ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Σχολή Οικονομικών, Επιχειρηματικών και Διεθνών Σπουδών

Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΟΙΚΟΝΟΜΙΑ-MASTER IN LAW AND ECONOMICS»

Μαρία-Ευαγγελία Κωνσταντοπούλου

Η ΟΙΚΟΝΟΜΙΚΗ ΑΝΑΛΥΣΗ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

ΤΑ ΟΙΚΟΝΟΜΙΚΑ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Cyber Crime Law & Economics

The Economics of Cyber Crime

Επιβλέπων Καθηγητής: Αριστείδης Χατζής

Πειραιάς 2020

Βεβαίωση Εκπόνησης Διπλωματικής Εργασίας

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΚΑΙ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΔΙΚΑΙΟ ΚΑΙ ΟΙΚΟΝΟΜΙΑ»

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Δηλώνω υπεύθυνα ότι η διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών, του Πανεπιστημίου Πειραιώς, «Δίκαιο και Οικονομία» με τίτλο «**Η Οικονομική Ανάλυση του Εγκλήματος στον Κυβερνοχώρο/Τα Οικονομικά του Ηλεκτρονικού Εγκλήματος- Cyber Crime Law & Economics/The Economics of Cyber Crime**» έχει συγγραφεί από εμένα αποκλειστικά και στο σύνολό της. Δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

Δηλώνω επίσης υπεύθυνα ότι οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης εργασίας, αναφέρονται στο σύνολό τους, κάνοντας πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου.

Υπογραφή Μεταπτυχιακού Φοιτητή/ τριας

Ονοματεπώνυμο **Μαρία-Ευαγγελία Κωνσταντοπούλου**

Ημερομηνία **13.11.2020**

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία επιχειρεί να καταδείξει τις πολυσύνθετες διαστάσεις του ηλεκτρονικού εγκλήματος ως κοινωνικού φαινομένου που γεννήθηκε με την ψηφιακή εποχή και αναδείχθηκε σε διεθνή απειλή, αόρατη, πλην όμως, με ορατό κοινωνικό και οικονομικό αντίκτυπο στον κόσμο του σήμερα. Το ηλεκτρονικό έγκλημα, για το οποίο δεν υπάρχει ομοφωνία ως προς τον ορισμό του από τα περισσότερα κράτη, εμφανίζεται με πολλές μορφές, ορισμένες εκ των οποίων γεννήθηκαν με την άνθηση του Διαδικτύου και ορισμένες αποτελούν την ψηφιακή διάσταση ήδη γνώριμων παραδοσιακών εγκλημάτων. Η εξαντλητική απαρίθμηση δεν είναι εφικτή όχι μόνο λόγω της περιορισμένης έκτασης της παρούσας μελέτης αλλά και λόγω της διαρκούς εμφάνισης νέων προεκτάσεων, οι οποίες γεννούν νομοθετικές προκλήσεις και φέρνουν στο προσκήνιο την αναγκαιότητα σύμπλευσης των μεθοδολογικών εργαλείων περισσότερων επιστημών επί τη βάσει της αναζήτησης κοινωνικά βέλτιστων λύσεων. Στην κατεύθυνση αυτή, στόχος της προκείμενης έρευνας είναι η παρουσίαση καίριων προβληματικών μέσα από την προσέγγιση του ηλεκτρονικού εγκλήματος από κοινωνιολογική, οικονομική και νομική σκοπιά, αφενός με εστίαση της προσοχής στην αναγκαιότητα διεθνούς νομοθετικής εναρμόνισης και συνεργασίας, και αφετέρου, με παράλληλη εξέταση μοντέλων εναλλακτικής δράσης που σκοπούν στην ενίσχυση της προληπτικής λειτουργίας του Ποινικού Δικαίου.

Στο πρώτο (1ο) κεφάλαιο παρουσιάζεται το ηλεκτρονικό έγκλημα ως κοινωνικό φαινόμενο μέσα από την κατάδειξη των συνηθέστερων μορφών του και των λαμβανόμενων προεκτάσεων που συχνά δεν περιορίζονται στα στενά όρια ενός μόνο κράτους, αλλά εμφανίζουν διασυνοριακά χαρακτηριστικά. Παρατίθενται ακόμη, προβληματικές σε σχέση με τις δυσκολίες ακριβούς αποτίμησης της προκαλούμενης ζημίας και τον οικονομικό-κοινωνικό αντίκτυπο που βαίνει ολοένα αυξανόμενος. Τέλος, θίγονται δικονομικά ζητήματα που προκύπτουν από το διασυνοριακό χαρακτήρα του ηλεκτρονικού εγκλήματος και αφορούν στη δικαιοδοσία και την έκδοση, παρατιθέμενης προσθέτως της προβληματικής της έρευνας και κατάσχεσης των ψηφιακών μέσων.

Στο δεύτερο (2ο) κεφάλαιο παρατίθενται οι σημαντικότερες, κατά τη γνώμη της γράφουσας, προσπάθειες νομοθετικής αντιμετώπισης σε επίπεδο Ποινικού Δικαίου,

εστιαζόμενες στο παράδειγμα της Αμερικής και των σχετικών ρυθμίσεων σε ομοσπονδιακό επίπεδο, τη Σύμβαση της Βουδαπέστης ως του κύριου διεθνούς κειμένου στο πλαίσιο επιδίωξης κοινής αντεγκληματικής πολιτικής με στόχο την προστασία της κοινωνίας από το ηλεκτρονικό έγκλημα, ιδίως μέσα από την υιοθέτηση της κατάλληλης νομοθεσίας και την ενίσχυση της ταχείας και καλά συντονισμένης διεθνούς συνεργασίας, και τέλος, αποτυπώνονται οι σχετικές προβλέψεις της ελληνικής έννομης τάξης.

Στο τρίτο (3ο) κεφάλαιο, επιδιώκεται η ανάδειξη της σημασίας των μεθοδολογικών εργαλείων της Οικονομικής Ανάλυσης του Δικαίου ως κλάδου που ερευνά τα κίνητρα στη συμπεριφορά των δραστών στη βάση της υπόθεσης του ορθολογικά δρώντος υποκειμένου που επιδιώκει τη μεγιστοποίηση της ωφέλειάς του. Στο πλαίσιο αυτό και υπό τη σκέψη ότι η διάπραξη του εγκλήματος συνιστά απόρροια της στάθμισης επιμέρους πιθανοτήτων, επιδιώκεται η κατάδειξη πρόσθετων παραμέτρων ικανών να συμβάλουν στη διαμόρφωση ενός νομοθετικού πλαισίου που δεν ερείδεται σε μια λειτουργία τιμωρητικού σκοπού, αλλά, που στοχεύει, πράγματι, στο κοινωνικά βέλτιστο αποτέλεσμα. Τέλος, και υπό τη σκέψη ότι η εύρεση αποτελεσματικών λύσεων είναι σκόπιμο να αναζητηθεί, παράλληλα με το νομοθετικό πλαίσιο, σε νέα μοντέλα που θα συνεπικουρούν το ρόλο του Ποινικού Δικαίου, παρατίθενται εναλλακτικοί τρόποι αντιμετώπισης από τη σκοπιά των ενδιάμεσων παρόχων υπηρεσιών, των υποψήφιων θυμάτων και των ίδιων των δραστών.

Στο τελευταίο κεφάλαιο, έχοντας υπόψη τις εκτεθείσες προβληματικές, η μελέτη καταλήγει στην παράθεση συμπερασμάτων με γνώμονα την παράλληλη δράση σε πλείονα επίπεδα με στόχο την καταπολέμηση των νέων φαινομένων, που απαιτεί, κατά την άποψη της γράφουσας, αποδέσμευση από τις παραδοσιακές μεθόδους δράσης και θέαση του προβλήματος με μια συνολική ματιά που θα περιλαμβάνει την προσαρμογή της νομοθεσίας στις αναδεικνυόμενες προκλήσεις σε μια εποχή που η τεχνολογία της πληροφορίας έχει διαποτίσει κάθε πτυχή της ανθρώπινης δραστηριότητας.

ABSTRACT

The present paper seeks to capture the aspects of cybercrime as a social phenomenon emerged in the digital age, which has received international dimensions, being an invisible threat but at the same time having a significant social and economic impact on the modern world. There is not a unanimous universal definition for what the cybercrime is and the latter occurs under many forms, some of which were born with the boom of the Internet and others constitute the digital dimension of familiar types of traditional crimes. The exhaustive enumeration is not feasible not only due to the limited scope of this thesis but also due to the constant development of new forms of cybercrime, which give rise to legislative challenges and highlight the need to combine the methodological tools of more scientific fields seeking social optimum solutions. Though, the aim of this research is to present the key problems by studying the cybercrime from a sociological, an economic and a legal point of view, focusing on the need for international legislative harmonization and cooperation while examining any alternative action models which could potentially enhance the preventive function of Criminal Law.

The first chapter examines cybercrime as a social phenomenon through the presentation of the most common types and the extensions received that go beyond the domestic context. Furthermore, another issue under consideration pertains to the difficulties of estimating accurately the damage being caused and the increasing socio-economic impact. Finally, some procedural issues arising from the cross-border nature of cybercrime are addressed, such as jurisdiction and extradition in combination to search and seizure problems of digital media.

The second chapter lists the most important, according to the writer's opinion, legislative efforts of Criminal Law to regulate cybercrime, focusing on the example of America and the relative legislative actions at a federal level, on the Budapest Convention as the main international treaty pursuing a common anti-crime policy of justice aiming at the protection of society from cybercrime by adopting appropriate legislation and enhancing a fast and well-coordinated international cooperation. Finally, the relevant provisions in the Greek legal system are presented.

In the third chapter, the analysis aim to highlight the importance of the methodological tools of the Economic Analysis of Law, being a field that investigates perpetrators' motivations on the basis of the assumption of existence of a rational individual who seeks to maximize her benefit. In this context, taking into account that the commission of crimes is a result of the weighting of individual probabilities, I present additional parameters in the creation of a legislative framework, not aiming at a punitive function but, instead, for the sake of social good. Finally, taking into consideration that effective solutions should be sought, alongside the legislative framework, in new models to complement the role of Criminal Law, the study examines alternative ways to deal with intermediary providers, potential victims and perpetrators themselves.

In the final chapter, taking into account the problems encountered, the thesis concludes with suggestions for parallel action at a number of different levels aiming at combating new phenomena, which, in the view of the writer, require release from the traditional approaches, towards a new holistic approach including adaptation of the legislation to emerging technological challenges.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ 2
ABSTRACT 5
ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ 7
ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ ΩΣ ΚΟΙΝΩΝΙΚΟ ΦΑΙΝΟΜΕΝΟ 7
1.1 Ορίζοντας το ηλεκτρονικό έγκλημα 9
1.2 Τα επιμέρους χαρακτηριστικά 10
1.3 Απαρχές 11
1.4 Τυποποίηση 12
1.4.1 Η προβληματική 12
1.4.2 Η τριμερής διάκριση 13
1.5 Νέες μορφές: ανεξέλεγκτες προεκτάσεις 13
1.5.1 Μη εξουσιοδοτημένη πρόσβαση (hacking και cracking) 14
Ιοί (viruses) 15
Σκουλήκια (Worms) 15
Λογικές βόμβες (Logic Bombs) 16
Δούρειος Ίππος (Trojan Horses) 16
Δίκτυο Μπότνετ (Botnet) 16
Ransomware 16
Επίθεση Άρνησης Υπηρεσιών (Denial of Service-DDoS Attacks) 17
Ανεπιθύμητη αλληλογραφία (Spamming) 17
Ηλεκτρονικό «ψάρεμα» (Phishing) 17
1.5.2 Η ψηφιακή διάσταση του παραδοσιακού εγκλήματος 18
Κλοπή ταυτότητας (identity theft) 18
Διαδικτυακές απάτες (fraud) 19
1.5.3 Φαινόμεναεποχής 18
Εκφοβισμός και παρενόχληση στο Διαδίκτυο 20
1.5.4 Παιδική πορνογραφία (child pornography) και grooming 21
1.5.5 Η άνοδος του κυβερνοπολέμου (cyber-war) και η προβληματική του δόγματος της μη παρέμβασης (The doctrine of non-intervation) 22
1.5.6 Τρομοκρατία στο Διαδίκτυο (cyber-terrorism) και επιτήρηση (surveillance) 23
1.6 Επιμέρους προβληματικές 24
1.6.1 Δικαιοδοσία και έκδοση 24
1.6.2 Έρευνα και κατάσχεση 26
1.7 Δυσκολίες αποτίμησης του ηλεκτρονικού εγκλήματος 28
1.8 Οικονομικός αντίκτυπος και κοινωνικό κόστος 29
ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ 31
ΝΟΜΟΘΕΤΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ 31
2.1 Εισαγωγικές Παρατηρήσεις 31
2.2.1 Αμερική 32
2.2.2 Computer Fraud and Abuse Act of 1986 (CFAA) 33
2.2.3 Οι επιμέρους προσβολές και το επαπειλούμενο πλαίσιο ποινής 35
2.2.4 Άλλα νομοθετήματα 37
2.3.1 Ευρώπη 39
2.3.2 Η Σύμβαση της Βουδαπέστης 40
2.3.3 Ευρωπαϊκές Οδηγίες 48
i) Η Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών 48
ii) Η οδηγία 2019/7313/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την καταπολέμηση της απάτης και της πλαστογραφίας πληρωμών με μέσα πλην των μετρητών σε αντικατάσταση της απόφασης-πλαισίου 2001/413/ΔΕΥ του Συμβουλίου για την online απάτη 49
iii) Η Οδηγία 2011/92/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 2011σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαισίου 2004/68/ΔΕΥ του Συμβουλίου 50

iv) Η Οδηγία 2016/1148/ΕΕ σχετικά με τα μέτρα για ένα υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση ('NIS')..... 51
2.4. Φορείς ευρωπαϊκής και διεθνούς συνεργασίας..... 53
2.5 Ελληνική Έννομη Τάξη..... 54
2.5.1 Ν. 4411/2016..... 54
2.5.2 Εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων και πληροφοριών στην ελληνική έννομη τάξη..... 55
i) Προσβολές ατομικού απορρήτου και επικοινωνίας: άρθρα 370 επ. ΠΚ..... 55
ii) Παρακώλυση λειτουργίας πληροφοριακών συστημάτων: άρθρα 292^{B}-292^{Γ} ΠΚ..... 58
iii) Παράνομη παρεμβολή σε δεδομένα κατ' άρθρον 381^{A} ως ίσχυε..... 59
2.5.3 Εγκλήματα σχετικά με υπολογιστές..... 60
i) Απάτη με υπολογιστή: άρθρο 386^{A} ΠΚ..... 60
2.5.4 Εγκλήματα σχετικά με το περιεχόμενο..... 61
i) Πορνογραφία και πορνογραφικές παραστάσεις ανηλίκων: άρθρα 348^{A}-348^{Γ} ΠΚ..... 61
2.5.5 Παρατηρήσεις..... 63
ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ..... 63
ΤΑ ΕΡΓΑΛΕΙΑ ΤΗΣ ΟΙΚΟΝΟΜΙΚΗΣ ΑΝΑΛΥΣΗΣ ΤΟΥ ΔΙΚΑΙΟΥ ΩΣ ΜΕΣΟ ΠΕΡΙΣΤΟΛΗΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ..... 63
3.1 Εισαγωγικές Παρατηρήσεις..... 65
3.2 Αναζητώντας τα κίνητρα των δραστών..... 66
3.3 Η συμβολή της οικονομικής ανάλυσης..... 69
3.4.1 Η θεωρία του Gary Becker..... 70
3.4.2 Τα συστατικά της ανάλυσης κόστους-οφέλους..... 73
3.5 Η έννοια της αποτροπής..... 74
3.5.1 Το μοντέλο της αγοράς και η διαμόρφωση του κόστους αποτροπής..... 74
3.5.2 Η εσωτερική υπακοή ως έτερος παράγοντας αποτροπής..... 76
3.6 Η πρόταση του Lessig..... 77
3.7 Στρατηγική τριών μερών..... 79
3.7.1 Η ευθύνη των ενδιάμεσων μερών..... 80
i) Η ποινική ευθύνη των ενδιάμεσων παρόχων και ιδίως των μέσων κοινωνικής δικτύωσης υπό το πρίσμα της Οδηγίας 2000/31/ΕΚ και του ΠΔ 131/2003..... 82
ii) Ποινική ευθύνη των μέσων κοινωνικής δικτύωσης για εγκλήματα εξωτερίκευσης δυνάμει του κοινού Ποινικού Δικαίου..... 84
3.7.2 Αυτοάμυνα ('Self-defense')..... 85
i) Από την παθητική ('passive defense') στην ενεργητική αυτοάμυνα ('active defense')85
ii) 'Mitigative counterstriking' και 'Socially optimal hackback'..... 86
iii) Η αυτοάμυνα υπό το πρίσμα του άρθρου 51 του Χάρτη Η.Ε...... 88
3.7.3 Διαμόρφωση προτιμήσεων ('Preference-shaping Theory')..... 89
i) 'Hacker Ethic'..... 89
ii) 'Hack-in' διαγωνισμοί..... 91
iii) Το μοντέλο..... 92
3.8 Στην κατεύθυνση μιας ορθής κουλτούρας..... 93
3.8.1 Δημόσια αφύπνιση..... 93
3.8.2 Παροχή κινήτρων στα υποψήφια θύματα..... 94
ΒΙΒΛΙΟΓΡΑΦΙΑ..... 104

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ
ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ ΩΣ ΚΟΙΝΩΝΙΚΟ ΦΑΙΝΟΜΕΝΟ

1.1 Ορίζοντας το ηλεκτρονικό έγκλημα

Η ραγδαία εξάπλωση του Διαδικτύου σε παγκόσμια κλίμακα έφερε στην επιφάνεια νέες δυνατότητες για τους χρήστες. Όπως ήταν αναμενόμενο δεν άργησαν να παρουσιαστούν οι αρνητικές διαστάσεις της ψηφιακής εποχής, η κυριότερη εκ των οποίων αντικατοπτρίζεται στο ηλεκτρονικό έγκλημα. Ο όρος «ηλεκτρονικό έγκλημα» δεν αντιστοιχεί σε μία μόνο έκφραση αποδοκιμαζόμενης πράξης αλλά εκφράζει περισσότερες μορφές εγκληματικής δραστηριότητας. Πολλές είναι ήδη γνωστές μέσα από τα εμπειρικά παραδείγματα, ενώ άλλες εξακολουθούν να εμφανίζονται γεννώντας νέες νομοθετικές προκλήσεις. Διεθνώς έχει αποδοθεί με τους γενικότερους όρους *e-crime* και *computer crime* και με τους ειδικότερους όρους *cybercrime* και *internet related crime*, οι οποίοι τελευταίοι συνδέονται άρρηκτα με το στοιχείο του Διαδικτύου.[1] Η συνήθης διάκριση αφορά στις αξιόποινες πράξεις που πραγματοποιούνται αποκλειστικά μέσω του Διαδικτύου, ήτοι τα αμιγώς ηλεκτρονικά εγκλήματα (*cybercrimes*), όπως η πειρατεία λογισμικού, και στις αξιόποινες πράξεις που λαμβάνονται σε περιβάλλον υπολογιστή χωρίς τη χρήση του Διαδικτύου (*computer crimes*), όπως η παραβίαση ή υποκλοπή προσωπικών δεδομένων (Σφακιανάκης 2016: 21). Πολλοί υποστηρίζουν ότι το ηλεκτρονικό έγκλημα δε συνιστά τίποτα περισσότερο από τη μετάλλαξη του παραδοσιακού εγκλήματος στην ψηφιακή εποχή, ενώ άλλοι το αντιλαμβάνονται ως μια ολότελα καινούργια κατηγορία εγκλήματος που απαιτεί τη δημιουργία ενός αντίστοιχα νέου νομοθετικού πλαισίου που θα απευθύνεται στη μοναδική φύση των αναδυόμενων τεχνολογιών και προβληματικών (Sussmann 1999: 453-455). Πιο συνεπής, ωστόσο, είναι η διατύπωση ότι στην έννοια του ηλεκτρονικού εγκλήματος υπάγονται τόσο τα γνήσια εγκλήματα, δηλαδή οι αμιγώς νέες μορφές αξιόποινης δράσης, όσο και τα παραδοσιακά. Κατά τους Forrester και Morrison ο όρος ανταποκρίνεται σε κάθε *«εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής*

[1] Στην ελληνική γλώσσα οι αντίστοιχοι όροι που χρησιμοποιούνται είναι «ηλεκτρονικό έγκλημα» ως γενικότερος όρος και «δικτυακό έγκλημα», «κυβερνοέγκλημα» και «έγκλημα στον κυβερνοχώρο» ως ειδικότεροι όροι για να περιγράψουν τις αξιόποινες πράξεις που τελούνται αποκλειστικά και μόνο μέσω του Διαδικτύου (Δαλακούρας 2018: 3).

