοντες. Όλα τα δεδομένα που ήταν αποθηκευμένα στο σκληρό δίσκο του υπολογιστή που χρησιμοποιούνταν *από κοινού* από τους δικηγόρους αντιγράφηκαν σε ένα υλικό φορέα USB το οποίο ανήκει στην κα Hanbayat.

Στη συνέχεια, οι προσφεύγοντες άσκησαν αναίρεση κατά της απόφασης του δευτεροβάθμιου δικαστηρίου, τόσο εξ ονόματός τους όσο και ως εκπρόσωποι του Ü.S. Ειδικότερα, ζήτησαν την *επιστροφή ή την καταστροφή των ψηφιακών τους δεδομένων*, υποστηρίζοντας ότι δεν ανήκαν στον Ü.S., προστατεύονταν από το *επαγγελματικό απόρρητο* και είχαν καταληφθεί χωρίς σχετική εντολή. Το γραφείο του εισαγγελέα παρουσίασε τις δικές του παρατηρήσεις, δηλώνοντας ότι δεδομένου ότι τα εν λόγω δεδομένα δεν είχαν ακόμη μεταγραφεί, ήταν αδύνατο να αναγνωριστεί ο κάτοχος των εν λόγω δεδομένων. Το Ανώτατο Δικαστήριο απέρριψε τους ισχυρισμούς των προσφευγόντων, εξετάζοντας ότι η αναιρεσιβαλλομένη απόφαση εκδόθηκε σύμφωνα με τον νόμο και τη νόμιμη διαδικασία.

Βασιζόμενοι στο άρθρο 8 (δικαίωμα σεβασμού της ιδιωτικής ζωής, της κατοικίας και της αλληλογραφίας) και άρθρο 13 (δικαίωμα για αποτελεσματική προσφυγή), οι προσφεύγοντες ισχυρίστηκαν ότι το επαγγελματικό απόρρητο τω δικηγόρων, βασιζόμενο στην ύπαρξη εχεμύθειας και εμπιστευτικότητας μεταξύ των σχέσεων τους με τους πελάτες τους, παραβιάστηκε λόγω του ότι τα εν λόγω ψηφιακά αρχεία αναφορικά με τις υποθέσεις αυτών των πελατών αντιγράφηκαν από τις δικαστικές αρχές κατά τη διάρκεια μιας έρευνας και ότι τα εν λόγω αντίγραφα κατασχέθηκαν παρά το γεγονός ότι ήταν *άσχετα* με τη διεξαγωγή της έρευνας σε σχέση με άλλο δικηγόρο.

Το Δικαστήριο σημείωσε ότι οι προσφεύγοντες, οι οποίοι δεν αποτέλεσαν αντικείμενο της ποινικής έρευνας, υποστήριξαν ενώπιον των δικαστικών αρχών ότι τα κατασχεθέντα ηλεκτρονικά δεδομένα ανήκαν σε αυτούς και καλύπτονταν από επαγγελματικό απόρρητο δικηγόρου-πελάτη. Σημείωσε επίσης ότι στην διάταξή του ο δικαστής του Κακουργιοδικείου επεσήμανε το εύρος της έρευνας των χώρων, δηλώνοντας ότι ο στόχος της επιχείρησης ήταν να «συγκεντρωθούν αποδεικτικά στοιχεία και να κατασχεθούν αντικείμενα», αποδεικνύοντας ότι ο ύποπτος (Ü.S.) είχε εμπλακεί σε δραστηριότητες της τρομοκρατικής οργάνωσης KCK/PKK. Η Διάταξη δεν διευκρίνισε ποιο *συγκεκριμένο* ή συγκεκριμένα στοιχεία ή έγγραφα έπρεπε να κατασχεθούν στις συγκεκριμένες διευθύνσεις, συμπεριλαμβανομένων των εγκαταστάσεων της δικηγορικής εταιρείας των προσφευγόντων ή του τρόπου με τον οποίο τα εν λόγω αποδεικτικά στοιχεία έχουν σχέση με την ποινική έρευνα. Έτσι, σύμφωνα με τη Διάταξη, οι αρχές που είναι υπεύθυνες για την έρευνα είχαν

γενικά τη δυνατότητα να εξετάσουν *όλα* τα ψηφιακά δεδομένα που είναι αποθηκευμένα στα γραφεία των προσφευγόντων, χωρίς να ανησυχούν υπερβολικά για το γεγονός ότι ερευνούσαν τις εγκαταστάσεις μιας δικηγορικής εταιρείας που θα μπορούσε να φιλοξενήσει τα έγγραφα που παρέδιδαν οι πελάτες στους νόμιμους εκπροσώπους τους.

Επιπλέον, το ευρύ πεδίο εφαρμογής της Διάταξης αντανακλάται στον τρόπο με τον οποίο εφαρμόστηκε. Παρόλο που υπήρξε εκπρόσωπος του δικηγορικού συλλόγου της Κωνσταντινούπολης και ο ένας προσφεύγων ήταν παρών κατά τη διάρκεια της έρευνας και τα κατασχεθέντα δεδομένα είχαν τοποθετηθεί σε σφραγισμένη τσάντα, *χωρίς να έχουν ληφθεί ιδιαίτερα μέτρα για την προστασία τους*, ώστε να μην λάβει χώρα παρέμβαση στο επαγγελματικό απόρρητο. Πράγματι, δεν υπήρχε μηχανισμός φιλτραρίσματος ηλεκτρονικών εγγράφων ή δεδομένων που καλύπτονται από το επαγγελματικό απόρρητο ή οποιαδήποτε ρητή απαγόρευση της κατάσχεσης των δεδομένων που καλύπτονται από την εμπιστευτικότητα αυτή κατά τη διάρκεια της έρευνας. Αντιθέτως, όλα τα δεδομένα στον σκληρό δίσκο του υπολογιστή που χρησιμοποιούνται από κοινού από όλους τους δικηγόρους που εργάζονταν στις εγκαταστάσεις και είχαν συλλεχθεί σε ένα stick USB είχαν κατασχεθεί.

Μόλις οι προσφεύγοντες ζήτησαν την επιστροφή των ψηφιακών δεδομένων, βασιζόμενοι στο επαγγελματικό απόρρητο της σχέσης μεταξύ δικηγόρου-πελάτη, οι δικαστικές αρχές βρίσκονταν σε νόμιμη υποχρέωση έγκαιρης αξιολόγησης των κατασχεθέντων δεδομένων και επιστροφής των δεδομένων που προστατεύονται από το απόρρητο ή την καταστροφή των δεδομένων, ανάλογα με την περίπτωση. Ωστόσο, η εθνική νομοθεσία και πρακτική ήταν *ασαφείς* ως προς τις συνέπειες οποιασδήποτε αδυναμίας των δικαστικών αρχών να τηρήσουν την υποχρέωση αυτή.

Το Κακουργιοδικείο είχε οριστικά αρνηθεί να επιστρέψει ή να καταστρέψει τα κατασχεθέντα αντίγραφα των δεδομένων, βασιζόμενο σε αιτιολογία, η οποία απλώς ανέφερε τη νομιμότητα των ερευνών που διενεργήθηκαν στα δικηγορικά γραφεία και δεν αντέδρασε στον συγκεκριμένο ισχυρισμό *περί παραβίασης της εμπιστευτικότητας της σχέσης δικηγόρου – πελάτη*. Φαίνεται ότι το Κακουργιοδικείο είχε σιωπηρά δεχτεί τους λόγους που πρόβαλε η εισαγγελία για να δικαιολογήσει την άρνηση επιστροφής των κατασχεθέντων δεδομένων, σύμφωνα με τους οποίους, αφού τα εν λόγω δεδομένα δεν είχαν ακόμη διερευνηθεί, ήταν αδύνατο να εξακριβωθούν οι ακριβείς ιδιοκτήτες τους. Το Δικαστήριο έκρινε όχι μόνο ότι ένας τέτοιος λόγος άρνησης δεν προβλέπεται σαφώς από το νόμο, αλλά ήταν επίσης *ασυμβίβαστος με την ουσία* του επαγγελματικού απορρήτου που προστατεύει τις σχέσεις μεταξύ των δικηγόρων και των πελατών τους. Σε κάθε περίπτωση, δεν μπορούσε να

συναχθεί το συμπέρασμα ότι η εξέταση του αιτήματος των προσφευγόντων από τις δικαστικές αρχές ότι είχαν συμμορφωθεί με την υποχρέωση να προβλέπουν ιδιαίτερα αυστηρή επαλήθευση των μέτρων σχετικά με τα δεδομένα που καλύπτονται από το επαγγελματικό απόρρητο. Τέλος, το αντισταθμιστικό ένδικο βοήθημα (άρθρο 141 του κώδικα ποινικής δικονομίας) στο οποίο αναφέρθηκε η κυβέρνηση ήταν πολύ διαφορετικό από την αίτηση για κήρυξη ακυρότητας μιας αμφισβητούμενης κατάσχεσης και δεν θα είχε οδηγήσει στην επιστροφή ή την καταστροφή των αντιγράφων που προστατεύονται από την επαγγελματική εχεμύθεια.

Συνεπώς, τα μέτρα που επιβλήθηκαν στους προσφεύγοντες (κατάσχεση των ψηφιακών τους δεδομένων και η άρνησή τους να τα επιστρέψουν ή να τα καταστρέψουν) δεν είχαν ανταποκριθεί σε μια πιεστική κοινωνική ανάγκη, *δεν ήταν αναλογικά προς τους επιδιωκόμενους νόμιμους σκοπούς* (πρόληψη αναταραχών, πρόληψη εγκληματικών αδικημάτων και προστασία των δικαιωμάτων και ελευθεριών των άλλων) και δεν ήταν απαραίτητα σε μια δημοκρατική κοινωνία. Συνεπώς, υπήρξε παραβίαση του άρθρου 8 της Σύμβασης.

Ελλείψει επαρκών διαδικαστικών εγγυήσεων στη σχετική νομοθεσία όπως ερμηνεύεται και που εφαρμόστηκαν από τις δικαστικές αρχές στην παρούσα υπόθεση, το Δικαστήριο έκρινε ότι οι καταγγελίες σύμφωνα με το άρθρο 13 της Σύμβασης, καλύπτονται από τον ίδιο λόγο με την καταγγελία βάσει του άρθρου 8.

9. Η επιβολή των μέτρων δικονομικού καταναγκασμού που σχετίζονται με την στέρηση ή περιορισμούς στο δικαίωμα του ατόμου στην περιουσία του, απαντάται και στην περίπτωση της κατάσχεσης προσωπικών αντικειμένων. Το ΕΔΔΑ αξιολόγησε τις δράσεις των αρχών μέσα και στο νομικό πλαίσιο των διατάξεων που προστατεύουν από παραβιάσεις της προσωπικής ζωής. Στην υπόθεση *Zosymov κατά Ουκρανίας* της 07.07.2016 (αριθ. προσφ. 4322/06)[364] αξιολογήθηκαν τα παράπονα του προσφεύγοντος σχετικά με έρευνα της αστυνομίας στο γραφείο, στο αυτοκίνητο και το γκαράζ του σπιτιού του, και στη διάρκεια της οποίας κατασχέθηκαν πολυάριθμα αντικείμενα.

Ο προσφεύγων και η σύζυγός του έχουν μια μικρή επιχείρηση η οποία, μεταξύ άλλων, αναπαρήγαγε ψηφιακά δεδομένα και πωλούσε άδειες συσκευές αποθήκευσης δεδομένων. Τον Αύγουστο του 2002 αρκετοί αξιωματικοί αστυνομικοί από τη μονάδα του οικονομικού εγκλήματος στο Κίεβο επιθεώρησαν το γραφείο τους και *κατάσχεσαν ένα*

[364] Βλ. https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-164467%22]}

μεγάλο αριθμό αντικειμένων, συμπεριλαμβανομένων πολλών υπολογιστών, πάνω από 3.000 σκληρούς δίσκους που περιείχαν δεδομένα και περίπου 30.000 κενούς δίσκους. Η επιτόπια έρευνα διήρκεσε μία ολόκληρη νύχτα, στη διάρκεια της οποίας οι αστυνομικοί ανέκριναν τον κ. Zosymov, την σύζυγό του και άλλα μέλη της οικογένειας σχετικά με την επιχείρηση και την τήρηση της νομοθεσίας περί πνευματικής ιδιοκτησίας. Δύο ημέρες αργότερα, μια έκθεση δημοσιεύτηκε στην ιστοσελίδα του Υπουργείου Εσωτερικών, δηλώνοντας ότι η αστυνομία είχε «*εντοπίσει την εγκληματική ομάδα των δύο ατόμων [που] ... εγκατέστησε και διαχειριζόταν ολόκληρη υπόγεια παραγωγή*». Η έκθεση επισύναπτε φωτογραφία της συζύγου του κ. Zosymov χωρίς καμία λεζάντα.

Τον Νοέμβριο του 2002 κινήθηκαν ποινικές διαδικασίες με την υποψία της παραβίασης δικαιωμάτων πνευματικής ιδιοκτησίας, χωρίς να αναφερθούν τα ονόματα των πιθανών παραβατών. Στην απόφασή του, ο ανακριτής αναφέρθηκε στην έρευνα του γραφείου του κυρίου και της κυρίας Zosymov και στην κατάσχεση της περιουσίας τους. Ο ανακριτής στη συνέχεια κήρυξε τα κατασχεθέντα αντικείμενα φυσικές αποδείξεις που έπρεπε να κατασχεθούν από την αστυνομία εν αναμονή της διερεύνησης της υπόθεσης. Μετά την εξονυχιστική έρευνα του διαμερίσματος του ζευγαριού η διαδικασία παρέμεινε σε αναμονή. Τελικά δεν ασκήθηκε ποτέ ποινική δίωξη εναντίον του κ. Zosymov ή οποιοδήποτε άλλου προσώπου.

Ο κ. Zosymov ζήτησε πολλές φορές από την αστυνομία και τον εισαγγελέα την επιστροφή της κατασχεθείσας περιουσίας του. Σε αρκετές περιπτώσεις, οι αρχές απέρριψαν τα αιτήματά του, ενημερώνοντάς τον ότι τα κατασχεθέντα περιουσιακά στοιχεία αποτελούσαν φυσικά αποδεικτικά στοιχεία σε μια ποινική υπόθεση. Ο εισαγγελέας και η αστυνομία επίσης απέρριψαν το αίτημά του να εισαχθεί η ποινική υπόθεση, για την οποία τα στοιχεία είχαν κατασχεθεί, ενώπιον δικαστηρίου ώστε να κλείσει η υπόθεση και να τερματιστούν οι ποινικές διαδικασίες λόγω ελλείψεων αποδεικτικών στοιχείων.

Ο προσφεύγων και η σύζυγός του ανεπιτυχώς εκκίνησαν διαδικασίες για δυσφήμηση κατά των αστυνομικών αρχών σχετικά με τη δημοσίευση ανακριβούς ποινικής αναφοράς στην ιστοσελίδα τους, επιδιώκοντας την αφαίρεση των πληροφοριών από την ιστοσελίδα. Ο κ. Zosymov επίσης ανεπιτυχώς κατάθεσε καταγγελίες κατά της αστυνομίας σχετικά με το παράνομο της έρευνας και ζητώντας την επιστροφή της κατασχεθείσας περιουσίας.

Το ΕΔΔΑ απεφάνθη ότι το γραφείο, το αυτοκίνητο και το γκαράζ του προσφεύγοντος είχαν ερευνηθεί παράνομα, παραβιάζοντας το άρθρο 8 (δικαίωμα στο σεβασμό της ιδιωτικής

και οικογενειακής ζωής, της οικίας και της αλληλογραφίας), ότι επίσης, η κατάσχεση της περιουσίας του παραβίαζε τα δικαιώματά του ιδιοκτησίας, σύμφωνα με το άρθρο 1 του Πρωτοκόλλου Νο 1. Τέλος, το ΕΔΔΑ καταδίκασε την Ουκρανία και για παράβαση του άρθρου 13 της ΕΣΔΑ, δεδομένου ότι ο προσφεύγων δεν είχε κανένα ένδικο μέσο να ζητήσει αποζημίωση αναφορικά με τις καταγγελίες του.

Οι σχετικές ενστάσεις και ανησυχίες αναφορικά με τις εξουσιαστικές πρακτικές θεσμών και οργάνων άσκησης της κρατικής εξουσίας, σαφώς και αποτελούν ένα σταθερό πεδίο αντιπαράθεσης στον τομέα της αποδεικτικής αξιοποίησης δεδομένων στα πλαίσια μιας ποινικής δίκης. Οι ανάγκες για πρόληψη αρχικά και καταστολή ακολούθως του (ηλεκτρονικού) εγκλήματος δημιουργούν ένα εκρηκτικό πεδίο αντιπαραθέσεων[365]. Τα ζητήματα που απασχολούν εδώ έχουν βάση στην προβληματική της αποδεικτικής αξιοποίησης στοιχείων, που ελήφθησαν χωρίς νομιμοποιητική βάση, αλλά τυγχάνει να είναι και τα μοναδικά που αποδεικνύουν την τέλεση της πράξης και την σύνδεσή της με τον κατηγορούμενο.