της». Από την άλλη, το Υπουργείο Δικαιοσύνης των ΗΠΑ έχει ορίσει το ηλεκτρονικό έγκλημα ως *«κάθε προσβολή του Ποινικού Δικαίου που απαιτεί τη γνώση τεχνολογίας υπολογιστών»* επεκτείνοντας, έτσι, τον ορισμό σε κάθε έγκλημα, στο οποίο ο υπολογιστής εμφανίζεται ως στόχος, εργαλείο, μέσο ή συσκευή αποθήκευσης, ενώ από το 2010 οι όροι *computer crimes, cybercrimes* και *network crimes* χρησιμοποιούνται αδιακρίτως. Παρά ταύτα, αποτελεί κοινό τόπο η διαπίστωση ότι δεν υπάρχει ενιαία αποδεκτός ορισμός ούτε σταθερή κατηγοριοποίηση των επιμέρους μορφών (Viano 2017: 3).

1.2 Τα επιμέρους χαρακτηριστικά

Τα αυξανόμενα ποσοστά ηλεκτρονικών εγκλημάτων σε σχέση με τις παραδοσιακές αξιόποινες πράξεις δεν αποδίδονται σαφώς σε μια εγγενή εγκληματογόνο διάθεση του διαδικτυακού χώρου, αλλά στα επιμέρους χαρακτηριστικά που εμφανίζει. Η ταχύτητα, η ευκολία και η ανωνυμία αποτελούν μόνο μερικά από τα χαρακτηριστικά που διευκολύνουν την τέλεσή του (ACLR 1992: 226-227). Στο χώρο του Διαδικτύου μια ενέργεια λαμβάνει χώρα σε λίγα μόλις δευτερόλεπτα, ενώ μπορεί να πλήξει ταυτόχρονα πλείονα συστήματα πληροφοριών, χωρίς να απαιτείται η φυσική παρουσία του δράστη στον τόπο του εγκλήματος[2], αφού μπορεί να ενεργήσει από την οικία του, προσβάλλοντας ένα στόχο ακόμη και σε άλλη ήπειρο. Υπό αυτή την έννοια, το ηλεκτρονικό έγκλημα είναι πάντοτε έγκλημα εξ αποστάσεως εφόσον αλλού εκδηλώνεται η συμπεριφορά του δράστη και αλλού το ενδεχόμενο αξιόποινο αποτέλεσμα (Κιούπης 2019: 41-42 σε Δαλακούρα 2019: 41-42). Στο πλαίσιο αυτό, η διασυνοριακή διάσταση που μπορεί να λάβει ένα ηλεκτρονικό έγκλημα, γεννά ερωτήματα για τον καθορισμό του τόπου τελέσεως του εγκλήματος και ζητήματα δικαιοδοσίας και προτεραιότητας μεταξύ των εμπλεκόμενων κρατών. Τα πράγματα γίνονται ακόμη πιο σύνθετα σε περιπτώσεις που ο δράστης δραστηριοποιείται σε μια χώρα Α, προσβάλλοντας συστήματα σε μια χώρα Β για να πλήξει τελικώς μια χώρα Γ. Την ίδια στιγμή η συλλογή των αποδεικτικών στοιχείων προϋποθέτει αφενός την αναγνώριση του αξιοποίνου για την αυτή εγκληματική ενέργεια σε περισσότερες έννομες τάξεις (dual ή double criminality) και αφετέρου, τη συνεργασία των κρατών. Από την άλλη πλευρά, η διεθνής συνεργασία είναι

[2] "There is a revolution going on in criminal activity. […] A criminal no longer needs to be at the actual scene of the crime (or within 1,000 miles, for that matter) to prey on his victim." (Sussmann 1999: 451).

καίρια, αλλά στην πράξη χωλαίνει καθώς τα κράτη συχνά δε διαθέτουν τους πόρους ή τη σωστή νομοθεσία για να συλλέξουν αποδείξεις ή να συλλάβουν τους δράστες (Koops & Brenner 2006: 1-3) ή μπορεί να εμφανίζονται απρόθυμα στη συνεργασία.[3] Αυτά όλα, συνδυαζόμενα με τα εργαλεία της κρυπτογράφησης και στεγανογράφησης (cryptography and steganography)[4] που συχνά υποκρύπτουν εξειδικευμένες τεχνικές γνώσεις δυσχεραίνουν την εξιχνίαση και ακολούθως την ευχερή αντιμετώπιση. Πολλώ δε μάλλον, που μεγάλο μέρος των ηλεκτρονικών εγκλημάτων δε γνωστοποιείται στις αρμόδιες αρχές με αποτέλεσμα τα στατιστικά στοιχεία να είναι ανακριβή και η προσοχή να στρέφεται στα εγκλήματα που συγκεντρώνουν περισσότερη δημοσιότητα, λαμβανομένου υπόψη του πεπερασμένου των εργαλείων αντιμετώπισης (ACLR 1995: 193-195, 204-205).

1.3 Απαρχές

Η δημιουργία του Παγκόσμιου Ιστού (World Wide Web) το 1989 και η δύναμη του Διαδικτύου μας έφερε αντιμέτωπους με νέες μορφές εγκλήματος και ανεξέλεγκτες δυνατότητες στον κυβερνοχώρο· ένα εναλλακτικό σύμπαν ευρισκόμενο σε μια διαρκή αλληλεπίδραση με το νομικό χώρο, που εγείρε ζητήματα περί μιας αρχικής αυτορρύθμισής του (self-regulation), πλην όμως, γρήγορα ενεφάνη ότι ένα μοντέλο αυτορρύθμισης του Διαδικτύου δε θα καθίστατο αποτελεσματικό επί μακρόν χωρίς τις αναγκαίες μεταβολές στη νομοθεσία (Miller 2004: 904). Τα πρώτα σοβαρά κρούσματα εισβολής σε συστήματα πληροφοριών προβάλλουν ήδη από τη δεκαετία του 1960 στην Αμερική με τις συνολικές απώλειες να υπολογίζονται στα $450.000, σχεδόν πέντε φορές υψηλότερο ποσοστό από τα συμβατικά εγκλήματα λευκού κολάρου (white collar crimes), ενώ μόνο το έτος 1977 οι εκτιμώμενες απώλειες στις ΗΠΑ άγγιξαν τα 200 εκατομμύρια δολάρια (Quinn 1978: 48). Τη δεκαετία του 1980 οι αριθμοί πολλαπλασιάζονται, ενισχυόμενοι από την πεποίθηση της ασυλίας των δραστών, που σταθμίζουν τις μηδαμινές πιθανότητες σύλληψης και παράλληλα την επαπειλούμενη ελάχιστη τιμωρία ακόμη και σε περίπτωση σύλληψης (Ghosh & Turrini 2010: 4). Αυτό απεδείχθη περίτρανα το 1988 στην περίπτωση του Robert Morris και του διαβόητου Morris worm, ενός κακόβουλου και αυτοαναπαραγόμενου προγράμματος, που εκτιμάται ότι κατέστειλε

[3] Ενδεικτικά , η Ρωσία και η Κίνα, δυο χώρες που έχουν πολλάκις κατηγορηθεί για χρηματοδότηση κακόβουλης διαδικτυακής δραστηριότητας, έχουν αρνηθεί να επικυρώσουν τη Σύμβαση της Βουδαπέστης.
[4] Η τακτική της απόκρυψης ενός αρχείου σε ένα άλλο αρχείο που χρησιμοποιείται για την μεταφορά μυστικών μηνυμάτων.

τις λειτουργίες 1.000 με 3.000 υπολογιστών, μεταξύ των οποίων το ερευνητικό κέντρο της NASA και το Εθνικό Εργαστήριο Λώρενς στο Λίβερμορ με πιθανές απώλειες στα $72.500 και $100.000, ενώ η επιβληθείσα ποινή ανήλθε σε μόλις 3 χρόνια φυλάκισης, πρόστιμο $10.000 και 400 ώρες κοινωφελούς εργασίας (GAO 1989). Ο ιός Melissa (Melissa Virus), μία περίπου δεκαετία αργότερα, που έπληξε τους διακομιστές ηλεκτρονικού ταχυδρομείου σε περισσότερες από 300 εταιρείες και κυβερνητικές υπηρεσίες ανά τον κόσμο, μεταξύ των οποίων η Microsoft, προκαλώντας γενικευμένο χάος, με το συνολικό κόστος για τον καθαρισμό και την αποκατάσταση των υπολογιστικών συστημάτων να ανέρχεται στα 80 εκατ. δολάρια (FBI 2019) καταδεικνύει τις ανεξέλεγκτες διαστάσεις του νέου φαινομένου. Αξιοσημείωτη είναι σίγουρα και η περίπτωση του "ILove computer worm" (Love Bug virus) με αυτουργό έναν μαθητή από τις Φιλιππίνες, που έχει χαρακτηριστεί ως το πιο καταστροφικό έγκλημα της ιστορίας με απώλειες άνω των 11 δισ. δολαρίων και έλαβε την μορφή άρνησης υπηρεσιών (DoS Attacks) σε Yahoo!, e-Bay, E*Trade και άλλες ιστοσελίδες που εκτιμάται ότι υπέστησαν ζημία 1,2 δισ. δολάρια (Katyal 2001: 1004). Μεταξύ 1999 και 2004, 27,3 εκατ. Αμερικανοί έπεσαν θύματα κλοπής ταυτότητας περιλαμβανομένων 9,9 εκατ. το 2003, ενώ επιχειρήσεις και οργανισμοί έχασαν περίπου 48 δισ. δολάρια. Την ίδια χρονιά εταιρείες στη Β. Αμερική αντιμετώπισαν ζημία 3,5 δισ. Από το 1997 63 εκατ. ιοί διοχετεύτηκαν στο Διαδίκτυο προκαλώντας εκτιμώμενη ζημία 65 δισ. δολάρια (Lewis 2004: 1354-355).

1.4 Τυποποίηση

1.4.1 Η προβληματική

Βασική προβληματική στην αντιμετώπιση του ηλεκτρονικού εγκλήματος αποτελεί η ανυπαρξία «τυπικού» εγκλήματος και «τυπικού» κινήτρου.[5] Ο δράστης μπορεί να αναζητηθεί τόσο ανάμεσα σε έναν νεαρό ή επαγγελματία hacker, διακατεχόμενο από την περιέργειά του να δοκιμάσει ή να επιδείξει τις τεχνικές του ικανότητες, έναν δυσαρεστημένο εργαζόμενο ή έναν αναξιόπιστο τεχνικό ή ακόμη μια εγκληματική

[5] Σύμφωνα με έρευνα του 2000 από την εταιρεία ασφαλείας Kessler International στη Νέα Υόρκη η κλοπή απόρρητων πληροφοριών διαπράττεται κατά 35% από δυσαρεστημένους εργαζομένους, κατά 28% από εξωτερικούς χάκερς, κατά 18% από άλλες αμερικάνικες εταιρείες, κατά 11% από εξωχώριες εταιρείες, κατά 8% από ξένες Κυβερνήσεις και κατά 10% από άλλους.

οργάνωση ή έναν τρομοκράτη διεθνούς δράσης (ACLR 1995: 185). Τα ηλεκτρονικά εγκλήματα συναντώνται σε πλήθος μορφών χωρίς να υπάρχει μια σταθερή κατηγοριοποίηση. Πολύ περισσότερο που υπάρχει διαφωνία εγχώρια και διεθνώς για τον ακριβή ορισμό του ηλεκτρονικού εγκλήματος ως έννοιας που καλύπτει ένα ευρύτερο φάσμα προσβολών, ώστε η τελική ομοφωνία να φαίνεται σχεδόν δυσεπίτευκτος στόχος (Collier & Spaul 1992: 308-320), χωρίς να παραβλέπεται, περαιτέρω, ότι, ένα μόνο ηλεκτρονικό έγκλημα είναι πιθανό να συνεπάγεται περισσότερες διαφορετικές προσβολές (Grabosky 2016: 8), οπότε τα πράγματα περιπλέκονται.

1.4.2 Η τριμερής διάκριση

Η βασική κατηγοριοποίηση, ωστόσο, σχετίζεται με τον ιδιαίτερο ρόλο που διαδραματίζει ο υπολογιστής σε κάθε συγκεκριμένη περίπτωση και αφορά στη γενική τριμερή διάκριση των ηλεκτρονικών εγκλημάτων σε α) εγκλήματα, στα οποία ο υπολογιστής είναι ο ίδιος στόχος της εγκληματική δράσης, οπότε κύρια επιδίωξη του δράστη είναι η κλοπή πληροφοριών από ή η πρόκληση ζημίας σε ένα υπολογιστή, ένα σύστημα ή ένα δίκτυο (π.χ. hacking, cracking, cyber war, κακόβουλοι ιοί), β) εγκλήματα, στα οποία ο υπολογιστής αποτελεί το μέσο διάπραξης των παραδοσιακών εγκλημάτων (π.χ. απάτη, κλοπή, εκβίαση[6]) και γ) εγκλήματα, στα οποία ο υπολογιστής εμφανίζεται ως παρεπόμενο του εγκλήματος υπό την έννοια ότι η χρήση του δεν αποτελεί προαπαιτούμενο του εγκλήματος, αλλά, παρόλα αυτά, συνδέεται με κάποιο τρόπο με την εγκληματική δραστηριότητα (π.χ. μια απειλητική επιστολή που έχει αποθηκευτεί στον υπολογιστή) (HJLT 1997: 469) και μπορεί να χρησιμοποιηθεί ως απόδειξη (σύνηθες στις περιπτώσεις εύρεσης πορνογραφικού υλικού, οπότε ο υπολογιστής συχνά κατάσχεται ως αποδεικτικό στοιχείο του ότι ο κατηγορούμενος παρήγαγε, κατείχε, έλαβε και/ή διέσπειρε πορνογραφικό υλικό, π.χ. *United States v. Simons*) (CHTLJ 2000: 189).

1.5 Νέες μορφές: ανεξέλεγκτες προεκτάσεις

[6]Τέτοιο είναι το παράδειγμα του George M. Rocha από τη Β. Καρολίνα που το 1999 αντιμετώπισε κατηγορίες ότι οργάνωσε τη διάπραξη επιθέσεων με εκρηκτικές ύλες (βομβαρδισμούς) σε καταστήματα πώλησης ειδών σπιτιού και απείλησε με τη συνέχισή τους αν δεν λάμβανε το ποσό των 250.000 δολαρίων σε λογαριασμό που διέθετε στη Λετονία. Στην προκειμένη περίπτωση το FBI κατόρθωσε τον εντοπισμό του και ανέστειλε τη δράση του.

Ο κυβερνοχώρος παρέχει ένα οπλοστάσιο εργαλείων για την εκδήλωση εγκληματικών συμπεριφορών και τη διαιώνιση μιας εγκληματικής δραστηριότητας. Σε κάποιες περιπτώσεις πρόκειται για εγκλήματα του παραδοσιακού Ποινικού Δικαίου (κατά μια διατύπωση 'old wine in new bottles') που δύνανται να διαπραχθούν τόσο σε «κοινό» περιβάλλον όσο και στο Διαδίκτυο, ενώ σε άλλες περιπτώσεις, για αμιγώς (γνήσια) ηλεκτρονικά εγκλήματα που συνιστούν νέες μορφές που αναπτύχθηκαν με την είσοδο των νέων τεχνολογιών στη ζωή μας (ACLR 2017: 1028-1034, Katyal 2001: 1023-1027). Πρόσθετα, το φάσμα των προσβολών που αποδίδονται στη νέα εποχή δεν είναι πεπερασμένο, δοθείσης της διαρκούς προόδου της τεχνολογίας και της εφευρετικότητας των δραστών. Συνεπώς, οι προσπάθειες ταξινόμησης των επιμέρους μορφών δεν είναι εξαντλητικές, αλλά στοχεύουν στην πληρέστερη κατανόηση με σκοπό την αποτελεσματική πρόληψη και καταστολή. Παρακάτω, παρατίθενται κάποιες από τις συνηθέστερες μορφές με γνώμονα το σημαντικό οικονομικό και κοινωνικό αντίκτυπο που συνεπάγονται σε επίπεδο ατόμων, επιχειρήσεων και κοινωνίας.

1.5.1 Μη εξουσιοδοτημένη πρόσβαση (hacking και cracking)

Ο όρος hacking αναφέρεται στη μη εξουσιοδοτημένη πρόσβαση σε έναν υπολογιστή, ένα πληροφοριακό σύστημα ή πρόγραμμα (Lewis 2004: 1354-1355) που στην πρώιμη διάστασή του[7] και ιδίως πριν την εδραίωση του ηλεκτρονικού εμπορίου, δεν έφερε συνήθως κακόβουλο χαρακτήρα,[8] γι' αυτό και αντιμετωπιζόταν αρχικά με κάποια ανοχή έναντι του όρου cracking που αποδίδεται συνήθως σε δράστες που δρουν με σκοπό την κακόβουλη εισβολή (Grabosky 2016: 10). Σύμφωνα με εκτιμήσεις του Sterling, συγγραφέα του βιβλίου *The Hacker Crackdown: Law and Disorder on The Electronic Frontier*, στα μέσα της δεκαετίας του 1990 ο συνολικός αριθμός των hackers ανερχόταν γύρω στις 100.000 από τους οποίους περίπου 10.000 ανήκαν στην κατηγορία των αφοσιωμένων και εμμονικών οπαδών των υπολογιστών και ένα ποσοστό μεταξύ 250-1.000 ανήκαν στην κατηγορία της ελίτ που διέθετε την απαιτούμενη τεχνική γνώση για να διεισδύσει σε συστήματα υπολογιστών και να διαταράξει την ασφάλειά τους (Sinrod & Reilly 2000: 183). Οι εκπρόσωποι των δύο αυτών κατηγοριών δεν τύγχαναν της ίδιας νομικής αντιμετώπισης εξαρτώμενης της μεταχείρισής τους από τον τρόπο της

[7] Γνώριμη είναι άλλωστε η πρώιμη έννοια της ηθικής των hackers (hacker ethic) που εδράζεται στις ηθικές αξίες και τη φιλοσοφία τους, ιδωμένου του έργου τους ως χρήσιμου και επιβοηθητικού (Levy 1984).
[8] Ευθεία αντιδιαστολή από τον όρο cracking.

εισβολής, τη χρησιμοποιούμενη μέθοδο, το είδος και το μέγεθος της βλάβης και την πρόθεση του δράστη. Για τους πρώτους η πρόθεση ταυτιζόταν συχνά με την καλοπροαίρετη διείσδυση σε υπολογιστές και συστήματα ασφαλείας με σκοπό την εύρεση των αδυναμιών και την επιδιόρθωσή τους. Στη σύγχρονη εποχή, υπό το φως της σκέψης ότι, για την ασφάλεια των δεδομένων που διακινούνται στο Διαδίκτυο, πρέπει να ικανοποιούνται οι απαιτήσεις της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων, ανεξάρτητα από την επέλευση ζημίας με πιθανή καταστροφή ή τροποποίηση δεδομένων και την αποκόμιση παράνομου περιουσιακού οφέλους, προωθήθηκε σε διεθνές επίπεδο η ανάγκη της ποινικοποίησης της άνευ δικαιώματος και εκ προθέσεως πρόσβασης στο σύνολο ή σε μέρος ενός συστήματος υπολογιστή (Δαλακούρας 2018: 5-6). Οι κύριες μορφές επιθέσεων πραγματοποιούνται δια της διασποράς κακόβουλου λογισμικού (malicious code) που συνίσταται σε αυτοαναπαραγόμενα προγράμματα που εισβάλλουν σε ένα σύστημα και στοχεύουν να πλήξουν δεδομένα και συστήματα υπολογιστή, με συνηθέστερα παραδείγματα τα εξής:[9]

- **Ιοί (viruses)**

Οι ιοί περιγράφουν προγράμματα που, με την εισβολή σε ένα υπολογιστή, τροποποιούν άλλα εγκατεστημένα προγράμματα, με τρόπο που το αρχικώς υγιές πρόγραμμα μεταλλάσσεται από τον ιό. Ο συνήθης τρόπος εξάπλωσής τους είναι μέσω μολυσματικού αρχείου από έναν κεντρικό υπολογιστή σε έναν άλλο, που μεταδίδεται με τη μεσολάβηση της ανθρώπινης δραστηριότητας π.χ. μέσω μηνύματος ηλεκτρονικού ταχυδρομείου είτε μέσω μιας κοινής δισκέτας. Χωρίς να είναι εγγενώς βλαπτικοί, μπορούν να επηρεάσουν την ομαλή λειτουργία του υπολογιστή εγκαθιστώντας κακόβουλο λογισμικό, καταστέλλοντας τη λειτουργία του ή διαγράφοντας αρχεία.