Οι υποθέσεις που κατά καιρούς απασχόλησαν το ΕΔΔΑ αλλά και εθνικά δικαστήρια αναφορικά με τις αστυνομικές πρακτικές, είναι πολλές αλλά η νομολογία δεν υπήρξε εναρμονισμένη, ιδίως μεταξύ των εθνικών δικαστών και του ΕΔΔΑ. Υπό την βασική προϋπόθεση της προστασίας του δημοσίου συμφέροντος, εδώ με τη μορφή της ασφάλειας, τόσο σε κοινωνικό όσο και σε ατομικό επίπεδο, ο εθνικός δικαστής πολλές φορές καταφεύγει (και τούτο είναι οδυνηρό να καταλογίζεται σε μια ανεξάρτητη συντεταγμένη εξουσία δημοκρατικού κράτους όπως είναι η δικαστική) σε πρακτικές που αντικειμενικά αξιολογούμενες διατηρούν ένα αρνητικό πρόσημο.

Κι εξηγούμαι. Δεν είναι λίγες οι περιπτώσεις, όπου ο εθνικός δικαστής προκειμένου να μην αχθεί σε μια κρίση απαλλακτική στην βάση της παραδοχής μιας ακυρότητας σε μια ποινική δίκη, ακόμη και απροκάλυπτα, καταφεύγει σε παιγνιδίσματα, σε τέτοιο βαθμό, που σε εργασία προπτυχιακού φοιτητή της νομικής, θα οδηγούσαν τον τελευταίο σε επανεξέταση στην επόμενη εξεταστική περίοδο. Απομακρυνόμενος από διακηρυκτικούς αφορισμούς, ξεκαθαρίζω ότι αναφέρομαι στις προσπάθειες, νομιμοποίησης παρανόμων συμπεριφορών των διωκτικών αρχών, στα πλαίσια ανοχής (από μέρους της δικαστικής εξουσίας) πρακτικών και μεθοδεύσεων της αστυνομίας. Έτσι λ.χ. στην περίπτωση κατά την οποία εντοπίζεται μια ποινικώς ενδιαφέρουσα ηλεκτρονική επικοινωνία και εφόσον δεν υπάρχει το νομιμοποιητικό

[365] Βλ. *Αργ. Καρράς*, Η αναίρεση στην ποινική δίκη, Νομική Βιβλιοθήκη, 2017, σελ. 239.

βούλευμα του Ν 2225/1994 (σε συνδυασμό με τις διατάξεις του Ν 3471/2006 για την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες), η παρανόμως κτηθείσα πληροφορία από την παρακολούθηση της ηλεκτρονικής επικοινωνίας, παρουσιάζεται στο αιτιολογικό της δικαστικής απόφασης ως αποδεικτική πληροφορία κτηθείσα όχι με τον πραγματικό τρόπο, που περιγράφηκε, αλλά μέσα από την κατάθεση του αστυνομικού που έκανε την έρευνα[366]. Με άλλα λόγια έχουμε την «νομιμοποίηση» της υποκλαπείσας ηλεκτρονικής επικοινωνίας με την ψευδαίσθηση του ότι η επίκληση της κατάθεσης του αστυνομικού που ενήργησε την παράνομη έρευνα, είναι δικονομικά συνεπής.

Λίγο θέλει να σημειωθεί το απαράδεκτο της συγκεκριμένης επιλογής[367]. Στις περιπτώσεις δε που ο κατηγορούμενος θα υποβάλλει το (αναιρετικό) παράπονό του αρμοδίως, υποκείμενος στην ιδιαίτερα μεγάλη δαπάνη μιας αναιρετικής δίκης, η αιτιολόγηση της αναιρεσιβαλλομένης απόφασης στην βάση του ότι ναι μεν προκύπτει η παρανομία στην έρευνα αλλά το δικαστήριο της ουσίας δεν στήριξε την κρίση του στην έρευνα αλλά στην κατάθεση του ... *ερευνητή* (αστυνομικού), ελέγχεται ικανοποιητική ως εξήγηση, κείθεν δε η απόφαση κρίνεται ότι διέλαβε την ειδική κι εμπεριστατωμένη αιτιολόγηση που απαιτεί το Σύνταγμα, απορρίπτοντας το σχετικό παράπονο του κατηγορουμένου.

Ουσιαστικά με τον τρόπο αυτόν έχουμε μια πολυεπίπεδη προσβολή των ατομικών δικαιωμάτων του κατηγορουμένου, τόσο στο αμιγώς δικονομικό πεδίο με την προσβολή των υπερασπιστικών του δικαιωμάτων, όσο και στο ουσιαστικό νομικό πεδίο, εκείνο των προσωπικών του δεδομένων, της σχετικής ατομικής ελευθερίας στον σεβασμό της αξίας του ανθρώπου αλλά και ειδικότερα στην προστασία του απορρήτου της επικοινωνίας του.

Διατυπώθηκε η άποψη ότι το εγκληματικό περιεχόμενο[368] μιας επικοινωνίας τηλεφωνικής ή ηλεκτρονικής, δεν μπορεί να τύχει προστασίας από το θεσμικό νομικό πλαίσιο του αρ. 19 Συντ, Ν 3115/2003, ΠΔ 47/2005, Ν 3471/2006 καθόσον το εγκληματικό περιεχόμενο από μόνο του δεν μπορεί να προστατεύεται από το νόμο, την στιγμή που το ίδιο είναι εγκληματικό. Κατ' επέκταση, σύμφωνα με την άποψη αυτήν, δεν υπάρχει νομική βάση στην αποτροπή αξιοποίησης οπωσδήποτε συλλεγέντος αποδεικτικού υλικού και μάλιστα δεν

[366] Βλ. ενδεικτικά από την πληθώρα της νομολογίας ΑΠ 962/2013, ΑΠ 1415/2013, ΒΔ Νόμος.
[367] Βλ. *Αθ. Γιαννακούλα, Μ. Μηλαπίδου*, Προσωπικά Δεδομένα (σειρά Ειδικοί Ποινικοί Νόμοι, υπό τη Διεύθυνση Μ. Καϊάφα – Γκμπάντι και Ελ. Συμεωνίδου – Καστανίδου), Νομική Βιβλιοθήκη, 2017, σελ. 118.
[368] Λ.χ. απειλητικό, παραπλανητικό, εξυβριστικό ή δυσφημιστικό.

πρέπει να τίθεται προβληματισμός αναφορικά με την ενεργοποίηση διαδικασιών αποκάλυψης στοιχείων της επικοινωνίας[369].

Φυσικά μια τέτοια προσέγγιση του προβληματισμού δεν με βρίσκει σύμφωνο. Η πρώιμη αξιολόγηση και χαρακτηρισμός μιας επικοινωνίας ως αξιόποινης στην βάση του ότι απλά ως τέτοια την έχει καταγγείλει κάποιος, δεν μπορεί να είναι επαρκές νομικό έρεισμα για την αποδέσμευση όλου του θεσμικού προστατευτικού πλαισίου κείθεν δε την πλήρη έκθεση των στοιχείων της επικοινωνίας.

Ακόμη και αν αποδειχθεί ακριβής και αληθινή η καταγγελία και πάλι αυτό δεν μπορεί να αιτιολογήσει νομικά και να δικαιολογήσει τεχνικά το πρωθύστερο στην σχετική συλλογιστική. Εξ άλλου μια τέτοια προσέγγιση θα κατέλυε κάθε έννοια δικαστικής κρίσης και θα λειτουργούσε σε βάρος της αρχής του τεκμηρίου της αθωότητας.

[369] Βλ. *Αθ. Γιαννακούλα, Μ. Μηλαπίδου*, Προσωπικά Δεδομένα (σειρά Ειδικοί Ποινικοί Νόμοι, υπό τη Διεύθυνση Μ. Καϊάφα – Γκμπάντι και Ελ. Συμεωνίδου – Καστανίδου), Νομική Βιβλιοθήκη, 2017, σελ. 124.

12. ΣΥΜΠΕΡΑΣΜΑΤΑ – ΤΕΛΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ

Από την ανάπτυξη και τους προβληματισμούς που εκτέθηκαν στις προηγούμενες ενότητες, καθίσταται ξεκάθαρο ότι η ερευνητική πρόκληση για την εκπόνηση της μελέτης, στηρίχθηκε στην παραδοχή ότι το Διαδίκτυο και οι τεχνολογίες αιχμής επηρεάζουν τους τρόπους τέλεσης αξιοποίνων πράξεων, εγκαθίδρυσαν και διαμορφώνουν νέες μορφές εγκληματικής συμπεριφοράς και επηρέασαν τους τρόπους απόδειξης ενώπιον των δικαστηρίων. Με το ζήτημα της εναρμόνισης των εθνικών δικαίων ασχολήθηκε το Συμβούλιο της Ευρώπης και ειδικότερα η Ευρωπαϊκή Επιτροπή νομικής συνεργασίας[370], που πραγματοποίησε συγκριτική μελέτη σχετικά με αυτό το ζήτημα (κυρίως σε τομείς αστικών και διοικητικών διαδικασιών).

Η ενσωμάτωση στον Κ.Ποιν.Δ. της διάταξης του άρθρου 265 αναφορικά με την κατάσχεση των ψηφιακών πειστηρίων, συντεταγμένη στις προτάσεις και τα νομικά πλαίσια που διαμορφώθηκαν με το Ν 4411/2016, που με την σειρά του ικανοποίησε τις απαιτήσεις συμμόρφωσης με την Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και το Πρόσθετο Πρωτόκολλό της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών, που συνιστά μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών, διαμόρφωσε ένα νέο πλαίσιο ερευνητικής δράσης στην εξιχνίαση και κυρίως στην δικαστική (αποδεικτική) αξιοποίηση των ψηφιακών ευρημάτων.

Η νέα διάταξη έρχεται να δώσει σαφές πεδίο δράσης των ερευνητικών δομών, πάντα προς τον σκοπό της εξεύρεσης της ουσιαστικής αλήθειας. Με τον τρόπο αυτόν αναδεικνύεται ακόμη περισσότερο η παραδοχή ότι σημαντική πληροφορία στην έρευνα δίνει το ψηφιακό στίγμα της καθημερινότητας του ανθρώπου, όπως αυτή έχει διαμορφωθεί από την ενσωμάτωση των τεχνολογιών αιχμής και των ηλεκτρονικών εφαρμογών επικοινωνίας και κοινωνικής επαφής στην ατομική καθημερινότητα. Από το στίγμα δράσης ενός απλού δρομέα κατά την προπόνησή του, μέχρι την μεταφορά αρχείων κειμένου ή εικόνας – ήχους για λόγους επαγγελματικούς ή ψυχαγωγίας, οι όροι της επικοινωνίας και της καθημερινής

[370] Βλ. Counsil of Europe/European Committee on Legal Co-operation, https://www.coe.int/en/web/cdcj/-/electronic-evidence

δράσης, πλέον είναι ψηφιακοί και τείνουν να καταστούν αποκλειστικά τέτοιοι. Αυτά τα ίχνη δημιουργούν νέες δομές δεδομένων, που με την σειρά τους είναι αξιοποιήσιμα στοιχεία στην απόδειξη σε όλους τους δικαιϊκούς τομείς.

Ανεξάρτητα από τον βαθμό αξιολόγησης που έλαβαν ως αποδείξεις σε υποθέσεις, που αναφέρθηκαν παραπάνω, σε διάφορες ενότητες και με παραδείγματα από τη νομολογία (κυρίως σε διεθνές επίπεδο) αλλά και από την ερευνητική πρακτική, αναδείχθηκε σε κάθε περίπτωση η σημασία που διαδραματίζουν πλέον στον τομέα της δικαιικής απόδειξης, όπου αποδεικτικές λύσεις δόθηκαν με την αξιοποίηση πληροφορίας από τα ψηφιακά δεδομένα που προκύπτουν από την καθημερινή ατομική ψηφιακή δράση. Βέβαια, επίσης με παραδείγματα αλλά και με την ερευνητική αναφορά, τονίστηκε η ευμεταβλητότητα των ψηφιακών δεδομένων και ο κίνδυνος διαμόρφωσης μιας ψευδούς εικόνας για τα πραγματικά περιστατικά, στην περίπτωση που δεν γίνεται ασφαλής δέσμευση των ψηφιακών υποδοχέων και ασφαλής ανάλυση των ψηφιακών δεδομένων.

Αυτή η διαπίστωση με την σειρά της οδήγησε στους προβληματισμούς αναφορικά με όλα τα διαδικαστικά στάδια από τον εντοπισμό, την κατάσχεση μέχρι και την άντληση των ψηφιακών δεδομένων και την μετέπειτα αξιολόγηση και ανάλυσή τους προκειμένου να αξιοποιηθούν αποδεικτικά.

Κάπου εκεί εντοπίστηκαν και οι σχετικοί προβληματισμοί, που θέτουν οι αντίρροπες δυνάμεις που δημιουργούνται στην βάση των διαφορετικών προσεγγίσεων από την μια των τεχνολογιών αιχμής στον τομέα της ηλεκτρονικής επικοινωνίας, από την άλλη στις νομικές δυνατότητες έρευνας, που παρέχονται στον ανακριτικό υπάλληλο σύμφωνα με τις κείμενες διατάξεις που ρυθμίζουν την έρευνα και εκ τρίτου από το πλαίσιο που διαμορφώνεται για τα προσωπικά δεδομένα και τις ατομικές ελευθερίες στο έδαφος των δεσμεύσεων από την Σύμβαση για τα δικαιώματα του ανθρώπου και τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR).

Η ερευνητική πρόκληση έφτασε το σημείο αιχμής στην περίπτωση της διαχείρισης των ζητημάτων που θέτει η παροχή υπηρεσιών νεφοϋπολογιστικής, όπου λειτουργούν δομές παγκοσμιότητας, που ανατρέπουν σε μεγάλο βαθμό τις παραδοσιακές προσεγγίσεις του εδαφικού εντοπισμού άσκησης αρμοδιοτήτων, στην βάση των ευρημάτων αλλά και του τόπου τέλεσης της αξιόποινης πράξης που είναι το αντικείμενο της ανακριτικής έρευνας.

Στην βάση των θέσεων που εκτέθηκαν ανωτέρω, σημαντικό πεδίο προβληματισμού αφορά στην άσκηση των δικαιωμάτων του κατηγορουμένου, ιδία αναφορικά με το

διαμορφούμενο απαγορευτικό πεδίο σχετικά με την πρόσβαση, αναπαραγωγή και αντιγραφή του ψηφιακού αρχείου - ασφαλούς αντιγράφου των ψηφιακών δεδομένων - (digital copy) που ενσωματώνεται στην ποινική δικογραφία που σχηματίζεται.

Εξ άλλου όλη η μελέτη πλαισιώθηκε από την αντίπαλη συνθήκη που δημιουργείται στην βάση της διασφάλισης των αποδείξεων από τη μια και στην τήρηση του νομικού πλαισίου που εξασφαλίζει τον σεβασμό των ανθρωπίνων δικαιωμάτων, όπως αυτά συμπεριλήφθηκαν στην Σύμβαση της Ρώμης και νομολογιακά καθορίστηκαν από το ΕΔΔΑ.

Κατά κύριο λόγο επιχειρήθηκε η ανάπτυξη των προβληματισμών, ώστε να αναδειχθούν τα φλέγοντα σημεία, τα οποία θα επιτρέψουν την διαμόρφωση προτάσεων για την εξεύρεση λύσεων που θα καλύπτουν το ιδιαίτερα απαιτητικό πεδίο της ψηφιακής εγκληματολογίας και της αποδεικτικής αξιοποίησης των ευρημάτων στο περιβάλλον της ποινικής δίκης.

Προτείνονται μικρές τροποποιήσεις στην υφιστάμενη δομή της διάταξης του άρθρου 265 Κ.Ποιν.Δ. Πρώτα και κύρια μια προσθήκη της μορφής του κατηγορουμένου στον κύκλο των προσώπων που έχουν πρόσβαση στο ασφαλές αντίγραφο των ψηφιακών δεδομένων (digital copy) θα λύσει οποιαδήποτε σχετική διχογνωμία αναφορικά με την έκταση των δικαιωμάτων του και θα άρει ενδεχόμενες αντίθετες σκέψεις του επικεφαλής της ανακριτικής έρευνας, αναφορικά με το κατά πόσον η μη αναφορά του κατηγορουμένου στα πρόσωπα διαχείρισης και φύλαξης του digital copy αποκλείει τον κατηγορούμενο από τα γενικά υπερασπιστικά του δικαιώματα. Με την ρητή αναφορά του κατηγορουμένου θα αποτρέπεται η επιβάρυνση του επικεφαλής της ανακριτικής έρευνας με την ενασχόληση του με την επίλυση ζητημάτων που θα αφορούν χορήγηση ή μη άδειας στον κατηγορούμενο για πρόσβαση στο ψηφιακό υλικό.