- **Σκουλήκια (Worms)**

Μοιράζονται κοινά στοιχεία με τους ιούς, αλλά η παραπάνω δυσκολία εξουδετέρωσής τους έγκειται στο ότι η μετάδοσή τους δεν προϋποθέτει τη μεσολάβηση της ανθρώπινης δραστηριότητας, αλλά αρκεί η χρήση ενός δικτύου υπολογιστή για να πολλαπλασιαστούν. Στις πιο σοβαρές περιπτώσεις περιλαμβάνεται το Stuxnet worm, που κατασκευάστηκε από την Κυβέρνηση των ΗΠΑ για την ανακοπή της κατασκευής

[9] Από τις πλέον καταστροφικές μορφές είναι το destructive malware που διαγράφει όλα τα αρχεία του μολυσμένου συστήματος και εμφανίζει ελάχιστες πιθανότητες ανάκτησης.

πυρηνικών όπλων στο Ιράν προκαλώντας αυτοκαταστροφή 984 φυγοκεντρητών εμπλουτισμού ουρανίου, μια ενέργεια που πυροδότησε σενάρια κυβερνοπολέμου (Holloway 2015).

- **Λογικές βόμβες (Logic Bombs)**

Οι λογικές βόμβες είναι προγράμματα που υποδεικνύουν σε ένα σύστημα την εκτέλεση συγκεκριμένων οδηγιών σε συγκεκριμένη χρονική στιγμή και υπό συγκεκριμένες προϋποθέσεις, άλλως, παραμένουν ανεξιχνίαστες μέχρι να ενεργοποιηθούν σε συγκεκριμένη ημερομηνία και ώρα. Με την ενεργοποίησή τους συνήθως προκαλούν ζημιά στο σύστημα ή μπορούν να χρησιμοποιηθούν για τη διευκόλυνση εγκλήματος στον πραγματικό κόσμο, λειτουργία που συνιστά και τη συνήθη χρήση τους.

- **Δούρειος Ίππος (Trojan Horses)**

Όπως μαρτυρεί η ονομασία του, πρόκειται για φαινομενικά αθώο πρόγραμμα που φαίνεται να επιτελεί χρήσιμες λειτουργίες για τον υπολογιστή, αλλά στην πραγματικότητα ενσωματώνει κακόβουλο λογισμικό που μπορεί να αποτελέσει τη δίοδο για την είσοδο ιού στον υπολογιστή ή για την πρόσβαση μη εξουσιοδοτημένου χρήστη.

- **Δίκτυο Μπότνετ (Botnet)**

Συντομογραφία του δικτύου ρομπότ (robot network), περιγράφει έναν αριθμό συσκευών συνδεδεμένων με το Διαδίκτυο (bots, zombies), μολυσμένων με κακόβουλο λογισμικό που τελούν υπό τις εντολές και τον έλεγχο ενός χειριστή (botherder) με στόχο την κλοπή προσωπικών ή οικονομικών πληροφοριών ή την επιτέλεση λειτουργιών, όπως η αποστολή ανεπιθύμητων μηνυμάτων, η επίθεση άρνησης υπηρεσιών ή η κλοπή ταυτότητας.

- **Ransomware**

Άλλο ένα κακόβουλο λογισμικό που πλήττει συστήματα υπολογιστών και με την είσοδό του ανακόπτει την πρόσβαση του χρήστη στα προσωπικά του δεδομένα και τον απειλεί με δημοσιοποίηση αυτών μέχρι την απόσπαση κάποιου χρηματικού ποσού, συχνά στη μορφή bitcoin. Πρόκειται για τεχνική δυνάμει της οποίας οι δράστες, εκμεταλλευόμενοι τις αδυναμίες συστημάτων στα οποία μεταφέρουν κακόβουλο

λογισμικό κατά την πλοήγηση στο Διαδίκτυο, μπλοκάρουν όλες τις λειτουργίες του υπολογιστή. Νεότερη μορφή του ιού αυτού αποτελεί το Cryptolocker-Cryptowall που κρυπτογραφεί όλα τα δεδομένα υπολογιστή και ζητάει λύτρα για την αποκρυπτογράφηση.

- **Επίθεση Άρνησης Υπηρεσιών (Denial of Service-DDoS Attacks)**

Σε τέτοιες περιπτώσεις ο υπολογιστής υπερφορτώνεται με σειρά αιτημάτων σε βαθμό που παρακωλύεται η επικοινωνία με άλλους υπολογιστές και εξουσιοδοτημένους χρήστες. Στην πράξη χρησιμοποιούνται δίκτυα τρίτων θυμάτων για να κατακλυστούν στοχευμένες ιστοσελίδες. Η εισβολή διευκολύνεται μέσω της μη εξουσιοδοτημένης πρόσβασης και εγκατάστασης λογισμικού που καθιστά το σύστημα κυρίαρχο (Master) και της παράλληλης εισβολής σε άλλα δίκτυα που μετατρέπονται σε πράκτορες (zombies, slaves). Χαρακτηριστικό τέτοιο παράδειγμα είναι αυτό του δεκαπεντάχρονου 'MafiaBoy' που κατάφερε να ρίξει συστήματα, όπως η Yahoo!, Amazon.com, Buy.com, E*Trade, CNN.com. και καταδικάστηκε σε μόλις οκτώ μήνες φυλάκισης (FCJ-057-Montreal Youth Court). Με παραδοσιακούς όρους τέτοιες επιθέσεις μπορούν να παρομοιαστούν με την τηλεφωνική παρενόχληση του προηγούμενου αιώνα, πλην όμως, με τους ίδιους όρους, μολονότι προκαλούν «βλάβη» δε μπορούν να χαρακτηριστούν εγκληματικές, καθότι το αποτέλεσμα δεν εμπίπτει στις παραδοσιακές έννοιες της ζημίας ή καταστροφής (Brenner 2007: 776).

- **Ανεπιθύμητη αλληλογραφία (Spamming)**

Πρόκειται για μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται μέσω του Διαδικτύου και φαινομενικά διαφημίζουν προϊόντα και υπηρεσίες με πραγματικό σκοπό τη διασπορά ιών ή άλλων κακόβουλων λογισμικών. Μολονότι το πιο γνωστό είδος spam είναι το ανεπιθύμητο e-mail, ο όρος καταλαμβάνει και άλλες μορφές ανεπιθύμητης επικοινωνίας, όπως μηνύματα που στοχεύουν να πλήξουν συστήματα άμεσης αποστολής μηνυμάτων, ιστολόγια, συστήματα Wiki και Usenet, και φόρουμ Διαδικτύου.

- **Ηλεκτρονικό «ψάρεμα» (Phishing)**

Άλλο ένα φαινομενικά αθώο μήνυμα ηλεκτρονικού ταχυδρομείου που εμφανίζει συνήθως ως αποστολέα μια αξιόπιστη πηγή, όπως π.χ. τη συνεργαζόμενη με τον παραλήπτη Τράπεζα και στοχεύει να αποσπάσει προσωπικά δεδομένα από τον

παραλήπτη. Στοχεύει στο «ψάρεμα» τραπεζικών και προσωπικών δεδομένων μέσα από πλαστές στην πραγματικότητα ιστοσελίδες που προσομοιάζουν στις πραγματικές. Τα κέρδη ανέρχονται σε περισσότερα από 1 δισεκατομμύρια το χρόνο. Διακρίνεται από το pharming το οποίο τελείται με ανακατεύθυνση της ιστοσελίδας την οποία πληκτρολογεί το θύμα σε άλλη πλαστή ιστοσελίδα-παγίδα που έχει κατασκευαστεί από το δράστη με σκοπό την υφαρπαγή των δεδομένων του θύματος. Παρεμφερή προς το phising είναι το vishing (voice phising) που αποσκοπεί στην κλοπή των τραπεζικών και προσωπικών δεδομένων μέσω ηχογραφημένου μηνύματος (Voice over IP) ενημερώνοντας το λήπτη ότι παρατηρήθηκε κάποια ύποπτη κίνηση στο λογαριασμό του και καλώντας τον να εισαγάγει τα προσωπικά του στοιχεία για να επιβεβαιώσει ή μη τη φερόμενη συναλλαγή, και το smishing που λαμβάνει χώρα μέσω μηνυμάτων που περιέχουν υπερσυνδέσμους με αποστολείς συνήθως πενταψήφια νούμερα.

1.5.2 Η ψηφιακή διάσταση του παραδοσιακού εγκλήματος

- **Κλοπή ταυτότητας (identity theft)**

Η πράξη συντελείται όταν κάποιο πρόσωπο αποκτήσει πρόσβαση χωρίς σχετικό προς τούτο δικαίωμα, μέσω π.χ. παραβίασης των κωδικών ασφαλείας, στην ψηφιακή ταυτότητα ενός άλλου προσώπου, την οποία χρησιμοποιεί συνήθως για διάπραξη αξιόποινων πράξεων. Πρόκειται για ευρύ όρο που χρησιμοποιείται σε περίπτωση κλοπής των προσωπικών στοιχείων κάποιου ατόμου για τη δημιουργία ενός νέου λογαριασμού, την πραγματοποίηση μιας αγοράς ή τη διάπραξη απάτης. Ως εκ τούτου, ενέχει την έννοια του σφετερισμού με σκοπό την πρόκληση ζημίας και αναλύεται σε εγκληματική κλοπή ταυτότητας για τη διάπραξη μιας προσβολής που φαινομενικώς προέρχεται από το θύμα της κλοπής, οικονομική κλοπή ταυτότητας για την απόκτηση και χρήση αριθμών τραπεζικών καρτών[10], αγαθών ή υπηρεσιών, μίμηση της ταυτότητας άλλου στην καθημερινή ζωή (χαρακτηριστικό παράδειγμα είναι η δημιουργία ψεύτικων προφίλ σε διαδικτυακές πλατφόρμες), κλοπή ιατρικής ταυτότητας για τη λήψη ιατρικών προϊόντων και υπηρεσιών και κλοπή παιδικής ταυτότητας για αθέμιτους σκοπούς (Viano 2017: 74).

[10] Το 2013 σημαντικός αριθμός Αμερικανών εμπόρων και περισσότεροι από 70 εκατ. πελάτες υπήρξαν θύματα κλοπής των προσωπικών τους δεδομένων. Η μείωση των κερδών σε σχέση με την προηγούμενη χρονιά μειώθηκε κατά 45% και το κόστος για την αποκατάσταση των καρτών και της ασφάλειας εκτιμήθηκε στα 100 εκατ. δολάρια (Harris 2014).

- **Διαδικτυακές απάτες (fraud)**

Με ένα γενικό ορισμό η διαδικτυακή απάτη μπορεί να αποτυπωθεί ως η συνειδητή παραπλάνηση κάποιου με σκοπό την παράνομη αποκόμιση οφέλους συνεπεία της απατηλής συμπεριφοράς. Μορφή διαδικτυακής απάτης αποτελούν τα γνωστά νιγηριανά μηνύματα ηλεκτρονικού ταχυδρομείου ('advance fee fraud', 'Nigerian advance fee fraud', '419 fraud') που πλέον έχουν επεκταθεί χωρικά και υπόσχονται αντάλλαγμα στους λήπτες με την προοπτική να βοηθήσουν οι τελευταίοι τον αποστολέα να μεταφέρει χρήματα. Σύμφωνα με εκτιμήσεις της Ομοσπονδιακής Επιτροπής Εμπορίου το 2018 προκάλεσαν στα θύματα ζημία 148 δισ. δολαρίων (Yuccas 2019). Στην ψηφιακή εποχή φαινόμενα απάτης εμφανίζονται με πλείονες μορφές μεταξύ των οποίων τραπεζικές και επενδυτικές απάτες, απατηλές φιλανθρωπικές εκστρατείες[11] και απατηλές πωλήσεις προϊόντων και υπηρεσιών.[12] Μεταξύ αυτών, συνήθη μορφή απάτης με ιδιαίτερα επιζήμιες επιπτώσεις αποτελούν οι επενδυτικές απάτες (Investment Fraud), οι οποίες συντελούνται με υποσχέσεις για υψηλά και άμεσα κέρδη σε μετοχές, αμοιβαία κεφάλαια και ούτω καθεξής. Το 2018 το Διεθνές Οικονομικό Φόρουμ επεσήμανε ότι η απάτη και το οικονομικό έγκλημα αποτελούν βιομηχανία 3 δισ. δολαρίων. Το 2017 τα θύματα ηλεκτρονικής απάτης έχασαν πάνω από 1,4 δισ. διεθνώς. Η συνολική αξία απατηλών συναλλαγών που διενεργήθηκαν με κάρτες το 2016 εντός της ζώνης SEPA (Single Euro Payments Area) ανήλθε στα 1,8 δισ. (ECB 2018: 5th Report on Card Fraud), καθώς επίσης, το ίδιο έτος η Βρετανική πλατφόρμα ασφάλειας Get Safe Online Ltd. και το Εθνικό Γραφείο Πληροφοριών για την Απάτη δήλωσαν ότι το κόστος στην οικονομία του Ηνωμένου Βασιλείου έφτασε σχεδόν τις 11 δισ. Λίρες (Business Insurance Report 2017).

[11] Το Φεβρουάριο του έτους 2016 στην ιστοσελίδα Go Fund Me περιλήφθηκε αίτημα χρηματικής υποστήριξης της Mila, ενός κοριτσιού που δηλωνόταν ως καρκινοπαθής. Η σχετική δημοσίευση κοινοποιήθηκε 591 φορές στο Facebook και το Twitter και συγκεντρώθηκαν $6.110 από 802 δωρητές μέχρι να αποκαλυφθεί πως επρόκειτο για απάτη. Αντίστοιχη είναι η περίπτωση της φερόμενης ως πάσχουσας από λευχαιμία Mandy Wilson, μιας περίπτωσης που ανέδειξε το σύνδρομο Munchausen ως ψυχική διαταραχή που αφορά άτομα που ψευδώς παρουσιάζονται στα μέσα κοινωνικής δικτύωσης ως πάσχοντες σοβαρών ή θανατηφόρων ασθενειών (Owen, Noble & Speed 2017: 223-224).

[12] Πλέον χαρακτηριστικό είναι το παράδειγμα της αμερικανικής εταιρείας "Xclusive Leisure and Hospitality", που μέσω της ιστοσελίδας "Beijing 2008 Ticketing" , προμηθεύτριας των εισιτηρίων των Ολυμπιακών Αγώνων του Πεκίνο του 2008, ενήργησε πωλήσεις πλαστών εισιτηρίων αξίας 50 δισ. δολαρίων.

1.5.3 Φαινόμενα εποχής

- **Εκφοβισμός και παρενόχληση στο Διαδίκτυο**

Στο χώρο του Διαδικτύου η ελευθερία της έκφρασης βρήκε πρόσφορο έδαφος, επιτρέποντας, ταυτόχρονα τη διασπορά λόγου που μπορεί να αποβεί προβληματικός εγείροντας νομικά ζητήματα σύγκρουσης δικαιωμάτων. Παράλληλα, τη νομική οριοθέτηση της ελευθερίας της έκφρασης και τον καθορισμό των επιτρεπόμενων ορίων άσκησης του δικαιώματος δυσχεραίνει η ρευστότητα του Διαδικτύου.[13] Η πράξη ανέδειξε φαινόμενα διαδικτυακής παρενόχλησης και βίας που διαφοροποιούνται ως προς το σκοπό και το κίνητρο του δράστη, και αντανακλώνται στους όρους cyberbullying, cyber-harassment και cyberstalking.[14] Τα φαινόμενα αυτά σε ορισμένες έννομες τάξεις τιμωρούνται ξεχωριστά είτε άλλοτε υπό έναν κοινό ορισμό, ενώ σε άλλες περιπτώσεις, τα θύματα πρέπει να θεμελιώσουν την αξίωσή τους σε έννοιες όπως η δυσφήμιση, η παραβίαση της ιδιωτικότητας ή η από πρόθεση πρόκληση συναισθηματικής δυσφορίας.[15]

Η ανυπολόγιστη δυναμική της διαδικτυακής βίας ως από πρόθεση επιθετικής συμπεριφοράς που παραβιάζει την προσωπική σφαίρα του ατόμου[16], γίνεται αντιληπτή στο παράδειγμα της Megan Taylor Meier (United States v. Drew), μιας δεκατετράχρονης έφηβης από την Αμερική που οδηγήθηκε στην αυτοκτονία το 2006 εξαιτίας εκφοβισμού που δεχόταν στον ιστότοπο κοινωνικής δικτύωσης MySpace. Η υπόθεση στάθηκε αφορμή για να τροποποιηθεί ο ομοσπονδιακός ποινικός κώδικας των ΗΠΑ (‘Megan

[13] Σε πολλές έννομες τάξεις ποινικοποιείται η μετάδοση επικοινωνίας με απειλητικό περιεχόμενο και η χρήση συσκευών επικοινωνίας για την ανώνυμη ενόχληση, κακοποίηση, παρενόχληση ή απειλή που τελείται από το δράστη προς το θύμα, ωστόσο, προβληματική μπορεί να είναι η αντιμετώπιση καταστάσεων που ο δράστης ενθαρρύνει τρίτα μέρη σε παρενόχληση του θύματος (Katyal 2001: 1035).

[14] Η κλινική εγκληματολογία εντάσσει το cyberstalking στις υποκατηγορίες του cyberbullying, ενώ εντάσσει σε διαφορετική κατηγορία το cyberharassment, το οποίο εμφανίζει τα ίδια χαρακτηριστικά με το cyberbullying αλλά διαφοροποιείται ως προς το ηλικιακό κοινό που προσβάλλει. Θύματα του τελευταίου είναι τα παιδιά ενώ του πρώτου οι ενήλικες. Άλλα φαινόμενα που μοιράζονται κοινά στοιχεία περιλαμβάνοντας αποδοκιμαζόμενες επιθετικές συμπεριφορές, πυροδοτούμενες από διασκέδαση, ανία ή εκδίκηση, σε βάρος συγκεκριμένων ατόμων για φυσικά ή συμπεριφορικά χαρακτηριστικά που φέρουν, συνοδευόμενα από τη συνήθως ανώνυμη απειλή βίας με στόχο την υπονόμευση του θύματος, αποτελούν η ρητορική μίσους (hate speech) και το trolling (Owen, Noble & Speed 2017: 113-139).

[15] Παρά τον αντίκτυπο για το θύμα της προσβολής, το δικαίωμα στην ελευθερία του λόγου και της έκφρασης δεν αποκλείεται κατά περίπτωση να θέσει εκποδών την αξίωση του θύματος (Jameson 2008: 237-246).

[16] Ο Nietzshe στο έργο του On the Genealogy of Morality (1887) προσεγγίζει την εξωτερικευόμενη κακία ως την τάση ατόμων μέτριων πασχόντων από συναισθηματική ανεπάρκεια που επιδιώκουν να στηλιτεύσουν τα επιτεύγματα άλλων πιο αδύναμων χαρακτήρων προκειμένου να αναδείξουν τη δική τους νομιζόμενη αξία.

Meier Cyberbullying Prevention Act') προκειμένου να περιλάβει ποινικές κυρώσεις σε όσους μεταδίδουν στο διακρατικό ή ξένο εμπόριο μια επικοινωνία που αποσκοπεί στο να εξαναγκάσει, να εκφοβίσει, να παρενοχλήσει ή να προκαλέσει ουσιαστική συναισθηματική δυστυχία σε άλλο άτομο χρησιμοποιώντας ηλεκτρονικά μέσα για την υποστήριξη σοβαρής, επαναλαμβανόμενης και εχθρικής συμπεριφοράς.[17] Άλλο παράδειγμα και συνάμα μία από τις πρώτες γνωστές περιπτώσεις cyber bullying είναι αυτό του καναδού φοιτητή Chyslain Raza γνωστού με το προσωνύμιο Star Wars Kid. Ο Raza, οπαδός της ομώνυμης σειράς ταινιών, βιντεοσκόπησε τον εαυτό του να υποδύεται έναν τζεντάι, αλλά κάποιοι συμφοιτητές του βρήκαν το βίντεο και το ανήρτησαν στο Διαδίκτυο. Το βίντεο, το οποίο εμπλουτίστηκε με ηχητικά και οπτικά εφέ, οδήγησε τον πρωταγωνιστή του σε κατάθλιψη. Παρά τις μηνύσεις που υπέβαλε κατά των ιθυνόντων, το βίντεο από το 2002 παραμένει ανηρτημένο στο Διαδίκτυο,[18] ενώ έχει αναπαραχθείσε τέτοιο βαθμό που φαίνεται αδύνατο να παύσει η δημόσια προβολή του (Brenner 2007: 724-725).