Ζητήματα αναφορικά με τις υπηρεσίες νεφοϋπολογιστικής πρέπει πρώτα και κύρια να αντιμετωπιστούν σε επίπεδο διεθνούς συνεργασίας αλλά και νομοθεσίας που θα επιβάλλει στους παρόχους την δέσμευση διατήρησης δεδομένων, τουλάχιστον για ένα διάστημα 30 ημερών μετά από κάθε εντολή διαγραφής από τον χρήστη της υπηρεσίας, με την λήψη βέβαια κατάλληλων τεχνικών και οργανωτικών μέτρων διασφάλισης τόσο της ακεραιότητας του δεδομένου όσο και με της μη δημοσιοποίησής του πέρα από την αρχή που βάσει θεσπισμένου νομικού πλαισίου θα επιτρέπει μια τέτοια διαβίβαση.

Αυτό το πλαίσιο δράσης σαφώς και απαιτεί διεργασίες στη βάση τόσο της νομικής ετοιμότητας όσο και των ισορροπιών πολιτικής υφής αναφορικά με τους παρόχους και την

εμπορική διάσταση της προσφοράς στον τομέα των υπηρεσιών νεφοϋπολογιστικής. Σαφώς κάτι τέτοιο απαιτεί δομές συντονισμού που φαντάζουν χρονοβόρες και ίσως αποτελέσουν πεδίο αντιπαράθεσης των συνεργαζομένων κρατών αναφορικά πάντα και με τα συμφέροντα που εξυπηρετούνται από την τελική, κάθε φορά, επιλογή. Φυσικά όλες οι προσεγγίσεις στόχο έχουν την διατήρηση κι ενδυνάμωση της χρήσης των υπηρεσιών αυτών και όχι την αποτροπή των χρηστών στην βάσει ενδοιασμών αναφορικά με την προστασία της ιδιωτικότητάς τους κατά την χρήση στο διαδίκτυο. Μια λύση περιορισμού του περιορισμού, στα πλαίσια της συμμόρφωσης προς την αρχή της αναλογικότητας που φαίνεται ότι πλέον διαπνέει όλους τους τομείς του δικαίου και μάλιστα σε διεθνές επίπεδο, θα ήταν η λειτουργία του μέτρου περιορισμένα σε ειδικές κατηγορίες διακίνησης αρχείων, όπως της πορνογραφίας ανηλίκων ή της διακίνησης αρχείων που αφορούν την εθνική ασφάλεια.

Στο πλαίσιο των προτάσεων αυτών θα πρέπει κατ' αναπόδραστη συνθήκη, να εντάξουμε και τις τεχνολογίες που αφορούν την διασύνδεση πραγμάτων, που θα επιτρέπουν την διαχείριση των ψηφιακών πειστηρίων με την μικρότερη δυνατή ανθρώπινη παρέμβαση. Η ενεργοποίηση της τεχνολογίας των Internet of things (IoT) θα ενισχύσει την αποτελεσματικότητα της έρευνας, τουλάχιστον στον τομέα της εξόρυξης των δεδομένων από τα ψηφιακά πειστήρια. Με την επιτάχυνση των διαδικασιών εξόρυξης, που σαφώς μπορούν να γίνονται με τρόπο ασφαλή, θα επιτευχθεί ο περιορισμός της απασχόλησης του ειδικού προσωπικού, ώστε να διοχετεύεται ο σχετικός ερευνητικός πόρος σε περισσότερες υποθέσεις και συνεπώς να αποφεύγεται η σημερινή συνθήκη που δημιουργεί χρονική καθυστέρηση στην εξέλιξη της ποινικής δίκης.

Περαιτέρω με τις μελέτες αναφορικά με την ανάπτυξη του τομέα της Τεχνητής Νοημοσύνης (Artificial Intelligence), η διαχείριση και του τομέα της ανάλυσης των ψηφιακών δεδομένων, που αντλήθηκαν, δεν θα είναι μακριά μια νέα μορφή τεχνικής έρευνας. Στην παρούσα φάση δεν θα μπορούσα να υποστηρίξω την αντικατάσταση του ερευνητή από μια δομή λειτουργίας τεχνητής νοημοσύνης και τούτο διότι δεν διαθέτω προσωπικά, αλλά και δεν εντόπισα στην έρευνά μου, τα εχέγγυα εκείνα που επιτρέπουν την αφαίρεση του ανθρωπίνου παράγοντα από το τελικό προϊόν της παραγωγικής αυτής διαδικασίας, που είναι η παρουσίαση των πορισμάτων της έρευνας. Κατά λογική ακολουθία, μια τέτοια προσέγγιση μπορεί να αποτελέσει μελλοντικό αντικείμενο της έρευνας, ώστε να επιτευχθεί ο αντίστοιχος εμπλουτισμός της μελέτης.

Προτάθηκε, παραπέρα, σε προηγούμενη θέση, η ψηφιακή κάλυψη του σταδίου της κατάσχεσης, από την αρχική επέμβαση των ανακριτικών υπαλλήλων μέχρι και την σφράγιση

των κατασχεθέντων πειστηρίων. Όπως αναφέρθηκε και στο σημείο της πρώτης καταγραφής, αυτό που φαντάζει ως υπερβολή, το μεν είναι μια ανέξοδη προσθήκη, το καλύπτει ζητήματα που πολλές φορές απασχόλησαν τη νομολογία, λειτουργεί δε προς εξασφάλιση πρωτίστως της ακρίβειας στην έρευνα αλλά και αποδυναμώνει κάθε σκέψη για εκκωφαντικούς αλλά κενούς ουσίας, ισχυρισμούς του κατηγορουμένου σε βάρος της ανακριτικής διαδικασίας. Δεν εκθέτει η πρόταση αυτή την αστυνομική δράση, αλλά μάλλον την ασφαλίζει και την ανυψώνει θεσμικά.

Σε όλες τις σκέψεις που προηγήθηκαν είναι ξεκάθαρη η σύγκρουση μεταξύ της διατήρησης της ασφάλειας στην κοινότητα από τη μια πλευρά και των ατομικών ελευθεριών από την άλλη, μέσα κυρίως από αναφορές στον σκληρό πυρήνα του δικαιώματος συμμετοχής στην κοινωνία της πληροφορίας. Φυσικά η αντιπαράθεση αυτή δεν είναι μια καινοτόμος συνθήκη αλλά μια καινούργια μορφή της ουσιαστικής αντιπαλότητας μεταξύ των ορίων κοινωνίας και ατόμου, που σαφώς έχει απασχολήσει πολλαπλώς και πολυεπίπεδα από τις απαρχές της λειτουργίας των κοινωνικών δομών.

Ας είναι λοιπόν η βάση αυτή που, με ειδικότερες αναφορές και προεκτάσεις στο αντικείμενο της μελέτης αυτής, θα επιτρέψει μια νέα μου ενασχόληση, με την διαμόρφωση ενός πλαισίου μέσα από την ηθική στην τεχνολογία.