1.5.4 Παιδική πορνογραφία (child pornography) και grooming

Στο απόγειο των δυνατοτήτων του Διαδικτύου η βιομηχανία παιδικής πορνογραφίας έλαβε διαστάσεις διεθνούς κρίσης ευνοούμενης από τις τεχνικές του Διαδικτύου και ενίοτε από τη νομοθεσία (π.χ. το κατέβασμα αρχείου JPEG που περιέχει το απαγορευμένο υλικό είναι παράνομο για όλους άρα και για τις αρχές). Πρόκειται δε για τη δεύτερη πιο προσοδοφόρα δραστηριότητα μετά το εμπόριο ναρκωτικών με κέρδη περισσότερα από 3 δισεκατομμύρια το χρόνο. Σύμφωνα με στοιχεία του μη κερδοσκοπικού οργανισμού NCMEC, το 2008, 70.000 άτομα ταυτοποιήθηκαν ως συνδρομητές υλικού παιδικής πορνογραφίας, ενώ το 2007 ελήφθησαν 500.000 αναφορές για εγκλήματα παιδικής πορνογραφίας και εκμετάλλευσης (Richards 2008: 513). Μολονότι η σχετική νομοθεσία έχει ενισχυθεί σημαντικά οι δυσκολίες που σχετίζονται με την εξιχνίαση και τη χρηματοδότηση απαιτούν οργανωμένες ενέργειες σε κρατικό και ιδιωτικό επίπεδο.[19] Η τακτική του grooming ειδικότερα, περιγράφει το φαινόμενο της αποπλάνησης κατά το οποίο ο δράστης προσεγγίζει ανήλικα θύματα αποκτώντας την

[17] Διαθέσιμο στο https://www.congress.gov/bill/111th-congress/house-bill/1966
[18] Διαθέσιμο στο http://news.bbc.co.uk/2/hi/entertainment/6187554.stm
[19] Αξιοσημείωτο είναι το ότι το μεγαλύτερο μέρος της χρηματοδότησης προέρχεται από τη βιομηχανία ενηλίκων με σημαντικότερους χρηματοδότες το Hustler, το Playboy και τη Wicked Pictures.

εμπιστοσύνη τους προκειμένου να τα συναντήσει και να τα ωθήσει σε σεξουαλικές πράξεις. Συνιστά έναν από τους μεγαλύτερους κινδύνους στο Διαδίκτυο εφόσον ο δράστης μπορεί εύκολα να αποκρύπτει την πραγματική του ταυτότητα και να εμφανίζεται ως συνομήλικος του παιδιού με το οποίο συνομιλεί (Davidson & Gottsehalk 2011:43).

1.5.5 Η άνοδος του κυβερνοπολέμου (cyber-war) και η προβληματική του δόγματος της μη παρέμβασης (The doctrine of non-intervation)

Παρότι η χρήση του όρου του πολέμου στον Κυβερνοχώρο δεν ικανοποιεί επαρκώς τις απαιτήσεις του νομικού πλαισίου για τον πόλεμο στον πραγματικό κόσμο (Law of War) και την επιτρεπόμενη χρήση βίας (use of force) σε απάντηση μιας ένοπλης επίθεσης (armed attacks)[20] η παρεμβολή σε υποδομές ζωτικής σημασίας (critical infrastructure) ενός Κράτους, μπορεί να επιφέρει καταστροφικές οικονομικές απώλειες και να πλήξει άμεσα το βιοτικό επίπεδο συνεπιφέροντας επιπτώσεις που συναντώνται σε καιρό πολέμου (Antolin-Jenkins 2005: 135). Αντιμετωπίζοντας τις διαδικτυκές επιθέσεις στις υποδομές ζωτικής σημασίας ως κυβερνοπόλεμο, η Κυβέρνηση των ΗΠΑ έχει αναπτύξει ειδικά συστήματα για την καταπολέμηση της απειλής, όπως το 'STRATCOM' (U.S. Strategic Command), τμήμα του Υπουργείου Δικαιοσύνης που παρακολουθεί τις επιθέσεις και τα εθνικά συστήματα διαδικτυακής ασφάλειας Einstein 2 και Einstein 3 εγείροντας, ωστόσο, ζητήματα υπέρμετρης παραβατικότητας της Κυβέρνησης και παραβίασης των ατομικών δικαιωμάτων.[21] Η προβληματική επεκτείνεται σε ό, τι αφορά τα επιτρεπόμενα όρια δράσης. Σύμφωνα με τους ορισμούς του Διεθνούς Δικαίου, τα Κράτη οφείλουν να μην παρεμβαίνουν στις εσωτερικές και εξωτερικές υποθέσεις άλλων κρατών (The doctrine of non-intervation). Εξορμούμενο από την αντίληψη του *domaine réservé* ως χώρου μη πρωταρχικά ρυθμιζόμενου από το Διεθνές Δίκαιο, το Διεθνές Δικαστήριο της Χάγης ορίζει την απαγορευμένη επέμβαση ως εκείνη που σχετίζεται με θέματα, για τα οποία κάθε Κράτος, δυνάμει της αρχής της κυριαρχίας (principle of sovereignty) διαθέτει το δικαίωμα να αποφασίζει ελεύθερα. Παρά ταύτα, ο διασυνοριακός χαρακτήρας του Διαδικτύου και η αυξανόμενη πρόσδεση των Κρατών στην τεχνολογία, δημιούργησαν

[20] Υπό το φως του άρθρου 24 του Χάρτη των Ηνωμένων Εθνών, τα Κράτη οφείλουν να απέχουν από τη χρήση βίας και την απειλή χρήσης βίας έναντι της εδαφικής ακεραιότητας ή της πολιτικής ανεξαρτησίας κάθε Κράτους με μόνη εξαίρεση αυτή του άρθρου 51 για την περίπτωση ένοπλης επίθεσης.

[21] Στην Κίνα λειτουργούν στρατιωτικές ενώσεις κατά του κυβερνοπολέμου, ενώ η Ρωσία εφαρμόζει το δόγμα του κυβερνοπολέμου αντιμετωπίζοντας τις διαδικτυακές επιθέσεις ως πολλαπλασιαστές ισχύος. Η Β. Κορέα έως το 2012 είχε 121 αντίστοιχες ενώσεις.

φαινόμενα παρέμβασης (Schmitt 2017: 312-315) και γέννησαν ερωτήματα για το αν οι διαδικτυακές επιθέσεις δύνανται να παραβιάζουν την εδαφική ακεραιότητα.[22] Στην πράξη η παρέμβαση μεταφράζεται με όρους κατασκοπείας, επιτήρησης και λοιπές μορφές ζημίας σε ένα αντίπαλο πληροφοριακό σύστημα, ώστε την τελική απάντηση, σε επίπεδο κρατών, καλείται να δώσει το Διεθνές Δίκαιο επί τη βάσει των κανόνων της αυτοάμυνας, της αναγκαιότητας, της αναλογικότητας, της ελαχιστοποίησης της βλάβης σε αμέτοχα τρίτα μέρη και της αποφυγής των παράπλευρων απωλειών (Grabosky 2016: 45-48).

1.5.6 Τρομοκρατία στο Διαδίκτυο (cyber-terrorism) και επιτήρηση (surveillance)

Μολονότι δεν υπάρχει ακριβής νομικός ορισμός, ο Denning αναλύει αυτής της μορφής την τρομοκρατία ως μη νόμιμη επίθεση σε υπολογιστές, δίκτυα και πληροφορίες αποθηκευμένες σε αυτούς με σκοπό τον εκφοβισμό ή τον εξαναγκασμό μιας Κυβέρνησης ή ενός λαού στην προώθηση πολιτικών ή κοινωνικών σκοπών. Τυπικά εννοείται ως κρατική δράση ισοδύναμη με μια ένοπλη επίθεση ή χρήση βίας στο Διαδίκτυο που μπορεί να πυροδοτήσει στρατιωτική αντίδραση με ανάλογη χρήση βίας (Rollins 2015: 1) και που στοχεύει να πλήξει υποδομές ζωτικής σημασίας (critical infrastructure), στις οποίες περιλαμβάνονται οι επικοινωνίες, η ηλεκτρική ενέργεια, το σύστημα εναέριου ελέγχου και το χρηματοπιστωτικό σύστημα. Το παράδειγμα της επίθεσης της 11ης Σεπτεμβρίου στο Κέντρο Διεθνούς Εμπορίου (World Trade Center) που άλλαξε ριζικά το νομοθετικό πλαίσιο για την παρακολούθηση και τον περιορισμό της τρομοκρατίας στις ΗΠΑ[23], αποτελεί ένα από τα πλέον κομβικά σημεία της σύγχρονης ιστορίας με εκτιμώμενες οικονομικές απώλειες 3,2 δισ. σε συστήματα πληροφοριών.[24] Άλλο παράδειγμα είναι αυτό του Ardit Ferizi (USA v. Ardit Ferizi), του πρώτου ατόμου που δικάστηκε για διαδικτυακή τρομοκρατία στις ΗΠΑ το 2015 και καταδικάστηκε σε 20 χρόνια φυλάκισης για κλοπή προσωπικών δεδομένων 1.300 στρατιωτικών και ομοσπονδιακών υπαλλήλων που έδωσε στον ISIS (Gronin 2019). Στον αντίποδα, η αναδυόμενη ανάγκη για επιτήρηση

[22] Φυσικά από μια άλλη σκοπιά η καταφατική απάντηση στο ερώτημα και η υπό εξέταση επιτρεπόμενη επέκταση της χρήσης βίας του άρθρου 24 του Χάρτη των Ηνωμένων Εθνών ενέχει τον υπαρκτό κίνδυνο να ανοίξει ο ασκός του Αιόλου για την καταχρηστική εφαρμογή τακτικών οικονομικού αποκλεισμού.

[23] Βλ. USA Patriot Act

[24] Οι διαδικτυακές επιθέσεις (cyber attacks) πλήττουν ευθέως τις οικονομικές συναλλαγές και έχουν τεράστιο οικονομικό αντίκτυπο στα χρηματοπιστωτικά συστήματα. Οι οικονομικές απώλειες περιλαμβάνουν την απώλεια διανοητικής ιδιοκτησίας, την οικονομική απάτη, τη ζημία της φήμης, τη χαμηλή παραγωγικότητα και την ευθύνη τρίτου μέρους.

(online surveillance) μέσω συστημάτων παρακολούθησης (monitoring) και τεχνικών εξόρυξης δεδομένων (data mining) εγείρουν ζητήματα προστασίας των προσωπικών δεδομένων και ρευστοποιούν τα όρια ανάμεσα στο θεμιτό παρεμβατισμό και τα ατομικά δικαιώματα.

1.6 Επιμέρους προβληματικές

1.6.1 Δικαιοδοσία και έκδοση

Καίριο ζήτημα στα διασυνοριακά εγκλήματα αποτελεί η δικαιοδοσία περιλαμβάνουσα την εξουσία ενός κράτους να νομοθετεί, να εκδίδει αποφάσεις και να επιβάλλει τους κανόνες του, τρεις εκφάνσεις της δικαιοδοσίας που απορρέουν από την αρχή της εδαφικότητας ως αρχή του Διεθνούς Ποινικού Δικαίου stricto sensu. Σε περιπτώσεις που περισσότερες χώρες θεμελιώνουν δικαιοδοσία, ο προβληματισμός έγκειται στη διαπίστωση της χώρας που θα καταστεί τελικώς αρμόδια να συλλάβει τους υπόπτους και να αποφασίσει επί της δικαιοδοτικής τους μεταχείρισης, λαμβάνουσα προτεραιότητα έναντι των άλλων. Συνεπώς, υπό εξέταση είναι το ζήτημα του βαθμού στον οποίο μια χώρα μπορεί να επικαλεστεί εξωεδαφική δικαιοδοσία στο χώρο του Διαδικτύου (Koops & Brenner 2006: 2-3). Επιπλέον, δεν παραβλέπεται ότι υπάρχουν χώρες που δεν έχουν θεσπίσει νομοθεσία ή επαρκή τουλάχιστον νομοθεσία σε αναφορά με το ηλεκτρονικό έγκλημα ενώ άλλες νομοθεσίες, όπως η Μαλαισία, περιλαμβάνουν τόσο ευρείες διατάξεις που μπορούν να επικαλεστούν δικαιοδοσία για σχεδόν κάθε ηλεκτρονικό έγκλημα (Koops & Brenner 2006: 3). Από την άλλη, στο δίπολο εδαφικότητα και εθνικότητα, η πρώτη θεωρείται η κύρια και η δεύτερη η επικουρική βάση για τη θεμελίωση δικαιοδοσίας. Πρόσθετα, ακόμη και υπό μία ευρεία θέαση της δικαιοδοσίας, αυτή πρέπει να είναι δικαιολογημένη ενώ η απόφαση επί αυτού επιτυγχανεται μέσω του συνυπολογισμού περισσότερων παραγόντων, στους οποίους περιλαμβάνεται η ένταση του συνδέσμου της πράξης με το έδαφος του κράτους, η νομοθεσία του κράτους σε σχέση με το βαθμό στον οποίο τα άλλα κράτη ρυθμίζουν νομοθετικά τις σχετικές προσβολές και η σημασία της προτασσόμενης νομοθεσίας για το διεθνές πολιτικό, νομικό και οικονομικό σύστημα (Koops & Brenner 2006: 5-6).

Κλασικό παράδειγμα συνιστά η υπόθεση της Yahoo (*Licra v. Yahoo*).[25] Τα πραγματικά περιστατικά της υπόθεσης έχουν ως εξής: μια γαλλική ιστοσελίδα, αποθηκευμένη σε server στις ΗΠΑ, που πωλούσε διάφορα αντικείμενα, μεταξύ άλλων, περιελάμβανε αντικείμενα που έφεραν Ναζιστικά διακριτικά γνωρίσματα και αμφισβητούσαν ευθέως το ολοκαύτωμα των Εβραίων, γεγονός που υπό τον Γαλλικό Ποινικό Κώδικα τυποποιείται ως σοβαρό ποινικό αδίκημα στρεφόμενο κατά της ανθρωπότητας, του κράτους και της δημόσιας ασφάλειας.[26] Η Διεθνής Ένωση κατά του Ρατσισμού και του Αντισημιτισμού και η Ένωση Εβραίων Φοιτητών της Γαλλίας προέβησαν σε μήνυση στα Γαλλικά Δικαστήρια κατά της Yahoo και της Yahoo France για παραβίαση της γαλλικής νομοθεσίας με αίτημα την αφαίρεση των σχετικών συνδέσμων και την προειδοποίηση των χρηστών για το παράνομο περιεχόμενο. Η Yahoo επικαλέστηκε τοπική αναρμοδιότητα, ισχυριζόμενη ότι αρμόδια Δικαστήρια ήταν αυτά των ΗΠΑ, όπου η εν λόγω πράξη, δυνάμει της εκεί ισχύουσας νομοθεσίας (Πρώτη Τροποποίηση του Συντάγματος των ΗΠΑ), δεν ήταν αξιόποινη. Παρά ταύτα οι ισχυρισμοί απορρίφθηκαν από το Γαλλικό Δικαστήριο που έκρινε ότι υπήρχε δυνατότητα τοποθέτησης ειδικών φίλτρων προσβασιμότητας, υποχρεώνοντας τελικώς τη Yahoo! να λάβει τα απαιτούμενα μέτρα που είναι σε θέση να εφαρμόσει σε τεχνικό επίπεδο, αποκλείοντας την πρόσβαση στους χρήστες που περιηγούνται από γαλλικούς servers και προειδοποιώντας για το παράνομο με βάση τη γαλλική νομοθεσία περιεχόμενο.[27]

Σε ό, τι αφορά, περαιτέρω, στις διαδικασίες που διέπουν την έκδοση, αυτές ρυθμίζονται γενικά από τις ισχύουσες συνθήκες ανάμεσα στα συμβαλλόμενα κράτη και αφορούν κυρίως τις προσβολές εκείνες που τιμωρούνται με τουλάχιστον 1 έτος φυλάκισης και θεωρούνται πιο σοβαρές. Στην πράξη, ωστόσο, είθισται τα κράτη να μην επιθυμούν την έκδοση των δικών τους πολιτών ανεξάρτητα από το περιεχόμενο των συνθηκών.[28] Σε κάθε περίπτωση, αντανακλώντας τον προβληματισμό σε σχέση με την εθνική κυριαρχία, οι συνθήκες που ρυθμίζουν την έκδοση των φερόμενων δραστών προϋποθέτουν τη διαπίστωση ποινικώς αξιόποινης πράξης σε αμφότερα τα

[25] Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Société Yahoo! France (LICRA c. Yahoo!).
[26] Article R645-1
[27] Ορισμένοι παρατηρητές έχουν επισημάνει ότι η συγκεκριμένη υπόθεση εγκαθιδρύει καθολική δικαιοδοσία για τα γαλλικά δικαστήρια να αποφασίζουν σε σχέση με τις υποθέσεις που αφορούν στο διαδικτυακό χώρο.
[28] Πολλές χώρες ανά τον κόσμο μεταξύ των οποίων η Β. Αμερική, η Δ. Ευρώπη και η Αυστραλία διαθέτουν σχετική νομοθεσία που τους επιτρέπει την έρευνα και εκδίκαση αντίστοιχων εγκλημάτων, παρά ταύτα, υπάρχουν ακόμα κράτη στα οποία δεν έχει θεσπιστεί νομοθεσία για το ηλεκτρονικό έγκλημα.

συμβαλλόμενα μέρη (double ή dual criminality) κατ' αναλογία με τα ισχύοντα στον πραγματικό κόσμο. Μη πληρουμένης αυτής της απαίτησης η έκδοση εμφανίζεται προβληματική. Ας φέρουμε στη σκέψη μας το παράδειγμα του Goodman για την ηθοποιό του Hollywood που επισκέπτεται τη Σαουδική Αραβία ενδεδυμένη κατά τρόπο μη ευπρεπή σύμφωνα με τον αυστηρό ισλαμικό νόμο (Sharia) και επιστρέφει κατόπιν στο Los Angeles από το οποίο ζητείται η έκδοσή της για ένα ποινικό αδίκημα που δεν αναγνωρίζεται ως τέτοιο στις ΗΠΑ (Goodman 2010: 323).

1.6.2 Έρευνα και κατάσχεση

Σε αρκετά κράτη κατοχυρώνεται νομοθετικά η προστασία της ιδιωτικότητας συνιστάμενης στην ελευθερία των ατόμων απέναντι στις αδικαιολόγητες κυβερνητικές παρεμβάσεις στην προσωπική τους ζωή. Η Οικουμενική Διακήρυξη των Ηνωμένων Εθνών για τα Ανθρώπινα Δικαιώματα και το Σύνταγμα των ΗΠΑ εμπεριέχουν σχετικές διατάξεις προς τη διασφάλιση αυτών, καθώς επίσης, σύμφωνα με την Τέταρτη Τροποποίηση του Συντάγματος των ΗΠΑ απαγορεύεται στην Κυβέρνηση η διενέργεια αδικαιολόγητης ('unreasonable') έρευνας σε ένα άτομο, οικία ή εργασιακό χώρο χωρίς νόμιμη αιτία και χωρίς δικαστική απόφαση ή διάταξη. Στον ψηφιακό χώρο τα ζητήματα που σχετίζονται με την έρευνα[29] και κατάσχεση[30] του αποδεικτικού υλικού και αφορούν στην τήρηση της νομίμως προβλεπόμενης διαδικασίας διασφαλιζόμενης της μη παραβίασης των αναγνωρισμένων δικαιωμάτων του ατόμου, χωρίς ταυτόχρονα να παρακωλύεται η εξιχνίαση του ηλεκτρονικού ίχνους του δράστη, είναι περίπλοκα,[31] ιδίως αν ληφθεί υπόψη ότι η δυναμική του Διαδικτύου και οι μέθοδοι που μπορεί να επιστρατεύσει ο δράστης για να καλύψει τα ηλεκτρονικά του ίχνη απαιτούν άμεση και ταχεία δράση. Η έρευνα και η κατάσχεση του ψηφιακού υλικού, όπως και στον πραγματικό κόσμο, αποτελούν βασικά συστατικά της εξιχνίασης των εγκλημάτων, τα οποία, ωστόσο, αντιμάχονται τη δικαιολογημένη προσδοκία του ατόμου σε ιδιωτικότητα,[32] που στον ψηφιακό κόσμο είναι δύσκολο να καθοριστεί με ακρίβεια.

[29] Η έρευνα λαμβάνει χώρα όταν οι πράξεις της Κυβέρνησης παραβιάζουν το δικαιολογημένο ενδιαφέρον του ατόμου στην ιδιωτικότητα ('reasonable expectation of privacy', *Florida v. Jardines, Katz v. United States*).

[30] Σύμφωνα με τη 4η Τροποποίηση του Συντάγματος των ΗΠΑ έχει την έννοια της σημαντικής παραβίασης του ιδιοκτησιακού συμφέροντος ενός προσώπου (*US v. Jones, US v. Miller, Lavan v. City of L.A.*).

[31] Στις ΗΠΑ υπάρχει Οδηγός που έχει δημιουργηθεί από το Υπουργείο Δικαιοσύνης που περιέχει κατευθυντήριες σε σχέση με θέματα έρευνας και κατάσχεσης, US Department of Justice.

[32] Η προσδοκία αυτή εμφανίζει δύο συνισταμένες: α) την υποκειμενική προσδοκία του ατόμου και β) την αξιολόγηση της προσδοκίας ως τέτοιας που τυγχάνει κοινωνικά αποδεκτή (*Kyllo v. United States*).

Σημαντική επίσης διάκριση που παρατηρείται σε ορισμένες έννομες τάξεις, εντοπίζεται στην προστασία των οικιακών υπολογιστών σε σχέση με τους ευρισκόμενους σε χώρο εργασίας, με τους μεν πρώτους να χαίρουν καθολικής προστασίας (*United States v. Heckencamp*), τους δε δεύτερους, να εξαρτούν την προστασία τους από την ιδιαιτερότητα-σημαντικότητα της περίπτωσης (*O' Connor v. Ortega, Leventhal v. Knapel, United States v. Long*).

Έτερη προβληματική αφορά στο περιεχόμενο του προαπαιτούμενου για την έναρξη της έρευνας εντάλματος, το οποίο, μολονότι σε περιπτώσεις ηλεκτρονικών εγκλημάτων τα δικαστήρια έχουν κρίνει ότι μπορεί να λαμβάνει πιο ευρύ περιεχόμενο, οφείλει, σε κάθε περίπτωση, να εξειδικεύει το διερευνώμενο έγκλημα ή το παράνομο περιεχόμενο στο οποίο αφορά η έρευνα (*Mink v. Knox*). Σε ορισμένες περιπτώσεις έχει κριθεί ότι οι αρχές δύνανται να ερευνήσουν το σύνολο του περιεχομένου του ελεγχόμενου υπολογιστή εφόσον συντρέχει η υπόνοια ότι θα βρεθούν τα στοιχεία τα οποία εμπεριέχονται στο ένταλμα, ενώ σε ορισμένες περιπτώσεις έχει κριθεί ότι το περιεχόμενο του εντάλματος πρέπει να είναι πιο στενό (*State v. Lehman, Burnett v. State*). Στο πλαίσιο αυτό, η προστασία της ιδιωτικής ζωής εμφανίζεται έωλη. Την παρατήρηση αυτή ενισχύει η διατύπωση του δόγματος του τρίτου μέρους (third party doctrine) του Ανώτατου Δικαστηρίου των ΗΠΑ,[33] δυνάμει του οποίου, στις περιπτώσεις που τα ίδια τα άτομα μοιράζονται οικειοθελώς πληροφορίες με τρίτα μέρη, όπως για παράδειγμα οι πάροχοι υπηρεσιών Διαδικτύου, δε νομιμοποιούνται σε λογική προσδοκία ιδιωτικότητας (ACRL 2017: 1053-1054).

Επιπλέον, δε λησμονούνται τα απορρέοντα από το διασυνοριακό χαρακτήρα του ηλεκτρονικού εγκλήματος προβλήματα. Μη εξουσιοδοτημένη έρευνα μπορεί δυνητικά να οδηγήσει σε παραβίαση της κυριαρχίας ενός κράτους. Χαρακτηριστικό είναι το ακόλουθο παράδειγμα δύο Ρώσων hackers, του Alexey V. Ivanof και του Vasiliy Gorshkov, που κλήθηκαν σε ανάληψη εργασίας στην Washington φαινομενικώς για λογαριασμό της εταιρείας ασφαλείας Invita, πλην όμως, στην πραγματικότητα επρόκειτο για επιχείρηση εξιχνίασης του FBI. Σε επίδειξη των ικανοτήτων τους οι δύο hackers εισήλθαν στο περιεχόμενο των υπολογιστών τους στη Ρωσία, στο οποίο

[33] Π.χ. *Smith v. Maryland*, 442 U.S. 735, 745-46 (1979), *United States v. Miller*, 425 U.S. 435, 443 (1976), *Unites States v. Davis*, 785 F.3d 498, 512 (11th Cir. 2015), *Unites States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008)

περιλαμβάνονταν αριθμοί λογαριασμών και κωδικοί των θυμάτων τους. Πριν την έκδοση εντάλματος έρευνας, το FBI έκανε λήψη του σχετικού αποδεικτικού υλικού. Η υπερασπιστική γραμμή του Gorshkov αφορούσε αφενός σε παραβίαση από το FBI των οριζόμενων στη Τέταρτη Τροποποίηση του Συντάγματος των ΗΠΑ, δυνάμει της οποίας οι αρχές δε νομιμοποιούνται σε αδικαιολόγητες (unreasonable) έρευνες και κατασχέσεις έναντι των πολιτών, και αφετέρου, σε παραβίαση της ρωσικής νομοθεσίας. Απορριπτομένων των ισχυρισμών ο Gorshkov καταδικάστηκε σε 36 μήνες φυλάκισης και ο Ivanof σε 48 μήνες φυλάκισης. Ωστόσο, προς το σκοπό της οριοθέτησης της δικαιοδοσίας των ΗΠΑ, τον ισχυρισμό περί παραβίασης της ρωσικής νομοθεσίας πρόβαλε και η Ρωσική Αντικατασκοπεία υποκινούμενη από τη σκέψη ότι η εν λόγω υπόθεση θα άνοιγε το δρόμο προς τις μυστικές υπηρεσίες των ΗΠΑ να μετέρχονται παράνομες μεθόδους για τη συλλογή κρατικών πληροφοριών.[34]

1.7 Δυσκολίες αποτίμησης του ηλεκτρονικού εγκλήματος

Υπό τη σκέψη ότι η συλλογή στατιστικών δεδομένων στην περίπτωση του κοινού εγκλήματος οδηγεί, ίσως, σε μια ατελή αντανάκλαση της πραγματικότητας, μπορούμε να υποθέσουμε ότι πρέπει να είμαστε πολύ πιο επιφυλακτικοί στην περίπτωση του ηλεκτρονικού εγκλήματος, η αποτίμηση του οποίου προσκρούει σε μια σειρά εμποδίων. Πρώτα απ' όλα, η ταχύτητα και η ποικιλία των ηλεκτρονικών εγκλημάτων δυσχεραίνει την αποτίμηση της συνολικής ζημίας και της συχνότητας του ηλεκτρονικού εγκλήματος (Maass & Rajagopalan 2012), ενώ έτερο ανασταλτικό παράγοντα συνιστά η μη καταγγελία τέτοιων φαινομένων (McGuire & Dowling 2013). Το μεγαλύτερο ποσοστό των εταιρειών που πέφτουν θύματα επιλέγουν να μην προχωρήσουν σε αναφορά, φοβούμενες, ότι η δημοσιοποίηση θα πλήξει τη φήμη τους και την εμπιστοσύνη του καταναλωτικού κοινού ή ότι ακόμα μπορεί να αποτελέσουν έτσι προσφιλή στόχο για νέες παραβιάσεις (ACRL 2017: 1026-1027).

Σύμφωνα με τον Sokolik (1980: 353), οι τέσσερις λόγοι που εξηγούν τη διστακτικότητα αναφοράς στην περίπτωση των επιχειρήσεων συνίστανται: α) στο φόβο της απώλειας της δημόσιας πίστης, β) στις δυσκολίες απόδειξης, γ) στις αξιώσεις αστικής

[34] Η υπόθεση αποτελεί χαρακτηριστικό παράδειγμα της δυσπιστίας που περιβάλλει τα κράτη σε αναφορά με ζητήματα κρατικής κυριαρχίας και της άρνησης των κρατών να προχωρούν σε διεθνή συνεργασία.

ευθύνης στο πρόσωπο των πελατών και δ) στην πεποίθηση ότι η δημοσιοποίηση θα διαιωνίσει τη ζημία γνωστοποιώντας τις αδυναμίες των συστημάτων ασφαλείας. Δεν αποκλείεται ακόμα να θεωρηθεί πιθανό το ενδεχόμενο οι αρχές να αδυνατούν να προβούν στις δέουσες ενέργειες είτε λόγω απουσίας υποδομών είτε λόγω έλλειψης του απαιτούμενου γνωσιακού υποβάθρου και του κατάλληλου τεχνολογικού εξοπλισμού. Υπαρκτός είναι περαιτέρω ο φόβος πιθανής επανάληψης της προσβολής από τον παραβάτη ιδίως σε περιπτώσεις διαδικτυακής παρενόχλησης ή εκφοβισμού, όπου παρατηρημένα οι επιθέσεις πολλαπλασιάζονται όταν οι παραβιάσεις τύχουν της προσοχής των αρχών. Δυσκολίες εντοπίζονται περαιτέρω, ως προν τον ακριβή καθορισμό της προκαλούμενης βλάβης και των οικονομικών απωλειών, ενεχουσών των τελευταίων τον κίνδυνο της υποτίμησης του ακριβούς μεγέθους του προκαλούμενου κόστους, σε ένα περιβάλλον πεπερασμένων πόρων, όπου η σχετική σοβαρότητα του εγκλήματος, υπολογιζόμενη σε αριθμούς, καθορίζει συχνά το βαθμό της επίσημης προσοχής από τις Αρχές (Grabosky 2016: 70). Πολύ πιθανό είναι ακόμη οι παθόντες να μην αντιληφθούν ότι υπήρξαν θύματα ηλεκτρονικού εγκλήματος,[35] ενώ κι αν ακόμα το αντιληφθούν συνηθέστερο είναι να επιλέξουν να επικοινωνήσουν με τον πάροχο υπηρεσιών ή την εμφανιζόμενη πηγή προέλευσης παρά με την αστυνομία (EC 2015: 93).

1.8 Οικονομικός αντίκτυπος και κοινωνικό κόστος

Απότοκο της ψηφιακής εποχής και της άρρηκτης σύνδεσης της καθημερινότητας με την τεχνολογία, αποτελεί η προσφορά σημαντικών οικονομικών και κοινωνικών ευκαιριών, καθώς επίσης, η ανάδειξη νέων ρίσκων και ευπαθειών που επιδιώκουν να εκμεταλλευτούν οι επιδρομείς του κυβερνοχώρου. Το 2016 εκτιμάται ότι 594 εκατ. άνθρωποι παγκοσμίως έπεσαν θύματα ηλεκτρονικού εγκλήματος, γεγονός που προκάλεσε ζημίες 30 δισ. δολαρίων (Morgan 2016). Σύμφωνα με εκτιμήσεις 90 ιστοσελίδες παραβιάζονται το λεπτό, ενώ ο μέσος χρόνος ταυτοποίησης μιας παραβίασης δεδομένων είναι 196 μέρες. Το δε κόστος από παραβιάσεις δεδομένων υπολογίζεται στα 3,51 εκατ. δολάρια ετησίως, καθώς επίσης, εκτιμάται ότι έως το 2023 κυβερνοεγκληματίες θα έχουν κλέψει περίπου 33 εκατομμύρια διαδικτυακά στοιχεία. Η

[35] Σύνηθες στις περιπτώσεις των botnet: αριθμός συσκευών συνδεόμενων με το Διαδίκτυο που χρησιμοποιούνται σε εκτέλεση επιθέσεων άρνησης υπηρεσιών-DDoS, κλοπή δεδομένων ή αποστολή ανεπιθύμητων μηνυμάτων, όπως απατηλές προσκλήσεις ή επιστολές βοηθείας που ζητούν σημαντικά χρηματικά ποσά που ο παραλήπτης συνήθως επιλέγει απλά να τις μεταφέρει στον κάδο ανακύκλωσης.

αποτίμηση του συνολικού κόστους συνθέτει ένα δύσκολο εγχείρημα, η ακρίβεια του οποίου είναι σχετική. Οι ζημίες δεν εξαντλούνται στις ευθείες [36] οικονομικές απώλειες,[37] μεταξύ των οποίων περιλαμβάνονται η άμεση οικονομική ζημία, το κόστος άμεσης απάντησης και ανάκτησης δεδομένων και το κόστος από τη διακοπή των λειτουργιών ενός συστήματος πληροφοριών, αλλά εμπεριέχουν προσθέτως έμμεσα κόστη,[38] περιλαμβανομένης της αποκατάστασης της τρωθείσας φήμης για τις παθούσες επιχειρήσεις και του ψυχικού κόστους για τα μεμονωμένα θύματα (Grabosky 2016: 70). Η διακοπή των λειτουργιών μιας επιχείρησης για παράδειγμα συνεπάγεται απώλεια παραγωγικού χρόνου, απώλεια ευκαιριών και απώλεια εισοδήματος (Lewis 2018: 5). Πλέον αυτού, το κόστος για τη θεραπεία της ζημίας και την αποκατάσταση της κλονισμένης πίστης και η επένδυση στην ενίσχυση των συστημάτων ασφαλείας, δεν αποκλείεται να υπερβαίνουν τις πραγματικές ζημίες (Kertysova 2018). Η διάδοση ενός εμπορικού μυστικού στους ανταγωνιστές ακόμη μπορεί να αποβεί μοιραία για την πορεία μιας επιχείρησης.

Σε ευρύτερο επίπεδο, τα κοινωνικά κόστη είναι ορατά. Μια ιστοσελίδα που φιλοξενεί παιδική πορνογραφία ή τρομοκράτες προκαλεί πραγματικά κόστη στην κοινωνία (CSIS 2013). Περαιτέρω, η προκαλούμενη ανησυχία γύρω από το ηλεκτρονικό έγκλημα μπορεί να επηρεάσει αρνητικά τις οικονομικές συναλλαγές και να οδηγήσει σε λιγότερο ορθολογικές οικονομικά συμπεριφορές (Goldberg 2016), ενώ η ευθεία προσβολή του χρηματοπιστωτικού συστήματος μιας χώρας μπορεί να οδηγήσει έως την κατάρρευσή της σηματοδοτώντας κυβερνοπόλεμο.[39] Το 2007 διαδικτυακές επιθέσεις προερχόμενες από την Κίνα έπληξαν 1.500 υπολογιστές στο Πεντάγωνο. Το 2010 ο ιός Stuxnet διείσδυσε στο σύστημα παραγωγής πυρηνικής ενέργειας του Ιράν. Το 2011 τα γκρουπ 'Anonymous' και 'Lulzsec' εξαπέλυσαν επιθέσεις τύπου DDoS σε κυβερνητικούς και εταιρικούς στόχους για συνεχόμενο διάστημα πενήντα ημερών.[40]

[36] Οι άμεσες πλήττουν την ακεραιότητα, αυθεντικότητα και διαθεσιμότητα των πληροφοριών, θεωρούνται όμως, παρά το κόστος αναστρέψιμες έναντι των έμμεσων.
[37] Κατά τον Anderson (2012: 5) ορίζονται ως «το χρηματικό ισοδύναμο των απωλειών, ζημιών και άλλων δεινών που αισθάνεται το θύμα ως συνέπεια του ηλεκτρονικού εγκλήματος».
[38] Κατά τον Anderson (2012: 5-6) ορίζονται ως «το χρηματικό ισοδύναμο των απωλειών και του κόστους ευκαιρίας που προκαλούνται στην κοινωνία από την τέλεση ηλεκτρονικών εγκλημάτων» και αφορούν στην προσπάθεια, το χρόνο και άλλες οργανικές δαπάνες.
[39] Η Ρωσία, η Β. Κορέα και το Ιράν είναι τα πλέον ενεργά κράτη στην πειρατεία χρηματοπιστωτικών ιδρυμάτων.
[40] Στις ΗΠΑ λειτουργούν τα συστήματα 'SCADA' (Supervisory Control and Data Acquisition) που ελέγχουν το μεγαλύτερο μέρος της σημαντικής υποδομής, παρά ταύτα, ο τραπεζικός τομέας, οι

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ
ΝΟΜΟΘΕΤΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

2.1 Εισαγωγικές Παρατηρήσεις

Η κεντρική προβληματική της νομοθετικής αντιμετώπισης του «χωρίς πατρίδα» εγκλήματος πηγάζει από το διασυνοριακό του χαρακτήρα. Ως εκ τούτου, η ανάγκη ομοιογενούς αντιμετώπισης ενός φαινομένου με διεθνείς διαστάσεις είναι επιτακτική. Αυτό προϋποθέτει εναρμόνιση των εθνικών ποινικών νομοθεσιών των κρατών σε επίπεδο Ουσιαστικού και Δικονομικού Ποινικού Δικαίου προκειμένου να περιληφθούν οι νέες προεκτάσεις τηρουμένης της αρχής nullum crimen nulla poena sine lege.[41] Μερίδα της θεωρίας έχει υποστηρίξει ότι η αποτελεσματική νομοθέτηση του ηλεκτρονικού εγκλήματος μπορεί να επιτευχθεί με προσαρμογή του ισχύοντος «παραδοσιακού» Δικαίου, ενώ σύμφωνα με άλλες προσεγγίσεις, πηγάζουσες από τις θεωρίες περί απόλυτης ελευθερίας και αυτορρύθμισης του Διαδικτύου (Μαργαρίτης 2009), έχει υποστηριχθεί ως περισσότερο αποτελεσματική η δημιουργία ενός ξεχωριστού οικοδομήματος Ποινικού Δικαίου του Διαδικτύου. Πρόσθετες δυσκολίες δημιουργεί η απουσία modus operandi. Οι δράστες δεν επαναλαμβάνουν τον τρόπο δράσης τους επιδιδόμενοι στην εεύρεση νέων μεθόδων δράσης, με αποτέλεσμα οι αρχές να βρίσκονται σχεδόν πάντα ένα βήμα πίσω, γεγονός που γεννά επιπλέον νομοθετικές και τεχνολογικές προκλήσεις. Οι πρώτες προσπάθειες νομοθετικής αντιμετώπισης του ηλεκτρονικού εγκλήματος εντοπίζονται στις ΗΠΑ, ενώ σε διεθνές επίπεδο η εναρμόνιση των ποινικών νομοθεσιών επιχειρήθηκε με τη Σύμβαση της Βουδαπέστης που ενσωματώθηκε στην ελληνική έννομη τάξη με το Ν. 4411/2016. Παρά ταύτα, πολλά κράτη εξακολουθούν να μην περιλαμβάνουν στη νομοθεσία τους σχετικές διατάξεις, ενώ σε ορισμένες περιπτώσεις οι υπάρχουσες νομοθετικές προβλέψεις έχουν επικριθεί ως ευρείες και προσκρούουσες σε ατομικά δικαιώματα. Από την άλλη πλευρά, η ενσωμάτωση διεθνών κειμένων δε συνεπάγεται απαραίτητα την από τα συμβληθέντα κράτη αποτύπωσή τους στο εγχώριο σύστημα με όμοιο τρόπο. Όπως καταδείχθηκε δε, η ευχερής αντιμετώπιση

επικοινωνίες και οι λοιπές αναγκαίες υποδομές εξακολουθούν να αποτελούν ευάλωτο στόχο (Kesan & Hayes 2012: 447-448, 458).

[41] Όπως εξειδικεύεται σε τέσσερις επιμέρους αρχές συνιστάμενες α) στην απαγόρευση θεμελίωσης ή επιβάρυνσης του αξιοποίνου βάσει εθίμου, β) στην απαγόρευση αναλογίας προς θεμελίωση ή επιβάρυνση του αξιοποίνου, γ) στην απαγόρευση της αναδρομικότητας και δ) στην απαγόρευση της θέσπισης αόριστων ποινικών διατάξεων (Μυλωνόπουλος 2007: 61).

προϋποθέτει στις περισσότερες περιπτώσεις συνεργασία, η οποία στην πράξη συχνά χωλαίνει. Σε αυτό το κεφάλαιο επιχειρείται η καταγραφή σημαντικών νομοθετικών κειμένων όπως ισχύουν σε ομοσπονδιακό επίπεδο στις ΗΠΑ όπου εμφανίστηκαν οι πρώτες μορφές ηλεκτρονικού εγκλήματος, η καταγραφή των διατάξεων της Σύμβασης της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο και σημαντικών Ευρωπαϊκών Οδηγιών που αφορούν στις πλέον ζημιογόνες μορφές ηλεκτρονικού εγκλήματος και τέλος, η καταγραφή της ελληνικής νομοθεσίας μέσα από τον ισχύοντα Ποινικό Κώδικα.