Σας ευχαριστώ όλους του δασκάλους μου
Θεόφιλος Παιδάμωνας

ΒΙΒΛΙΟΓΡΑΦΙΑ
-αρθρογραφία

Ι. Ελληνική

1. *Ι. Αγγελής*, Διαδίκτυο και ποινικό δίκαιο, ΠοινΧρον 2000, σελ. 676,
2. *Ι. Αγγελής*, Ηλεκτρονικό έγκλημα και απονομή της ποινικής δικαιοσύνης, ΠοινΔικ 2005, σελ. 1062 επ.,
3. *Δ.Π. Αγγελόπουλος*, Ψηφιακά Πειστήρια, Γενικές Αρχές – Χειρισμός, http://www.elesme.gr /elesmegr /periodika/t16/t16_5.htm
4. *Β. Αδάμπας/ Μ. Παπαχρήστου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, τομ. Α, Νομική Βιβλιοθήκη 2018,
5. *Β. Αδάμπας/ Χ. Αθανασίου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, Νομική Βιβλιοθήκη 2018,
6. *Στ. Αλεξιάδης*, το τεκμήριο αθωότητας του κατηγορουμένου, ΕΕΕυρΔ 1986, σελ. 52,
7. *Ν. Ανδρουλάκης*, Κώδικας Ποινικής Δικονομίας, Π.Ν. Σάκκουλας/Δίκαιο και Οικονομία 2015,
8. *Ν. Ανδρουλάκης*, Θεμελιώσεις έννοιες της ποινικής δίκης, Π.Ν. Σάκκουλας 2007,
9. *Ν. Ανδρουλάκης*, Τα όρια της ανακριτικής δράσεως και η αρχή της «αναγκαιότητας», ΠοινΧρον 1975, σελ. 15 επ.
10. *Μ. Γεωργιάδου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, τομ. Α, Νομική Βιβλιοθήκη 2018,
11. *Αθ. Γιαννακούλα, Μ. Μηλαπίδου*, Προσωπικά Δεδομένα (σειρά Ειδικοί Ποινικοί Νόμοι, υπό τη Διεύθυνση Μ. Καϊάφα – Γκμπάντι και Ελ. Συμεωνίδου – Καστανίδου), Νομική Βιβλιοθήκη, 2017, σελ. 118
12. *Δ. Γιαννουλόπουλος*, Η γνωστοποίηση του δικαιώματος σιωπής στον κατηγορούμενο και η ανάγκη εναρμόνισης της ελληνικής νομοθεσίας με το διεθνές και συγκριτικό δίκαιο, ΠοινΔικ 2012, 640.
13. *Αν. Γκιουζέπας*, ΓΕΕΘΑ/Διεύθυνση Κυβερνοάμυνας στο 2ο Ετήσιο Συνέδριο Ασφάλειας Ψηφιακών Συστημάτων, 2016, https://www.youtube.com/watch?v=48gLcE_-dQY&t=410s,
14. *Ν. Δαγκλής*, Η αποδεικτική και διαγνωστική ελευθερία του ποινικού δικαστή σε ζητήματα που απαιτούν ειδικές γνώσεις: Εγγύηση ή ανάχωμα στην διερεύνηση του ηλεκτρονικού εγκλήματος σε Θ. Δαλακούρα, Το ηλεκτρονικό έγκλημα, Νομική Βιβλιοθήκη 2019, σελ. 188 επ.,
15. *Θ. Δαλακούρας*, Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν 4411/2016), σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019,
16. *Θ. Δαλακούρας*, Ο νέος Κώδικας Ποινικής Δικονομίας, Συνοπτική κατ' άρθρο ερμηνεία Ν 4620/2019, ΝομΒιβλ 2019,
17. *Θ. Δαλακούρας*, Οι ειδικές ανακριτικές πράξεις του άρθρου 6 του Ν 2928/2001, ΠοινΧρ 2001, 1022,
18. *Θ. Δαλακούρας*, Η ανακριτική διαδικασία στα εγκλήματα διαφθοράς. Όρια επέμβασης στα δικαιώματα του ατόμου υπό το φως της ΕΣΔΑ, ΠοινΔικ 2016, 1105.
19. *Θ. Δαλακούρας*, Επεμβάσεις στον ΚΠΔ, Ο μύθος της επιτάχυνσης της απονομής της ποινικής Δικαιοσύνης, ΠοινΧρ 2016, 326,
20. *Θ. Δαλακούρας*, Ειδικές ανακριτικές πράξεις κατ' αρ. 253 Α ΚΠΔ και ηλεκτρονικό έγκλημα, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2018, 247 επ.,

21. *Θ. Δαλακούρας*, Αρχή της αναλογικότητας και μέτρα δικονομικού καταναγκασμού, Αντ. Σάκκουλας 1993, σελ. 240,
22. *Θ. Δαλακούρας*, Οι Ακυρότητες στο ποινικοδικονομικό μας σύστημα, σε Θ. Δαλακούρα, Ηλεκτρονικό έγκλημα, νομική βιβλιοθήκη 2019, 23 επ.
23. *Θ. Δαλακούρας*, Ποινικό Δίκαιο τόμος Ι, 2012,
24. *Σ. Δασκαλόπουλος*, Η προκαταρκτική εξέταση και η άσκηση ποινικής δίωξης κατά το Ν 3160/2003, ΠοινΧρον 2003, 1027 επ.,
25. *Δ. Ζημιανίτης*, Το πράσινο βιβλίο της Ευρωπαϊκής Επιτροπής για «τις δικονομικές εγγυήσεις υπέρ υπόπτων και κατηγορουμένων σε ποινικές διαδικασίες σε ολόκληρη την ΕΕ», ΠοινΔικ 2003, σελ. 443 επ.
26. *Μ. Καϊάφα – Γκμάντι*, Η πρόσφατη νομολογία του ΕΔΔΑ για την αστυνομική διείσδυση και το δικαίωμα σε δίκαιη δίκη, ΠοινΧρον 2011, 59 επ.,
27. *Π. Καίσαρης/Σπ. Παππάς*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 156 επ.,
28. *Π. Καίσαρης/Σ. Τσάκος*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 1320-1
29. *Γ. Κακαβούλης*, Η ανωνυμία στο Διαδίκτυο, https://www.homodigitalis.gr/posts/1908.
30. *Ειρ. Καμπερίδου*, Ψηφιακές δεξιότητες και ψηφιακός αποκλεισμός: Γεφυρώνοντας το έμφυλο ψηφιακό χάσμα (Digital skills and digital exclusion: Bridging the gender digital divide), αλλά και γενικότερα σε πρακτικά 6ου Τακτικού Συνεδρίου της ΕΚΕ, «Η Κοινωνιολογία και ο Δημόσιος Ρόλος της στην Εποχή της Μεταμόρφωσης του Κόσμου», Ελληνική Κοινωνιολογική Εταιρεία, 2018,
31. *Αλ. Καργόπουλος*, Ανακριτικές πράξεις επί ψηφιακών δεδομένων: Δικαιικοί άξονες και προβληματισμοί, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019,
32. *Ε. Καρρά – Τανισκίδου*, Δικανική Υπολογιστών (ComputerForensics), 2014, https://core.ac.uk/ download/pdf/38466068.pdf
33. *Αργ. Καρράς*, Ποινικό Δικονομικό Δίκαιο, εκδ. ε΄ 2017, εκδ. ε΄,
34. *Αργ. Καρράς*, Η αναίρεση στην Ποινική Δίκη, εκδ. Σάκκουλα, Αθήνα – Θεσσαλονίκη 2013,
35. *Β. Κάτος*, Ψηφιακά Πειστήρια, σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019,
36. *Δ. Κιούπης*, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος σε Θ. Δαλακούρα το Ηλεκτρονικό έγκλημα, εκδ ΝομΒιβλ 2019,
37. *Δ. Κιούπης*, Δημοσίευση ιστοσελίδων με αξιόποινο περιεχόμενο, ΠοινΛογ 2001, 398,
38. *Δ. Κιούπης*, Ποινικό Δίκαιο και internet, σειρά ΠΟΙΝΙΚΑ, Νο 57,
39. *Γ. Κιστάκις*, Η ανωνυμία στο Διαδίκτυο, https://www.kathimerini.gr/726387/ opinion/epikairothta/arxeio-monimes-sthles/h-anwnymia-sto-diadiktyo,
40. *Αθ. Κονταξής*, Κώδικας Ποινικής Δικονομίας, Συνδυασμός θεωρίας και πράξης, α΄ τομ., Δ΄ εκδ., 2006,
41. *Γ. Κουρβούλης*, Computer & Network, Εύρεση, ανάλυση ψηφιακών πειστηρίων σε υπολογιστές και δίκτυα (computer forensics), 2011 http://doccdn.simplesite.com/d/5e/99/282319406962284894/605fd94f-ab02-4248-823c-0351d371acb1 /KourvoulisGeorgiosMsc2011.pdf,
42. *Γ. Κωνσταντάς*, Εγκληματολογική εξέταση ψηφιακών πειστηρίων, 2016, https://www.forensicssociates.gr /el/psifiaka-peistiria,
43. *Ν. Λίβος*, Η διεξαγωγή διοικητικών και ανακριτικών ερευνών από το Σώμα Δίωξης Οικονομικού Εγκλήματος (ΣΔΟΕ), σε Ι. Φωτόπουλου, Φορολογικές Κυρώσεις, 2002, 119,