2.2.1 Αμερική

Εκκινώντας από μια σύντομη αναδρομή στην ιστορία του Διαδικτύου εντοπίζουμε τα πρώτα ψήγματα της ψηφιακής εποχής στις ΗΠΑ όταν το 1958 δημιουργήθηκε η στρατιωτική υπηρεσία ARPA (Advanced Research Project Agency) με αντικείμενο την ενασχόληση με την επιστήμη των υπολογιστών και σκοπό την παροχή τεχνολογικών οφελών στις ΗΠΑ έναντι του υπόλοιπου κόσμου. Το 1966 ζητήθηκε από διάφορα ερευνητικά ιδρύματα να κατασκευάσουν ένα δίκτυο υπολογιστών, γνωστό ως Arpanet[42] ή αλλιώς πρόγονος του σημερινού Internet. Αργότερα και συγκεκριμένα στις 12 Νοεμβρίου 1990 το CERN συστήνει τον Παγκόσμιο Ιστό (World Wide Web) και ο χώρος του Διαδικτύου καθίσταται πλέον και επίσημα ένας χώρος προσβάσιμος στο ευρύ κοινό. Ακολούθως, οι πρώτες αρνητικές πτυχές του διαδικτυακού χώρου παρατηρούνται λίγο αργότερα στις ΗΠΑ, όπου εμφανίζεται ένας νέος τύπος εγκληματικής δραστηριότητας επωφελούμενης από τα πλεονεκτήματα του Διαδικτύου, τελούμενης σε ορισμένες περιπτώσεις από μεμονωμένα άτομα και σε ορισμένες άλλες περιπτώσεις από οργανωμένες ομάδες, όπως οι '414s', 'Legion of Doom', 'Chaos Computer Club' (Koops & Brenner 2006: 313). Στο πλαίσιο αυτό, οι ΗΠΑ κλήθηκαν τόσο σε ομοσπονδιακό επίπεδο όσο και σε επίπεδο πολιτειών να προσαρμόσουν την υπάρχουσα νομοθεσία στη νέα τεχνολογική απειλή και πολύ σύντομα να την εντάξουν σε ένα ξεχωριστό πλαίσιο ειδικά προσαρμοσμένο στις νέες απαιτήσεις.[43]

[42] Ξεκίνησε το 1966 με 4 υπολογιστές και έως το 1977 είχε επεκταθεί σε 177.

[43] Ειδική μνεία όσον αφορά στη δράση υπέρ της καταπολέμησης των ηλεκτρονικών απειλών αξίζει στην Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ (National Security Agency-NSA), με καθήκον να κατευθύνει, να συντονίζει και να καταρτίζει ειδικό σχέδιο δράσης για την προστασία των κυβερνητικών πληροφοριακών συστημάτων. η ίδρυση της οποίας ανάγεται ήδη στο έτος 1952.

2.2.2 Computer Fraud and Abuse Act of 1986 (CFAA)

Προ του έτους 1984 σε περιπτώσεις ηλεκτρονικών επιθέσεων, όπως το hacking ή η διασπορά κακόβουλου λογισμικού εφαρμοζόταν η νομοθεσία για την απάτη ('wire and mail fraud statutes'), πλην όμως, η όξυνση των διαδικτυακών επιθέσεων τη δεκαετία του 1980, κατέστησε εμφανή την αδυναμία του τότε ισχύοντος νομοθετικού πλαισίου να αντιμετωπίσει τις εγκληματικές δραστηριότητες που ανέδειξαν οι νέες τεχνολογίες. Ενόψει αυτής της παραδοχής, το 1984 το Κογκρέσο προχώρησε στην πρώτη ολοκληρωμένη αναθεώρηση του Αμερικάνικου Ποινικού Κώδικα ('Comprehensive Crime Control Act of 1984'), στον οποίο περιελήφθησαν διατάξεις για την ηλεκτρονική απάτη και την απάτη με πιστωτικές κάρτες, και το 1986 τέθηκε σε ισχύ το πρώτο ομοσπονδιακό νομοθέτημα για την ποινικοποίηση της μη εξουσιοδοτημένης πρόσβασης και χρήσης υπολογιστών και δικτύων ('Computer Fraud and Abuse Act of 1986') που παρέχει τα μέσα για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας (confidentiality, integrity and availability-CIA) των συστημάτων και των δικτύων. Στο περιεχόμενο της CFAA εμπίπτει η προστασία έναντι της «χωρίς εξουσιοδότηση» ή «καθ' υπέρβαση εξουσιοδότησης»,[44] πρόσβασης σε «προστατευόμενο υπολογιστή» (protected computer),[45] δύο έννοιες που έχουν εγείρει σημαντικά προβλήματα ερμηνείας για το εύρος του περιεχομένου τους. Σε όλες τις περιπτώσεις η ομοσπονδιακή προσέγγιση περιορίστηκε στις περιπτώσεις που δικαιολογούν επιτακτικό ομοσπονδιακό ενδιαφέρον, όπως για παράδειγμα σε ζητήματα εθνικής ασφάλειας, διακρατικού βεληνεκούς ή επηρεασμού του εμπορίου μεταξύ κρατών.[46] Ακολούθησαν εξαντλητικές τροποποιήσεις το 1990, το 1994, το 1996, το 2001 ('USA Patriot Act') και το 2008 ('Identity Theft Enforcement and Restitution Act').

[44] Από τις πιο διάσημες περιπτώσεις οριοθέτησης των όρων αποτελεί αυτή του Morris το 1989, γιου ενός υπαλλήλου της NSA που ενόσω φοιτούσε στο Πανεπιστήμιο εξαπέλυσε το 'Morris worm'.
[45] 18 U.S.C. § 1030(e)(2)
[46] Στην αρχική του διάσταση ο όρος σήμαινε έναν υπολογιστή συνδεδεμένο στο internet που χρησιμοποιείται ή επηρεάζει το διακρατικό ή ξένο εμπόριο ή τις επικοινωνίες. Μετά τη θέση σε ισχύ του USA Patriot Act τροποποιήθηκε ο ορισμός και πρακτικά περιλαμβάνει κάθε υπολογιστή με σύνδεση στο internet.

Ιδιαίτερης μνείας δε, χρήζει η θέση σε ισχύ της USA Patriot Act[47] που επακολούθησε των τρομοκρατικών επιθέσεων της 11ης Σεπτεμβρίου 2001 που στάθηκαν η αιτία να αλλάξει άρδην το νομοθετικό πλαίσιο των ΗΠΑ. Στο κείμενο του Νόμου περιλαμβάνονται σημαντικές αλλαγές Ουσιαστικού και Δικονομικού Δικαίου. Διευρύνονται οι περιστάσεις υπό τις οποίες οι πάροχοι υπηρεσιών απαιτείται να ειδοποιούν τις αρμόδιες αρχές για ύποπτες ενέργειες όταν δικαιολογημένα πιστεύεται ότι συντρέχει επείγουσα περίπτωση συνιστάμενη σε άμεσο κίνδυνο για τη ζωή ή βαριά σωματική βλάβη,[48] καθώς επίσης, ενισχύονται σημαντικά τα μέτρα επιτήρησης.[49] Επιπλέον, προστίθενται πράξεις κακουργηματικού χαρακτήρα και αναγνωρίζεται η ανάγκη της ενίσχυσης των εργαλείων εξιχνίασης του ηλεκτρονικού εγκλήματος[50] και των συμμετεχουσών αρχών με προτεραιότητα στο FBI (Podgor 2002). Στα πιο καίρια σημεία του Νόμου περιλαμβάνεται ο ορισμός των πράξεων τρομοκρατίας στο πλαίσιο της προσπάθειας ενσωμάτωσης πράξεων κατασκοπίας και κυβερνοτρομοκρατίας (18 USC § 2332 (b)) και επεκτείνεται η αρμοδιότητα της Κυβέρνησης των ΗΠΑ σε εξωεδαφική εγκληματική δραστηριότητα μέσα από τον επαναπροσδιορισμό του όρου 'protected computer', στον οποίο περιλαμβάνεται οποιοσδήποτε υπολογιστής με πρόσβαση στο Internet, ακόμη κι αν ο δράστης δεν προχωρήσει σε περιήγηση (*United States v. Trotter* /8th Circ. 2007).[51] Ακόμη, οι όροι «ζημία» (damage)[52] και «απώλεια» (loss)[53] επανερμηνεύονται ως δομικά στοιχεία της απόφασης και της επιμέτρησης της ποινής και το πλαίσιο ποινής αυξάνεται.[54] Ειδικώς, ως προς το περιεχόμενο της ζημίας, πριν τις τροποποιήσεις του 2001, σε αυτό περιλαμβανόταν ενδεικτικά το κόστος αντιμετώπισης μιας προσβολής, οι δαπάνες αποτίμησης της ζημίας και επιδιόρθωσης της βλάβης σε προγράμματα, συστήματα, δεδομένα, πληροφορίες και λοιπές ακολουθούσες απώλειες, εστιαζόμενες

[47] 'Uniting and Strengthening America by Providing Appropriate tools Required to Intercept and Obstruct Terrorism Act of 2001'. Παρά ταύτα, δεν περιέχονται μόνο ρυθμίσεις που βρίσκονται σε άμεση συνάρτηση με τον τίτλο.

[48] 18 USC §2702, (C) 'if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay'

[49] Το Κεφάλαιο ΙΙΙ με τίτλο 'International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001', κατατείνει στη διευκόλυνση της αποτροπής και εξιχνίασης του ξεπλύματος χρήματος σε διεθνές επίπεδο και της χρηματοδότησης της τρομοκρατίας.

[50] Section 816, 'Development and Support of Cybersecurity Forensic Capabilities', Section 814, 'Deterrence and Prevention of Cyberterrorism'.

[51] 'used in a manner that affects interstate or foreign commerce or communication of the United States'

[52] 'any impairment to the integrity or ability of data, a program, a system or information'

[53] 'any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any revenue lost, cost incurred or other consequential damages concurred because of interruption of service'

[54] Ένας δράστης που με πρόθεση προκαλεί ζημία απειλείται με ποινή έως 10 έτη, ενώ αν επαναλάβει την προσβολή εκούσια ή ακούσια απειλείται με ποινή έως 20 έτη.

στην υλική-οικονομική βλάβη,[55] ενώ μετά τις τροποποιήσεις του 2001 προστέθηκαν συγκεκριμένα παραδείγματα μη οικονομικής ζημίας.[56] Στην ισχύουσα μορφή της και έπειτα από διαδοχικές τροποποιήσεις η CFAA ποινικοποιεί επτά τύπους ηλεκτρονικού εγκλήματος.[57]

2.2.3 Οι επιμέρους προσβολές και το επαπειλούμενο πλαίσιο ποινής

Ουσιώδες στοιχείο της CFAA αποτελεί η ποινικοποίηση της «χωρίς εξουσιοδότηση» ή «καθ' υπέρβαση εξουσιοδότησης»[58] πρόσβασης σε προστατευόμενο υπολογιστή ('protected computer'), δύο έννοιες που, όπως προελέχθη, έχουν εγείρει προβληματισμούς για το περιεχόμενο της CFAA με τους επικριτές να χαρακτηρίζουν το εριεχόμενο ευρύ και ξεπερασμένο (*United States v. John, United States v. Rodriguez., Int l Airport Ctrs. v. Citrin, EF Cultural Travel BV v. Explorica, Amphenol Corp. v. Paul, WEC Carolina Energy Solutions v. Miller, United States v. Nosal*),[59]. Ειδικότερα, στη διάταξη 18 USC § 1030 (a) (1) τιμωρείται, το πρώτον, όποιος αποκτά πρόσβαση σε απόρρητες πληροφορίες σχετιζόμενες με την εθνική άμυνα και τις διεθνείς σχέσεις και η ποινή συνίσταται σε χρηματικό πρόστιμο $250.000 ή φυλάκιση έως 10 έτη, καθώς επίσης, επανάληψη της παράβασης τιμωρείται με φυλάκιση έως 20 έτη. Έννομο αγαθό της διάταξης 18 USC § 1030 (a) (2) είναι η προστασία της εμπιστευτικότητας έναντι αθέμιτων παραβάσεων προστατευόμενων υπολογιστών, ανεξάρτητα από το ύψος της

[55] 818 U.S.C. § 1030(e)(11)

[56] 'the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; [access that causes] physical injury to any person; a threat to public health or safety; or damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.918 U.S.C. §§ 1030(a)(5)(B)(ii)-(v).

[57]18 USC § 1030 (a)(1): Obtaining National Security Information, 18 USC § 1030 (a)(2): compromising the confidentiality of a computer, 18 USC § 1030 (a)(3): trespassing in a government computer, 18 USC § 1030 (a)(4): accessing a computer to defraud and obtain something of value, 18 USC § 1030 (a)(5): damaging a computer, 18 USC § 1030 (a)(6): trafficking in passwords, 18 USC § 1030 (a)(7): threatening to damage a computer.

[58] Σε μία από τις πιο διάσημες περιπτώσεις που έχει ήδη παρατεθεί, αυτή του 'Morris worm', ο Morris που ενόσω ακόμα φοιτούσε στο Πανεπιστήμιο εξαπέλυσε το 'Morris worm', στη δίκη του ισχυρίστηκε ότι εφόσον είχε την άδεια να αποστέλλει μηνύματα ηλεκτρονικού ταχυδρομείου σε άλλους υπολογιστές έπρεπε να θεωρηθεί ότι έχει εξουσιοδότηση να εισέρχεται κατ' επέκταση σε αυτούς τους υπολογιστές. Ο ισχυρισμός του απορρίφθηκε.

[59] Μολονότι ο όρος «χωρίς εξουσιοδότηση» αναφέρεται σε hackers εξωτερικούς προς το παραβιαζόμενο περιβάλλον (outsiders) δεν περιλαμβάνεται σχετικός ορισμός, ενώ ο όρος «καθ' υπέρβαση εξουσιοδότησης» έχει χαρακτηριστεί υπερβολικά ευρύς. Μία εκ των προσπαθειών στην κατεύθυνση της εξειδίκευσης των όρων, της αποφυγής του διπλού αξιοποίνου και της μείωσης της ποινής για τους παραβάτες πρώτης φοράς ήταν ο 'Aaron's Law' που πήρε το όνομά του από τον Aaron Swartz, ο οποίος αυτοκτόνησε το 2013 υπό την πίεση των κατηγοριών της CFAA. Ο νόμος εισήχθη το 2015 αλλά τελικώς δεν τέθηκε σε ισχύ.

ζημίας, ενώ δεν αποκλείεται η καταδίκη ακόμη και σε περιπτώσεις online θέασης υπό την έννοια της μη «απόκτησης» της πληροφορίας (*United States. v. Tanimowo*). Ανάλογα δε με την σοβαρότητα της προσβολής, η παραβίαση της διάταξης 18 USC § 1030 (a) (2), τιμωρείται άλλοτε ως πλημμέλημα για πληροφορίες κοστολογούμενες κάτω των 5.000, πλέον χρηματικού προστίμου 100.000 και φυλάκιση έως 1 έτους (*United States. v. Carron*). Κακουργηματικού χαρακτήρα καθίστανται οι προσβολές που αφορούν σε σκοπό άντλησης εμπορικού πλεονεκτήματος ή άντλησης εικονικού οφέλους και διάπραξης ποινικά κολάσιμων πράξεων,[60] ενώ για παραβάτες που συλλαμβάνονται εκ νέου προβλέπεται 10ετής φυλάκιση και χρηματική ποινή $250.000. Η περίπτωση της διάταξης 18 USC § 1030 (a) (3) κατατείνει στην προστασία της ακεραιότητας των κυβερνητικών υπολογιστών, η οποία πλήττεται ανεξάρτητα από την πρόσβαση σε προσωπικές ή απόρρητες πληροφορίες. Πρώτη προσβολή τιμωρείται με φυλάκιση 1 έτους και χρηματικό πρόστιμο $100.000 και δεύτερη με 10ετή φυλάκιση και χρηματικό πρόστιμο $250.000. Η διάταξη της 18 USC § 1030 (a) (3) ποινικοποιεί τις πράξεις εξαπάτησης με σκοπό την αποκόμιση παράνομου οφέλους με την εξαίρεση ('computer use' exception) των περιπτώσεων που η εξαπάτηση αφορά σε χρήση υπολογιστή και η χρήση αυτή δεν υπερβαίνει τις $5.000 κατ' έτος.[61] Η πιο ευρέως χρησιμοποιούμενη πρόβλεψη είναι της διάταξης 18 USC § 1030(a) (5) που τιμωρεί όποιον εισβάλλοντας χωρίς εξουσιοδότηση σε προστατευόμενο υπολογιστή προκαλεί ζημία, ιδίως με την εν γνώσει του μετάδοση προγραμμάτων, πληροφοριών, κωδίκων ή εντολών (*Airlina Coach Service and Sky Limousine Company v. Alan Giang Lee*). Σε περίπτωση δόλου η πράξη ανάγεται σε κακούργημα, ενώ ηπιότερη είναι η μεταχείριση σε περίπτωση αμέλειας, οπότε το αδίκημα φέρει πλημμεληματικό χαρακτήρα. Πρόσθετα, στη διάταξη 18 USC § 1030(a) (6) ποινικοποιείται η διακίνηση κωδικών ή πληροφοριών που διευκολύνουν τη μη εξουσιοδοτημένη πρόσβαση με πρόθεση εξαπάτησης. Τέλος, η διάταξη18 USC § 1030(a) (6) ποινικοποιεί κάθε απειλή απέναντι σε προστατευμένο υπολογιστή με σκοπό τον προσπορισμό παράνομου περιουσιακού οφέλους. Η διάταξη καλύπτει τις απειλές σε σχέση με την απόκτηση ή αποκάλυψη εμπιστευτικών πληροφοριών χωρίς ή καθ' υπέρβαση εξουσιοδότησης (ACLR 2017: 1035-1037).

[60] Όροι που υιοθετούνται από το Δίκαιο πνευματικής ιδιοκτησίας 17 USC § 506 (a)

[61] Πρόκειται για εξαίρεση που εισήχθη για πρώτη φορά το 1986 με σκοπό την τιμωρία μόνο των σοβαρότερων μορφών και την αποφυγή της θεώρησης ότι συνέτρεχε σωρηδόν δόλος εξαπάτησης.

2.2.4 Άλλα νομοθετήματα

Παράλληλα με την προστασία που παρέχει η CFAA απέναντι στις τυποποιούμενες μορφές ηλεκτρονικού εγκλήματος, πεδίο εφαρμογής βρίσκουν και ορισμένα άλλα ομοσπονδιακά νομοθετήματα. Υπό τις προβλέψεις της 'Wiretap Act'[62] (18 U.S.C. §2510 επ.) που καθιστά παράνομη τη με πρόθεση διακοπή επικοινωνιών που διεξάγονται μέσω καλωδίου, ακουστικών ή ηλεκτρονικών μέσων και προβλέπει επαπειλούμενο πλαίσιο ποινής φυλάκισης έως 5 έτη ή/και χρηματική ποινή έως $250.000, μπορούν να τιμωρηθούν οι δράστες εκείνοι που εισβάλλουν σε συστήματα και παρακολουθούν άλλους υπολογιστές σε πραγματικό χρόνο ('real time').

Στα σημαντικότερα ομοσπονδιακά νομοθετήματα των ΗΠΑ ανήκει επίσης η 'Electronic Communications Privacy Act' (ECPA) που τιμωρεί όποιον με πρόθεση εισέρχεται χωρίς εξουσιοδότηση ή καθ' υπέρβαση εξουσιοδότησης σε ένα σύστημα, στο οποίο διεξάγεται μια ηλεκτρονική επικοινωνία και τροποποιεί ή εμποδίζει άλλους από την είσοδό τους σε αυτό. Συνεπώς, σε περιπτώσεις κατά τις οποίες hackers εισβάλλουν για παράδειγμα στο ηλεκτρονικό ταχυδρομείο χρήστη αποκτώντας ακολούθως πρόσβαση στις πληροφορίες του, οι διατάξεις της ECPA εφαρμόζονται αναλογικά. Παράλληλα, ρυθμίζονται οι προϋποθέσεις υπό τις οποίες η Κυβέρνηση μπορεί να αποκτά πρόσβαση σε αποθηκευμένες πληροφορίες μέσω των παρόχων υπηρεσιών Διαδικτύου – η ευθύνη των παρόχων προβλέπεται, περαιτέρω, στα άρθρα 18 U.S.C. § 2701-2712- και περιγράφονται οι διαδικασίες για την απόκτηση των πληροφοριών (Koops & Brenner 2006: 315-316). Στο άρθρο 18 USC § 1343 ενσωματώνεται η 'Federal wire fraud statute' που εφαρμόστηκε στην υπόθεση *United States v. Sheier*. Δυνάμει της 'Federal wire fraud statute' οι δράστες καταδικάστηκαν υπό την κατηγορία της παράνομης πρόσβασης στο σύστημα ηλεκτρονικών κρατήσεων της 'American Airlines' (Koops & Brenner 2006: 315).

Στο άρθρο 18 USC § 1028 καλύπτεται γενικά η κλοπή ταυτότητας, καθώς επίσης, σημαντική κρίνεται και η αναφορά του άρθρου 18 USC § 1029 που εισήχθη τη δεκαετία του 1980 προς αντιμετώπιση των ήδη εμφανών κρουσμάτων απατών με χρεωστικές και

[62] Τροποποιήθηκε από το Κογκρέσο το 1986 προκειμένου να περιλάβει διατάξεις για το ηλεκτρονικό έγκλημα.

πιστωτικές κάρτες και εφαρμόστηκε στην περίπτωση του Kevin Mitnick (*United States v. Mitnick*), ο οποίος, υπό την εφαρμογή της διάταξης 18 USC § 1029 (a) (3), καταδικάστηκε για μη εξουσιοδοτημένη πρόσβαση με σκοπό εξαπάτησης. Άλλη περίπτωση είναι αυτή του Brewer (*United States v. Brewer*) που καταδικάστηκε υπό την εφαρμογή της 18 USC § 1029 (a) (1) επειδή επικοινώνησε με εταιρεία τηλεφωνίας και μάντεψε τους έγκυρους κωδικούς που θα του εξασφάλιζαν υπηρεσίες εξυπηρέτησης μακράς διάρκειας. Η πράξη του κρίθηκε ως εξαπάτηση και το Δικαστήριο σημείωσε ότι η είσοδός του κατέστη εφικτή χάρη στους «πλαστούς» κωδικούς που χρησιμοποιήθηκαν υπό την έννοια ότι επρόκειτο για κατασκευασμένους κωδικούς που έτυχε να συμπίπτουν με τους κωδικούς της εταιρείας.

Τέλος, σε ό, τι αφορά στη διακίνηση υλικού παιδικής πορνογραφίας υπό την Πρώτη Τροποποίηση του Συντάγματος των ΗΠΑ παρέμενε αρρύθμιστη έναντι της ελευθερίας της έκφρασης στο Διαδίκτυο. Ομοσπονδιακά νομοθετήματα που επιχείρησαν να επεκτείνουν το προστατευτικό περιεχόμενο μέσω του περιορισμού των πληροφοριών που διακινούνται στο διαδίκτυο και της ελευθερίας της έκφρασης δια της απαγόρευσης της μετάδοσης άσεμνου και εμφανώς προσβλητικού περιεχομένου σε ανηλίκους (Communications Decency Act of 1996-CDA, Child Pornography Act of 1996-CPPA, Child Online Prevention Act of 1998-COPA) κρίθηκαν σε ορισμένα σημεία τους αντισυνταγματικά ως περιλαμβάνοντα ασαφείς και ευρείες διατυπώσεις (*United States v. Williams)*.[63] Τελικώς το 2003, προς άρση των ασαφειών των προηγούμενων νομοθετημάτων, τέθηκε σε ισχύ ο Νόμος 'PROTECT Act' ('Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003') για την αποτροπή της εκμετάλλευσης παιδιών και την ευχερή έρευνα και δίωξη των δραστών, δυνάμει του οποίου απαγορεύεται η διαφήμιση, προώθηση, παρουσίαση και διανομή πορνογραφικού υλικού που δημιουργεί την πεποίθηση ότι σε αυτό απεικονίζονται παιδιά (ACLR 2017: 1042) ακόμη και αν δεν πρόκειται πράγματι για παιδιά (π.χ. anime ή manga που αναπαριστούν παιδιά εμπίπτουν στο απαγορευτικό περιεχόμενο, Overbeck & Belmas 2012).

[63] Η Communications Decency Act of 1996 κατά το μέρος που είναι σε ισχύ η εις γνώσει μετάδοση άσεμνου λόγου ή εικόνων σε ανηλίκους τιμωρείται με πρόστιμο ή/και φυλάκιση έως 2 ετών. 47 USC § 223 (a)

2.3.1 Ευρώπη

Οι προκλήσεις που παρουσιάστηκαν με την εμφάνιση του ηλεκτρονικού εγκλήματος αποτέλεσαν τη βάση συζήτησης όχι μόνο για τα κράτη μεμονωμένα αλλά και για ευρωπαϊκούς οργανισμούς μεταξύ των οποίων το Συμβούλιο της Ευρώπης. Προηγουμένως, είχαν γίνει προσπάθειες από διεθνή φόρα και οργανισμούς, όπως η ομάδα των G8, για την υιοθέτηση αρχών και σχεδίου δράσης με σκοπό την καταπολέμηση εγκλημάτων υψηλής τεχνολογίας (Principles and Action Plan to Combat High-tech crime) και τα Ηνωμένα Έθνη στην κατεύθυνση της αποτροπής και του ελέγχου του ηλεκτρονικού εγκλήματος (Manual on the prevention and control of computer-related crime). Ήδη από τη δεκαετία του '70, το Συμβούλιο της Ευρώπης είχε τονίσει τη διεθνή φύση των «εγκλημάτων πληροφορικής», οπότε εκκίνησε μια συζήτηση υπό την προσέγγιση των οικονομικών εγκλημάτων. Μία από τις πρώτες απόπειρες κατηγοριοποίησης των διαδικτυακών απειλών που έπρεπε να νομοθετηθούν έλαβε χώρα υπό την αιγίδα του ΟΟΣΑ,[64] ο οποίος το 1986 προχώρησε στη δημοσίευση πέντε κατηγοριών ηλεκτρονικών απειλών (OECD 1986), ενώ λίγο νωρίτερα, το 1985, υπό τη διαπίστωση της απουσίας μιας συνεκτικής πολιτικής σε ενωσιακό επίπεδο, συστάθηκε μια επιτροπή εμπειρογνωμόνων, αρμόδια για ποινικά ζητήματα, στο πλαίσιο του Συμβουλίου της Ευρώπης (European Comittee on Crime Problems), με σκοπό τη διάσκεψη επί νομικών ζητημάτων που ανέκυψαν με την άνοδο του ηλεκτρονικού εγκλήματος, στοχεύουσα στην εναρμόνιση των εθνικών νομοθεσιών. Σχετική μελέτη δημοσιεύτηκε το Σεπτέμβριο του 1989 περιλαμβάνουσα μια μικρή λίστα απειλών που έχρηζαν επιτακτικής ανάγκης ποινικής νομοθέτησης (ECCP 1990) διαπιστωθείσας της μεταμόρφωσης του κόσμου σε μια διεθνή κοινωνία της πληροφορίας, όπου δεν υπάρχουν πλέον σύνορα.

Υπό τη σκέψη αυτή, έγινε αντιληπτός ο εντοπισμός υπερεθνικών στοιχείων σχεδόν σε κάθε έγκλημα και υποτέθηκε ότι ελάχιστα άτομα και φορείς επρόκειτο να μείνουν πλέον ανέπαφα από τις νέες και απειλητικές εγκληματικές δραστηριότητες (Sussmann). Η μελέτη δημοσιεύτηκε μαζί με την υπ' αριθμόν 89 Σύσταση του

[64] Ο ΟΟΣΑ αποτέλεσε τον πρώτο οργανισμό που έθεσε επί τάπητος τα προβλήματα εφαρμογής του παραδοσιακού ποινικού Δικαίου στο ηλεκτρονικό έγκλημα και εκκίνησε τις προσπάθειες εναρμόνισης του Ποινικού Δικαίου του Διαδικτύου στην Ευρώπη προβαίνοντας σε συστάσεις 'soft law'. Ακολούθησαν τα Ηνωμένα Έθνη στο Κογκρέσο του 1990 σχετικά με την πρόληψη του εγκλήματος και τη μεταχείριση των δραστών υπό τις νέες διεθνείς προκλήσεις.

Υπουργικού Συμβουλίου [Recommendation No. R (89)] για το ηλεκτρονικό έγκλημα (computer-related crime) περιέχουσα κατευθυντήριες σε ζητήματα ουσιαστικού Δικαίου[65]. Αντιμέτωπο, περαιτέρω, με τις ποινικές δικονομικές προκλήσεις, το 1995 το Υπουργικό Συμβούλιο υιοθέτησε την υπ' αριθμόν 95 (13) Σύσταση [Recommendation No. R (95) 13] που παρείχε τις κατευθυντήριες σε καίρια δικονομικά ζητήματα, όπως η έρευνα και κατάσχεση του αποδεικτικού υλικού, η αναγκαιότητα ταχείας δράσης, η προοπτική επιβολής υποχρέωσης στους παρόχους τηλεπικοινωνιών προς παροχή πληροφοριών σχετικά με την ταυτότητα των χρηστών και επιπλέον, ρυθμίσεις για ζητήματα αμοιβαίας βοήθειας και διεθνούς συνεργασίας. Παρά ταύτα, οι Συστάσεις αυτές δεν είχαν δεσμευτικό χαρακτήρα με αποτέλεσμα την κατάδειξη της ανάγκης ουσιαστικής εναρμόνισης της ποινικής νομοθεσίας για την αντιμετώπιση ενός φαινομένου διεθνούς εμβέλειας. Οι προσπάθειες του Συμβουλίου της Ευρώπης προς την κατεύθυνση αυτή κατέληξαν το 1997 στον σχεδιασμό μιας διεθνούς συνθήκης που φιλοδοξούσε να εναρμονίσει τις εθνικές νομοθεσίες, να προαγάγει αποτελεσματικές μεθόδους εξιχνίασης και να ενισχύσει τη διεθνή συνεργασία.

2.3.2 Η Σύμβαση της Βουδαπέστης

Στις 23 Νοεμβρίου του 2001, στο πλαίσιο της επιδίωξης κοινής αντεγκληματικής πολιτικής με στόχο την προστασία της κοινωνίας από το ηλεκτρονικό έγκλημα, μέσα από την υιοθέτηση της κατάλληλης νομοθεσίας και την ενίσχυση της ταχείας και καλά συντονισμένης διεθνούς συνεργασίας, υπεγράφη από 26 κράτη μέλη και 4 χώρες παρατηρητές[66], η υπ' αριθμόν 185 Σύμβαση για το έγκλημα στον Κυβερνοχώρο ή αλλιώς Σύμβαση της Βουδαπέστης, η οποία συμπληρώθηκε από το Πρόσθετο Πρωτόκολλο για την ποινικοποίηση πράξεων ρατσισμού και ξενοφοβίας που διαπράττονται μέσω Διαδικτύου και υπογράφηκε στις 28 Ιανουαρίου 2003. Έναρξη ισχύος της Σύμβασης ήταν η 1η Απριλίου 2004. Έως σήμερα έχει υπογραφεί από όλα τα κράτη μέλη του Συμβουλίου της Ευρώπης πλην της Ρωσικής Ομοσπονδίας, ενώ δεν έχει επικυρωθεί από την Ιρλανδία και τη Σουηδία. Πλέον των κρατών μελών, τη Σύμβαση έχουν επικυρώσει οι ΗΠΑ, ο Καναδάς και η Ιαπωνία που συμμετείχαν στη διαδικασία σχεδιασμού που

[65] Διαθέσιμη εδώ: https://rm.coe.int/1680500b15
[66] Καναδάς, Ιαπωνία, Ν. Αφρική, ΗΠΑ. Μεταξύ των υπογραφόντων και η Ελλάδα, η οποία ενσωμάτωσε την Σύμβαση με τον Ν. 4411/2016.

κατέληξε στην υπογραφή της Σύμβασης το 2001, η Αργεντινή, η Αυστραλία, το Κάβο Βέρντε, η Χιλή, η Κόστα Ρίκα, η Δομινικανή Δημοκρατία, η Γκάνα, το Ισραήλ, ο Μαυρίκιος, το Μαρόκο, Ο Παναμάς, η Παραγουάη, το Περού, οι Φιλιππίνες[67], η Σενεγάλη, η Σρι Λάνκα και η Τόνγκα, ενώ η Ν. Αφρική, μολονότι έχει υπογράψει τη Σύμβαση από το 2001, δεν την έχει επικυρώσει έως σήμερα.[68]

Η Σύμβαση αποτελεί τη συλλογική απάντηση των υπογραφόντων κρατών στο ηλεκτρονικό έγκλημα έπειτα από μια μακρά επεξεργασία τεσσάρων ετών, με γνώμονα τις κατευθυντήριες των προηγούμενων συστάσεων, στο πλαίσιο της προσπάθειας εναρμόνισης των νομοθετικών ορισμών και των ποινικών δικονομικών προβλημάτων που ανέδειξε η κοινωνία της πληροφορίας, της καθιέρωσης κοινών κανόνων για την έρευνα και συλλογή του αποδεικτικού υλικού στο τεχνολογικό περιβάλλον και της δημιουργίας ενός πλαισίου συνύπαρξης παραδοσιακών και νέων μορφών διεθνούς συνεργασίας με στόχο την ταχεία έρευνα και δίωξη (Csonka 2006: 483).

Η Σύμβαση περιλαμβάνει διατάξεις Ουσιαστικού (κεφάλαιο Ι) και Δικονομικού (κεφάλαιο ΙΙ) Ποινικού Δικαίου που υποχρεώνουν τα κράτη να λάβουν μέτρα για την ενσωμάτωσή τους στο εσωτερικό τους Δίκαιο και διατάξεις που αφορούν τη διεθνή συνεργασία (κεφάλαιο ΙΙΙ). Οι ουσιαστικού Δικαίου διατάξεις αναλύονται στο πρώτο κεφάλαιο[69] και αφορούν στην κατηγοριοποίηση των προσβολών σε α) αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας πληροφοριακών δεδομένων και συστημάτων (άρθρα 2-6) που, σύμφωνα με τα στατιστικά δεδομένα της United Nations Office on Drugs and Crime, αποτελούν τον πυρήνα του ηλεκτρονικού εγκλήματος,[70] β) αδικήματα που σχετίζονται με υπολογιστή (άρθρα 7-8)[71] και γ) αδικήματα που σχετίζονται με το περιεχόμενο (άρθρα 9-10).[72] Στόχο αποτελεί η

[67] Οι Φιλιππίνες επικύρωσαν τη Σύμβαση στις 28.3.2018 ενώ μέχρι πρότινος αποτελούσαν μία εκ των αναπτυσσόμενων χωρών με ασθενή νομοθεσία στο ηλεκτρονικό έγκλημα και προσφιλή τοποθεσία για τους επίδοξους δράστες.

[68] Διαθέσιμη εδώ: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

[69] Στον ορισμό των προβλεπόμενων αδικημάτων επιδιώκεται η χρήση τεχνολογικά ουδέτερης γλώσσας ώστε οι προβλεπόμενες ρυθμίσεις να δύνανται να εφαρμοστούν τόσο κατά το παρόν στάδιο όσο και ενόψει μελλοντικών εξελίξεων. Σκέψη 36, Αιτιολογική Έκθεση της Σύμβασης της Βουδαπέστης.

[70] Πρόκειται για τα γνήσια ηλεκτρονικά εγκλήματα που περιλαμβάνουν την παράνομη πρόσβαση, παράνομη παρακολούθηση, παρεμβολή δεδομένων και παρεμβολές συστημάτων και κακή χρήση συσκευών.

[71] Απάτη και πλαστογραφία.

[72] Παιδική πορνογραφία και παραβιάσεις των δικαιωμάτων πνευματικής ιδιοκτησίας και των συγγενικών δικαιωμάτων.

εναρμόνιση των νομοθετικών ορισμών προς την καταπολέμηση των περιορισμών του διπλού αξιοποίνου (dual criminality). Εν συνεχεία, παρουσιάζονται τα σχετικά με την παρεπόμενη ευθύνη και τις κυρώσεις. Ειδικότερα, υπό τον Τίτλο 1 καλύπτεται ο πυρήνας των ηλεκτρονικών εγκλημάτων που πλήττουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων υπολογιστών και των συστημάτων υπολογιστών που αντιπροσωπεύουν τις βασικές απειλές, στις οποίες εκτίθενται τα συστήματα ηλεκτρονικής επεξεργασίας δεδομένων και επικοινωνιών. Σε αυτά περιλαμβάνεται η μη εξουσιοδοτημένη πρόσβαση, ιδίως το hacking και το cracking και λοιπές παραβιάσεις που αναλύονται στην παράνομη πρόσβαση, υποκλοπή, παρεμβολές σε δεδομένα και συστήματα επεξεργασίας (στην τελευταία περίπτωση ουσιώδες είναι το στοιχείο της σοβαρής παρακώλυσης της λειτουργίας του συστήματος π.χ. DDoS attacks) και η κακή χρήση συσκευών.[73] Τα αδικήματα αυτής της κατηγορίας λαμβάνονται, περαιτέρω, ως σημεία αναφοράς δυνάμενα να οδηγήσουν σε περαιτέρω προσβολές, όπως η παράνομη πρόσβαση σε εμπιστευτικές πληροφορίες, διάπραξη απάτης και πλαστογραφίας. Πολλές νομοθεσίες περιλαμβάνουν ρυθμίσεις σχετικά με τις προσβολές hacking αλλά οι επιμέρους προϋποθέσεις ποινικής τιμωρίας ποικίλλουν, ώστε σε ορισμένες περιπτώσεις οι διατυπώσεις εμφανίζονται στενές, ενώ σε ορισμένες άλλες περιπτώσεις μπορεί να απαιτείται η πλήρωση πρόσθετων περιστάσεων, η θεμελίωση των οποίων απόκειται στα κράτη (Csonka 2006: 484).

Στους Τίτλους 2-4 περιλαμβάνονται άλλες μορφές ηλεκτρονικών εγκλημάτων, οι οποίες εμφανίζονται με μεγάλη συχνότητα και στις οποίες οι υπολογιστές χρησιμοποιούνται ως μέσο τέλεσης του εγκλήματος σε βάρος εννόμων αγαθών, ήδη προστατευόμενων με τα παραδοσιακά μέσα του Ποινικού Δικαίου (ηλεκτρονική απάτη και πλαστογραφία). Ειδικής μνείας χρήζει η ηλεκτρονική απάτη περιλαμβανομένων περιστατικών απάτης με πιστωτικές κάρτες, τα οποία πολλαπλασιάστηκαν.[74] Σκοπός της

[73] Η κακή χρήση συσκευών όπως προβλέπεται στο άρθρο 5 αναφέρεται σε μέσα όπως τα εργαλεία hacking που προορίζονται κατ' εξοχήν για διάπραξη εγκληματικών δραστηριοτήτων, απαιτούμενης για τη θεμελίωση του αδικήματος της συνδρομής σκοπού διάπραξης μίας από τις ως άνω αναφερόμενες εγκληματικές δραστηριότητες. Ratio της διάταξης αποτελεί η ποινικοποίηση της εγκληματικής πρόθεσης, γι' αυτό και τιμωρείται και η απλή κατοχή τέτοιων συσκευών, ενώ από το πεδίο της διάταξης αποκλείονται συσκευές που μπορούν να χρησιμοποιηθούν και για νόμιμους σκοπούς.

[74] Το αδίκημα περιλαμβάνει την «εκ προθέσεως» και «χωρίς δικαίωμα» διάπραξη, απαιτώντας δόλια ή άλλη ανέντιμη συμπεριφορά για την απόκτηση οικονομικού οφέλους για τον δρώντα ή για τρίτο, ενώ η γενική απαίτηση της πρόθεσης αναφέρεται στη χρήση υπολογιστή ή παρεμβολές που προκαλούν απώλεια ιδιοκτησίας, ώστε π.χ. εμπορικές πρακτικές στο πλαίσιο της αγοράς, που μπορεί να προκαλέσουν οικονομική ζημία σε ένα άτομο και να ωφελήσουν ένα άλλο, πλην όμως, που δεν εκτελούνται με δόλια ή

διάταξης για την απάτη είναι η ποινικοποίηση κάθε αδικαιολόγητης ενέργειας, όπως η τροποποίηση, διαγραφή ή καταστολή δεδομένων και η παρέμβαση στη λειτουργία ενός συστήματος υπολογιστή με πρόθεση προσπορισμού οικονομικού οφέλους. Η διάταξη για την πλαστογραφία στοχεύει στην κάλυψη των κενών των παραδοσιακών ρυθμίσεων σε αναφορά με τον χειρισμό των ηλεκτρονικά αποθηκευμένων δεδομένων. Ο Τίτλος 3 καλύπτει τα σχετιζόμενα με το περιεχόμενο εγκλήματα της παράνομης παραγωγής και διανομής υλικού παιδικής πορνογραφίας με τη χρήση συστημάτων πληροφορικής ως αδικήματα περιλαμβάνοντα από τα πιο επικίνδυνα modi operandi.[75] Στον Τίτλο 4 περιγράφονται τα αδικήματα που σχετίζονται με παραβιάσεις πνευματικών και συγγενικών δικαιωμάτων.