44. *Ν. Λίβος*, «Πολύ κακό για το τίποτα»; Οι ανακριτικές αρμοδιότητες της Αρχής Καταπολέμησης της Νομιμοποίησης Εσόδων από Εγκληματικές Δραστηριότητες, ΠοινΧρον 2006, 380,
45. *Ν. Λίβος*, Το Οργανωμένο έγκλημα, έννοια και δικονομικοί τρόποι αντιμετώπισης του, σε Το οργανωμένο έγκλημα από τη σκοπιά του ποινικού δικαίου, Πρακτικά Ζ' Πανελ. Συνεδρ. ΕΕμπΔ 2000,
46. *Λ. Μαργαρίτης*, Νέος Κώδικας Ποινικής Δικονομίας, Αιτιολογική έκθεση Ν 4620/2019, Νομική Βιβλιοθήκη, σελ. 383,
47. *Λ. Μαργαρίτης*, Οι δικονομικού περιεχομένου διατάξεις του Ν 2408/1996, Υπερ 1997, 519,
48. *Λ. Μαργαρίτης*, Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου και Ελληνική Ποινική Δίκη, σε «Εμβάθυνση στην Ποινική Δικονομία», τ. Ι, 2006,
49. *Γ. Μπουρμάς*, Η νομιμότητα των ερευνών σε ηλεκτρονικά δίκτυα και δεδομένα στις περιπτώσεις εγκλημάτων στον κυβερνοχώρο, ΠοινΔνη 2019, σελ. 557,
50. *Π. Μπρακουμάτσος*, Ερμηνευτικές παρατηρήσεις και προτάσεις στο Ν 2408/1996, ΠοινΧρον 1996, 1193,
51. *Γ. Νούσκαλης*, Κατοχή και διανομή/διάθεση πορνογραφικού υλικού ανηλίκων (άρθρο 348 Α ΠΚ): Η νομολογιακή προσέγγιση κρισίμων ζητημάτων ουσιαστικού και δικονομικού δικαίου σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη 2019, σελ. 86,
52. *Γ. Νούσκαλης*, Παιδική πορνογραφία, ΠοινΔνη 2006, 161,
53. *Γ. Νούσκαλης*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, τομ. Ι, Νομική Βιβλιοθήκη 2018, σελ. 555,
54. *Π. Παναγιωτόπουλος*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, Ερμηνεία κατ' άρθρο, τομ. Α, σελ. 1535 επ.,
55. *Αδ. Παπαδαμάκης*, Προκαταρκτική εξέταση – προανάκριση: Μορφές και όρια της ερυενητικής δραστηριότητας, ΠοινΔικ 2008, 338 επ.,
56. *Π. Παπανδρέου*, Η Προκαταρκτική εξέταση, ΠοινΔικ 2006, 191,
57. *Π. Παπανδρέου*, Η ποινική δίωξη, ΠοινΔικ 2006, 439,
58. *Π. Παπανδρέου*, Η περάτωση της προανάκρισης, ΠοινΔικ 2006, 1287,
59. *Π. Παπανδρέου*, σε Λ. Μαργαρίτη, Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, τομ Ι, 2η έκδοση, Νομική Βιβλιοθήκη, 2018, σελ. 989,
60. *Σ. Πετρίδου*, ΤΠΕ – το πρωτόκολλο του Παγκόσμιου ιστού HTTP,
61. *Σ. Πετρίδου*, Διαρροή Προσωπικών Δεδομένων: Ζητήματα Ασφάλειας, σε Τεχνολογίες Πληροφορικής κι Επικοινωνιών/Compus/Uom.
62. *Χ. Σεβαστίδης*, Κώδικας Ποινικής Δικονομίας, ερμηνεία κατ' άρθρο, 2015 τ. ΙΙΙ, σελ. 2798.,
63. *Δ. Σπανός, Α. Σοφός, Β. Οικονόμου,* Οι συνέπειες ως προς τον ψηφιακό γραμματισμό των μαθητών σε περιβάλλον ενός φορητού υπολογιστή ανά μαθητή, https://economu.wordpress.com/11-2/,
64. *Ελ. Συμεωνίδου – Καστανίδου,* Αστυνομική Βία: Νομικό πλαίσιο και προβλήματα εφαρμογής, ΝοΒ 2006, σελ. 1641,
65. *Θ. Τάσης*, Ψηφιακός Ανθρωπισμός, Εικονιστικό υποκείμενο και τεχνητή νοημοσύνη, εκδ. Αρμός 2019. *Th. Porter*, History of Psychology, Vol 21(4), Nov 2018, 369-373,
66. *Γρ. Τσόλιας*, Οι ελεγκτικές αρμοδιότητες της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Μια πρώτη προσέγγιση), ΔiΜΕΕ 2005, 539,
67. *Ν. Χωραφάς*, Ποινικόν Δίκαιον, τομ. 1ος, εκδ. 9η, 1978,

I. Ξενόγλωσση

1. *Ak. Ajijola, P. Zavarsky, R. Ruhl*, A Review and Comparative Evaluation of Forensics, Guidelines of NIS T SP 800-101 Rev. 1:2014 and ISO/IEC 27037:2012
2. *Alvarez, Lizette* (July 18, 2011). "Software Designer Reports Error in Anthony Trial". nytimes.com/. Retrieved, July 18, 2011. https://en.wikipedia.org/wiki/Death_ of_Caylee_Anthony#Opening_statements_ and_witness_testimony,
3. *R. Anderson, Chr. Barton, R. Boehme, R. Clayton, M. J.G. van Eeten, M. Levi, T. Moore, St. Savage*, Measuring the Cost of Cybercrime, https://www.econinfosec.org/archive/weis2012 /papers/Anderson_WEIS2012.pdf,
4. *R. Anderson, R. Boehme, R. Clayton, and T. Moore*. Security Economics and the Internal Market. January 2008, http://www.enisa.europa.eu/act/sr/reports/ econ-sec/economics-sec,
5. *Ali Alkaabi, G. Mohay, Adr. McCullagh, and N. Chantler*, Dealing with the Problem of Cybercrime, σε Digital Forensics and Cyber Crime, Second International ICST Conference ICDF2C 2010 Abu Dhabi, UnitedArab Emirates, October 4-6, 2010, σελ. 12 επ.
6. *Silvia Barnová, Slávka Krásna*, Digital Humanism in Education – Meaningful Use of Digital Technologies, 2nd International EMI Entrepreneurship & Social Sciences Congress, 09-11 November 2018, Cappadocia, https://www.researchgate.net/profile/Silvia_ Barnova/publication/330345608_Digital_Humanism_in_Education_-_Meaningful_Use_of_ Digital_Technologies/links/5c3a15efa6fdccd6b5a752ec/Digital-Humanism-in-Education-Meaningful-Use-of-Digital-Technologies.pdf,
7. *C. Brown*, «Computer Evidence: Collection & Preservation.» Hingham, Thomson/Delmar, 2006,
8. *J. Brunty*, «Validation of Forensic Toolsand Software, «A Quick Guide for the Digital Forensic Examiner», 2011, https://www.researchgate.net/profile/Josh_Brunty/ publication/320808735_Validation_of_ Forensic_Tools_and_Software_A_Quick_Guide_for _the_Digital_Forensic_Examiner/links/5e2f0643a 6fdcc309 6941501/Validation-of-Forensic-Tools-and-Software-A-Quick-Guide-for-the-Digital-Forensic-Examiner.pdf,
9. *Canalys Inc.* Enterprise security market to exceed $22 billion in 2012, December 2011. http://www.canalys.com/static/press_release/2011/canalys-pressrelease-201211-enterprise-security-market-exceed-22-billion-2012.pdf, Communications Fraud Control Association. 2011 global fraud loss survey. http://www. cfca.org/fraudlosssurvey/, 2011,
10. *B. Carrier*, «Defining digital forensic examination and analysis tools», International Journal of Digital Evidence 1, 2003, σελ. 2 επ. σε http://citeseerx.ist.psu.edu/ viewdoc/download?doi=10.1.1.14.9813&rep=rep1& type=pdf
11. *E. Casey*, Digital Evidence and Computer Crime, https://www. semanticscholar.org/paper/Digital-Evidence-and-Computer-Crime-Casey/8c28fbef0af2d0 b0dfb772c82a8059e9094eb4c3,
12. *S. E. Goodison, R. C. Davis, and Br. A. Jackson*, Digital Evidence and the U.S. Criminal Justice System, Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf,
13. *M.U. Farooq, M. Waseem, Anj. Khairi, S. Mazhar*, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)", International Journal of Computer Applications (0975 8887), Volume 111 - No. 7, February 2015,
14. *D. Gray*, Data Ownership In The Cloud, σε https://dataconomy.com/2014/03/data-ownership-in-the-cloud/,
15. *Cl. Hewson, D.W. Stewart*, Internet Research Methods, 2016, https://onlinelibrary.wiley.com/ doi/full/10.1002/9781118445112.stat06720.pub2, D. Miller and D. Slater, The Internet, An

Ethnographic Approach, Oxford 2000, https://dourish.com/~dourishc/classes/readings /MillerSlater-InternetChapter1.pdf, https://el.wikipedia.org/wiki,

16. *R.W Hockney, C.R Jesshope*, Parallel Computers 2: Architecture, Programming and Algorithms, https://books.google.gr/books?hl=el&lr=&id=7ZKpDwAAQBAJ&oi=fnd&pg=PP9&dq=computers&ots=D1JyJyHoLr&sig=viqiosf2r2tI6H7rdb4sNRCs4mU&redir_esc=y#v=onepage&q=computers&f=false,
17. *Gr. Horsman*, ACPO principles for digital evidence: Time for an update?, February 2020, Forensic Science International: Reports https://www.sciencedirect.com/science/article/pii/S2665910720300220
18. *A. Huseinović, S. Mrdović*, «Comparison of Computer Forensics Investigation Models for Cloud Environment», http://people.etf.unsa.ba/~smrdovic/publications/MIPRO2018_Huseinovic_Mrdovic.pdf,
19. *C. Johnston*, A county's only unsolved murder has a victim without a digital footprint, https://arstechnica.com/tech-policy/2014/05/a-countys-only-unsolved-murder-has-a-victim-without-a-digital-footprint/,
20. *Ar. Karataş, S. Şahin,* A Review on Social Bot Detection Techniques and Research Directions, 2016, σε https://www.researchgate.net/profile/Serap_Sahin2/publication/322853694_AReview_on_Social_Bot_Detection_Techniques_and_Research_Directions/links/5a72d272a6fdcc53fe131e99/A-Review-on-Social-Bot-Detection-Techniques-and-Research-Directions.pdf,
21. *St Levy*, Hackers: Heroes of the Computer Revolution, 1984,
22. *D. Lupton*, Feeling your data: Touch and making sence of personal digital data, New Media and Society 19 (10), 2017, http://www.researchprofiles.canberra.edu.au/
23. *V. A. Memos, K. E. Psannis, Y. Ishibashi, Byung-Gyu Kim, B.B. Gupta*, An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework, Researchgate 2018,
24. *B. A. Motsios*, Forensics Analysis for e-Wallet, 2017, http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/10152/Motsios_Vasileios.pdf?sequence=1&isAllowed=y,
25. *Aine MacDermott, Th. Baker, Qi Shi*, IoT Forensics: Challenges For The IoA Era, https://www.google.com/search?q=IoT+Forensics%3A+Challenges+For+The+IoA+Era&rlz=1C1NDCM_enGR841GR841&oq=IoT+Forensics%3A+Challenges+For+The+IoA+Era&aqs=chrome..69i57.1845j0j8&sourceid=chrome&ie=UTF-8,
26. *M. B. Mukasey, J. L. Sedgwick, D. W. Hagyhttps*://www.ncjrs.gov/pdffiles1/nij/219941.pdf,
27. *J. R. Norgaard, H.J. Walbert, R. A. Hardy*, Shadow Markets and Hierarchies: Comparing and Modeling Networks in the Dark Net, https://s3.amazonaws.com/academia.edu.documents/51205101/ Shadow_Markets_and_Hierarchies_-_Comparing_and_Modeling_Networks_in_the_Dark_Net_Norgaard.pdf?response-content-disposition=inline% 3B%20filename%3DShadow_Markets_and_Hierarchies_Comparing.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=ASIATUSBJ6BAFRPY66IU%2F20200404%2Fus-east-1%...-Amz-Signature=e0c846e73557dbca224d0b2f7329500a1922654e686745abc 90046b3436c8c2a.,
28. *An. Papathanasiou, Al. Papanikolaou, V. Vlachos, K. Chaikalis, M. Dimou, M. Karadimou and V. Katsoula*, Legal and Social Aspects of Cyber Crime in Greece, ResearchGate 2015, https://www.researchgate.net/publication/260390705,
29. *D. B. Parker*, Fighting Computer Crime, 1983, NY.,

30. *J. Ratkiewicz, M. Conover, M. Meiss, B. Gonçalves, A. Flammini, and F. Menczer,* «Detecting and Tracking Political Abuse in Social Media," ICWSM, vol. 11, pp. 297-304, 2011,
31. *M. Reith, C. Carr, G. Gunsch,* An examination of digital forensic models. International Journal of Digital Evidence, (2002), https://pdfs.semanticscholar.org/c73f/47d8385f452dfd25bbaab754874b65594ccd.pdf,
32. *L. D. X. Z. Shancang Li,* «The internet of things: a survey,» Information Systems, Frontiers, p. 243–259, April 2015,
33. *N. Shaukata, S.M. Alia, C.A. Mehmooda, B. Khana, M. Jawadb, U. Farida, Z. Ullaha, S.M. Anwarc, M. Majidd,* A survey on consumers empowerment, communication technologies, and renewable generation penetration within Smart Grid, Renewable and Sustainable Energy Reviews, Volume 81, Part 1, January 2018, Pages 1453-1475, https://www.researchgate.net/profile/Zahid_Ullah2/publication/317621899_A_survey_on_consumers_empowerment_communication_technologies_and_renewable_generation_penetration_within_Smart_Grid/links/5b9e8dc5a6fdccd3cb5dd08b/A-survey-on-consumers-empowerment-communication-technologies-and-renewable-generation-penetration-within-Smart-Grid.pdf,
34. *R. Sobti, G.Geetha,* Cryptographic Hash Functions: A Review, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, March 2012, https://www.researchgate.net/profile/Geetha_Ganesan3/publication/267422045_Cryptographic_Hash_Functions_A_Review/links/549cf6d10cf2b8037138c35c/Cryptographic-Hash-Functions-A-Review.pdf
35. *S. Srinivasan,* Digital Forensics Curriculum in Security Education, Journal of Information Technology Education: Volume 12, 2013 Innovations In Practice, http://www.jite.informingscience.org/ documents/Vol12/JITEv 12IIPp147-157Srinivasan1232.pdf
36. *Chr. Stergiou, K. Psannis, Br. Gupta, Yut. Ishibashi,* Security, Privacy and Efficiency of Sustainable Cloud Computing for Big Data and IoT, 2018, https://www.researchgate.net/profile/Kostas_Psannis/publication/325767407_Security_Privacy_Efficiency_of_Sustainable_Cloud_Computing_for_Big_Data_IoT/links/5b2c12564585150d23c1a958/Security-Privacy-Efficiency-of-Sustainable-Cloud-Computing-for-Big-Data-IoT.pdf,
37. *Chr. Stergiou and K. Psannis,* Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: a survey, 2017, international journal of network management, Int. J. Network Mgmt, Published online in Wiley Online Library (wileyonlinelibrary.com) DOI: 10.1002/nem.1930,
38. *Chr. Stergiou, K. Psannis, B.-G. Kimb, Br. Gupta,* Secure integration of IoT and Cloud Computing, https://www.researchgate.net/profile/Kostas_Psannis/publication/311065854_Secure_Integration_of_Internet-of-Things_and_Cloud_Computing/links/5a44ca35aca272d2945c4b1b/Secure-Integration-of-Internet-of-Things-and-Cloud-Computing.pdf,
39. *D. Sudyana, Yudi Prayudi, B. Sugiantoro,* Analysis And Evaluation Digital Forensic Investigation Framework Using ISO 27037:2012, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(1): 1-14 The Society of Digital Information and Wireless Communications (SDIWC), 2019 ISSN: 2305-001
40. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, «Electronic Crime Scene Investigation, A Guide for First Responders, Second Edition», https://www.econinfosec.org/ archive/weis2012/papers/Anderson_WEIS2012.pdf,

41. *M Yar, KF Steinmetz*, Cybercrime and society, SAGE 2019, σε https://books.google.gr/books?id=_nN7DwAAQBAJ&printsec=frontcover&hl=el&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false,
42. *B. Yadegari, S. Debray*, Bit-Level Taint Analysis, 2014, https://raptor.cs.arizona.edu/~debray/Publications/ bit-level-taint.pdf.,