Δυσκολίες αποτελούν η διαπίστωση βλάβης και διακινδύνευσης που έχουν οδηγήσει πολλά κράτη στην αποχή από την ποινικοποίηση προπαρασκευαστικών ενεργειών με την εξαίρεση περιπτώσεων που αφορούν σε πολύ σοβαρά εγκλήματα (Brenner 2009). Στο άρθρο 6 ποινικοποιούνται η παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή άλλως διάθεση ή κατοχή συσκευών και συστημάτων επεξεργασίας υπολογιστών, περιλαμβανομένων των κωδικών πρόσβασης ή παρόμοιων δεδομένων με την πρόθεση της χρήσης για διάπραξη οιασδήποτε εκ των περιγραφόμενων προσβολών. Τυπικά παραδείγματα αποτελούν το phishing σε ιστοσελίδες (Deleon 2008) ή ακόμα το grooming (Viano 2017: 11).

Η ιδιαιτερότητα των περιλαμβανόμενων αδικημάτων έγκειται στη χωρίς δικαίωμα διάπραξή τους, ώστε η διαπίστωσή τους να μην καθιστά την πράξη per se αξιόποινη[76] τόσο στις περιπτώσεις που συντρέχουν οι προϋποθέσεις άρσης του αξιοποίνου, όπως η άμυνα ή η κατάσταση ανάγκης, όσο και σε ορισμένες πρόσθετες περιπτώσεις που οδηγούν σε αποκλεισμό της ποινικής ευθύνης.[77] Σε ό,τι αφορά στην

ανέντιμη πρόθεση, δεν προορίζονται να περιληφθούν στο συγκεκριμένο άρθρο. π.χ. η χρήση προγραμμάτων συλλογής πληροφοριών στο Διαδίκτυο (bots). Σκέψη 90

[75] Άρθρο 35, Αιτιολογική Έκθεση της Σύμβασης της Βουδαπέστης.

[76] Το νόημα της υπό κρίση επομένως πράξης αντλείται από το context, στο οποίο εντοπίζεται, ώστε να αποκλειστεί η ποινική ευθύνη σε νόμιμες και συνήθεις δραστηριότητες, ενώ η περαιτέρω εξειδίκευση της έννοιας απόκειται στα κράτη.

[77] Π.χ. στην περίπτωση της υποκλοπής δια τεχνικών μέσων του άρθρου 3, η πράξη θεωρείται δικαιολογημένη αν ο παρακολουθούμενος έχει το δικαίωμα να ενεργεί σύμφωνα με τις οδηγίες ή με την άδεια των συμμετεχόντων στη μετάδοση, συμπεριλαμβανομένων των εγκεκριμένων δραστηριοτήτων δοκιμών ή προστασίας που συμφωνούν οι συμμετέχοντες, ή εάν η επιτήρηση επιτρέπεται νόμιμα προς το συμφέρον της εθνικής ασφάλειας ή της ανίχνευσης αξιόποινων πράξεων. Η χρήση εμπορικών πρακτικών όπως τα cookies, δεν εμπίπτει στο προστατευτικό περιεχόμενο της υποκλοπής «χωρίς δικαίωμα».

υποκειμενική υπόσταση των περιεχόμενων αδικημάτων, αναγκαία είναι η διαπίστωση δόλου, η διαβάθμιση του οποίου απόκειται στις εθνικές έννομες τάξεις, ενώ σε ορισμένες περιπτώσεις τα κράτη μπορούν να θεσπίζουν πρόσθετα υποκειμενικά στοιχεία του αδίκου, όπως π.χ. η πρόθεση προσπορισμού οικονομικού οφέλους στο άρθρο 8 σχετικά με την απάτη.[78]

Επιπλέον, η Σύμβαση αντιμετωπίζει τα ζητήματα ευθύνης σε σχέση με την απόπειρα και την υποβοήθηση ή συνέργεια (άρθρο 11) και την εταιρική ευθύνη (άρθρο 12), καθώς επίσης, αναγνωρίζει την υποχρέωση των συμβαλλομένων κρατών να λαμβάνουν τα νομοθετικά και άλλα μέτρα που απαιτούνται προς τον σκοπό της εξασφάλισης ότι τα ποινικά αδικήματα που κατοχυρώνονται στα άρθρα 2-11 τιμωρούνται με αποτελεσματικές, αναλογικές και αποτρεπτικές (effective, proportional, dissuasive criminal sanctions) ποινικές κυρώσεις και μέτρα περιλαμβανομένων των χρηματικών κυρώσεων (άρθρο 13).[79]

Το δεύτερο κεφάλαιο της Σύμβασης, το οποίο εκτείνεται πέραν των προσβολών που προβλέπονται στο πρώτο κεφάλαιο, ρυθμίζει τα ζητήματα Δικονομικού Δικαίου που τα κράτη μέλη οφείλουν να ενσωματώσουν στην εθνική τους νομοθεσία.[80] Σε αυτά περιλαμβάνονται μέτρα για την κατεπείγουσα διατήρηση των αποθηκευμένων δεδομένων υπολογιστών (άρθρο 16),[81] την κατεπείγουσα διατήρηση και αποκάλυψη στοιχείων κίνησης (άρθρο 17), τη συλλογή, έρευνα και κατάσχεση δεδομένων υπολογιστών (άρθρα 18-19), τη συλλογή διακινούμενων δεδομένων σε πραγματικό χρόνο (άρθρο 20) και την άρση του απορρήτου των δεδομένων περιεχομένου (άρθρο

Αντιθέτως, μη δημόσιες επικοινωνίες υπαλλήλων εμπίπτουν στο προστατευτικό περιεχόμενο του άρθρου (ΕΔΔΑ, *Halford v. United Kingdom*) Σκέψεις 37, 54 και 58 ό.π.

[78] Σκέψη 39 ό.π.

[79] Καθίσταται σαφές ότι με βάση το άρ. 13 παρ. 1, τα κράτη-μέλη υποχρεώνονται να λάβουν τα απαιτούμενα κατά την κρίση τους μέτρα για την αντιμετώπιση των επιθέσεων κατά των συστημάτων υπολογιστών, ώστε να υπάρχουν κυρώσεις που να είναι «αποτελεσματικές, ανάλογες και αποτρεπτικές», τόσο για τα ΠΦ και για τα ΝΠ.

[80] Το περιεχόμενο των διατάξεων έχει εγείρει προβληματισμούς με τους επικριτές να κάνουν λόγο για «οργουελικό σύστημα» και υπερβολική επιτήρηση. Ο αντίλογος αφορά στις συγκεκριμένες και αναλογικές δυνατότητες που δεν εκτείνονται στη συστηματική επιτήρηση προσωπικών επικοινωνιών από τις Αρχές ή τους παρόχους υπηρεσιών Διαδικτύου, παρεκτός αν κρίνεται αναγκαίο για τους σκοπούς συγκεκριμένης έρευνας (Csonka 2006: 490).

[81] Σε ορισμένα κράτη απαιτείται η μη διατήρηση των δεδομένων, όπως τα προσωπικά δεδομένα, εφόσον δε συντρέχει ανάγκη διατήρησής τους για τους σκοπούς της πρόληψης, διερεύνησης ή δίωξης ποινικών αδικημάτων. Η έννοια της διατήρησης των δεδομένων αποτελεί νέα νομοθετική πρόβλεψη και εργαλείο για την καταπολέμηση του ηλεκτρονικού εγκλήματος μέσω της διατήρησης της ακεραιότητας των αποδεικτικών στοιχείων της αυτής μορφής. Σκέψεις 154, 155.

21),[82] καθώς επίσης, στο ακροτελεύτιο άρθρο του κεφαλαίου ρυθμίζονται ζητήματα δικαιοδοσίας (άρθρο 22).[83] Πρόκειται δε, για ρυθμίσεις-πυλώνες στην κατεύθυνση της ταχείας δράσης.

Τα άρθρα 16 και 17 εφαρμόζονται σε περιπτώσεις αποθηκευμένων δεδομένων που έχουν συλλεγεί και διατηρηθεί από φορείς όπως οι πάροχοι υπηρεσιών Διαδικτύου, χωρίς, ωστόσο, να καταλαμβάνουν περιπτώσεις συλλογής δεδομένων σε πραγματικό χρόνο. Σημειώνεται ότι παρά τις σχετικές συζητήσεις κατά τη σύνταξη της Σύμβασης δεν επιβλήθηκε στους παρόχους υπηρεσιών υποχρέωση συλλογής και διατήρησης δεδομένων κίνησης για καθορισμένο χρονικό διάστημα.[84] Αμφότερες οι διατάξεις στοχεύουν στη διατήρηση των δεδομένων. Η πρώτη εφαρμόζεται σε περιπτώσεις που τα δεδομένα τυγχάνουν ιδιαιτέρως ευάλωτα σε απώλεια ή τροποποίηση, χωρίς να δικαιολογείται, ωστόσο, πρόσβαση των αρχών στο σύνολο των δεδομένων (Csonka 2006: 492). Το άρθρο 17 ενισχύει τις προσπάθειες των αρχών στην ανίχνευση της πηγής των δεδομένων, εκεί όπου παρεμβάλλονται περισσότεροι πάροχοι υπηρεσιών.

Στο άρθρο 19 ρυθμίζονται τα ζητήματα έρευνας και κατάσχεσης του αποδεικτικού υλικού, όπου πολλά από τα παραδοσιακά χαρακτηριστικά παραμένουν, πλην όμως, η προβληματική έγκειται στην άυλη μορφή των δεδομένων. Σε πολλές νομοθεσίες τα ψηφιακά δεδομένα δε θεωρούνται πράγμα υπό την έννοια του αντικειμένου κατάσχεσης, με την εξαίρεση του μέσου στα οποία αυτά είναι αποθηκευμένα. Στόχος της πρόβλεψης είναι η καθιέρωση ισοδύναμης ισχύος σε σχέση

[82] Στην Ελληνική νομοθεσία στα άρθρα 3 και 4 του Ν. 2225/94 για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας προβλέπονται οι περιπτώσεις που δικαιολογούν την ενεργοποίηση της διαδικασίας άρσης απορρήτου. Στην προστασία του απορρήτου περιλαμβάνεται η διεύθυνση IP ως ο μοναδικός αριθμός που λαμβάνει κάθε συσκευή που συνδέεται στο Διαδίκτυο και που μπορεί να οδηγήσει στην εύρεση του δράστη διάπραξης διαδικτυακού εγκλήματος ως μία εκ των βασικότερων ενδείξεων για την ταυτότητα των υπόπτων. Κομβικής σημασίας στη διαδικασία εύρεσης των ηλεκτρονικών ιχνών των υπόπτων τέλεσης διαδικτυακών εγκλημάτων είναι οι γνωμοδοτήσεις ΑΠ 9 & 12/2009, 9/2011 και 4569/2012, δυνάμει των οποίων οι εισαγγελικές και προανακριτικές αρχές, δικαιούνται να ζητούν από τους παρόχους των υπηρεσιών επικοινωνίας, τα ηλεκτρονικά ίχνη μιας εγκληματικής πράξης και τα στοιχεία του προσώπου στο οποίο αντιστοιχεί το ηλεκτρονικό ίχνος και ο πάροχος υποχρεούται να τα παραδίδει, χωρίς να απαιτείται να προηγηθεί άδεια ή έλεγχος κάποιας Αρχής, ιδίως της Α.Α.Δ.Ε. κλπ.

[83] Σύμφωνα με το άρθρο 22§5 όταν περισσότερα από ένα συμβαλλόμενα μέρη διεκδικούν δικαιοδοσία επί ενός εγκλήματος που ποινικοποιείται σύμφωνα με τη Σύμβαση, τα εμπλεκόμενα μέρη οφείλουν να διαβουλεύονται, όπου αυτό απαιτείται, με σκοπό τον προσδιορισμό της καταλληλότερης δικαιοδοσίας για την άσκηση δίωξης.

[84] Σχετική ρύθμιση περιλήφθηκε στη USA Patriot Act και σε επίπεδο Ένωσης προωθήθηκε στο πλαίσιο της Οδηγίας 2006/24/ΕΚ για τη διατήρηση των δεδομένων, ωστόσο, η τελευταία δεν τέθηκε σε ισχύ δυνάμει της υπ' αριθμόν 54/2014 απόφασης του Δικαστηρίου της Ευρωπαϊκής Ένωσης, κρινομένου ότι περιελάμβανε ρυθμίσεις ιδιαίτερα ευρείες.

με τα αποθηκευμένα δεδομένα μέσω της λήψης κατάλληλων μέτρων[85] εξουσιοδοτούμενων των Αρχών σε αναζήτηση δεδομένων υπολογιστή σε ένα σύστημα υπολογιστή ή μέρος αυτού ή σε ανεξάρτητο μέσο αποθήκευσης δεδομένων (δισκέτα, cd-Rom).[86] Η εξουσία έρευνας και κατάσχεσης περιορίζεται στην επικράτεια του κράτους επιβολής και δεν επεκτείνεται στη διασυνοριακή έρευνα και κατάσχεση που αναπτύσσεται στο επόμενο κεφάλαιο.[87] Η αποτελεσματική συνεργασία μεταξύ Αρχών και διαχειριστών αποτελεί έτερο σημαντικό παράγοντα με σκοπό τον περιορισμό της έρευνας στις αναγκαίες πληροφορίες για την υπό κρίση περίπτωση.[88]

Η τελευταία και πιο παρεμβατική ρύθμιση σε επίπεδο Δικονομικού Δικαίου προβλέπεται στο άρθρο 20 και αφορά τη συλλογή δεδομένων κίνησης σε πραγματικό χρόνο,[89] η εφαρμογή της οποίας επεκτείνεται σε περιπτώσεις επικοινωνιών που περιλαμβάνουν μετάδοση μέσω δικτύου πριν ακόμη γίνει λήψη της επικοινωνίας από άλλο σύστημα υπολογιστή (Csonka 2006: 494). Λόγω του αυξημένα παρεμβατικού χαρακτήρα της ρύθμισης η εφαρμογή της περιορίζεται στην εξιχνίαση των σοβαρότερων προσβολών. Σε κάθε περίπτωση, ο καθορισμός του πεδίου εφαρμογής παραμένει στην ευχέρεια των κρατών.

Στο άρθρο 22 ρυθμίζονται τα ζητήματα σχετικά με τη δικαιοδοσία. Η §1στοιχείο α΄ βασίζεται στην αρχή της εδαφικότητας, βάσει της οποίας κάθε κράτος είναι αρμόδιο για τα διαπραττόμενα εντός του εδάφους του αδικήματα, η §1 στοιχείο β΄ στηρίζεται σε μια παραλλαγή της αρχής της εδαφικότητας, η §1 στοιχείο γ΄ στην αρχή της ιθαγένειας, ενώ η §1 στοιχείο δ΄ στην αρχή της εθνικότητας. Το τελευταίο αυτό στοιχείο περιλαμβάνει δυο υποχρεώσεις των κρατών: την εδραίωση δικαιοδοσίας των κρατών για αδικήματα τελούμενα από πολίτες τους στο έδαφος άλλων κρατών μελών της Σύμβασης και την εδραίωση δικαιοδοσίας για αδικήματα διαπραττόμενα από πολίτες τους στο έδαφος άλλων κρατών ακόμη και εκτός του εδάφους των κρατών μελών της Σύμβασης. Η υποχρέωση αυτή αντλεί τη δικαιολογητική της βάση από την αρχή της καθολικότητας (universality principle), εφαρμοζόμενη στις περιπτώσεις των πλέον σοβαρών

[85] Σκέψη 184
[86] Σκέψη 188
[87] Σκέψη 194
[88] Σκέψη 202
[89] Η Ελλάδα επιφυλάχθηκε να προβαίνει σε συγκέντρωση δεδομένων κίνησης σε πραγματικό χρόνο σύμφωνα με τα προβλεπόμενα για την άρση του απορρήτου των επικοινωνιών.

εγκλημάτων (Koops & Brenner 2006: 14-15). Στην §3 περιέχεται ο κανόνας *dedere aut judicare (έκδοση ή δίωξη)*, δυνάμει του οποίου στις περιπτώσεις που ένα κράτος αρνείται την έκδοση πολιτών του σε απάντηση αιτήματος άλλου κράτους μέρους της Σύμβασης, οφείλει να ασκήσει δίωξη ενάντια στον ύποπτο το ίδιο (Koops & Brenner 2006: 17). Στις περιπτώσεις που περισσότερα κράτη διεκδικούν δικαιοδοσίας προτάσσεται η διαβούλευση, όπου αυτό απαιτείται, με σκοπό τον προσδιορισμό της καταλληλότερης δικαιοδοσίας για την άσκηση της δίωξης, σε επίπεδο κρατών, χωρίς, να ρυθμίζονται εγγυήσεις για τους υπόπτους.

Το τρίτο κεφάλαιο ρυθμίζει ζητήματα διεθνούς συνεργασίας (άρθρο 23), η οποία οφείλει να είναι εκτεταμένη, ώστε να ελαχιστοποιηθούν τα εμπόδια στην ομαλή και ταχεία ροή πληροφοριών και αποδεικτικών στοιχείων σε διεθνές επίπεδο,[90] έκδοσης ('double jeopardy' protection)[91] (άρθρο 24) και αμοιβαίας συνδρομής.[92] (άρθρα 25-34) Επιπλέον, καθιερώνεται εικοσιτετράωρο δίκτυο επαφής για τη διασφάλιση της παροχής άμεσης συνδρομής κατά την έρευνα, δίωξη και συλλογή αποδεικτικών στοιχείων (άρθρο 35). Το τελευταίο (δίκτυο επαφής) συγκαταλέγεται στα σημαντικότερα μέσα που παρέχει η Σύμβαση για την αποτελεσματική απάντηση στις νομοθετικές προκλήσεις και είναι διαθέσιμο 24 ώρες την ημέρα και 7 ημέρες την εβδομάδα (24/7 network). Στις αρμοδιότητες του δικτύου ανήκουν η παροχή τεχνικών και νομικών συμβουλών, η διατήρηση των δεδομένων, η συλλογή των αποδείξεων και ο εντοπισμός των ηλεκτρονικών ιχνών, καθώς επίσης, η συντονισμένη συνεργασία περισσότερων Αρχών (Csonka 2006: 496).

[90] Σκέψη 242 ό.π.

[91] Στο άρθρο 24§1^{α} καθιερώνεται η αρχή του διπλού αξιοποίνου σε θέματα έκδοσης υπό την προϋπόθεση ότι η επαπειλούμενη ποινή ανέρχεται σε τουλάχιστον 1 έτος υπό την επιφύλαξη της §1β και σκοπείται η προστασία έναντι της δίωξης σε περισσότερα κράτη για το ίδιο αδίκημα. Η έκδοση υπόκειται στις προϋποθέσεις που προβλέπει το Δίκαιο του συμβαλλόμενου μέρους, προς το οποίο απευθύνεται το αίτημα ή οι ισχύουσες συμβάσεις περί έκδοσης, συμπεριλαμβανομένων και των λόγων για τους οποίους το συμβαλλόμενο μέρος, προς το οποίο απευθύνεται το αίτημα, μπορεί να αρνηθεί την έκδοση. Η Σύμβαση καθιερώνει τη δυνατότητα έκδοσης για όλες τις προσβολές που περιλαμβάνει. Η έκδοση απαιτεί από κάθε κράτος-μέλος να συμφωνήσει να παραδώσει τον υποψήφιο δράστη σε άλλο κράτος-μέλος, δοθέντος ότι υπάρχει εν ισχύι συνθήκη έκδοσης μεταξύ των δύο κρατών, εν τη απουσία της οποίας, η Σύμβαση ενθαρρύνει τα συμβαλλόμενα κράτη να χρησιμοποιούν την ίδια τη Σύμβαση ως τη νομική αρχή έκδοσης για υπόπτους τέλεσης διαδικτυακών εγκλημάτων.

[92] Τα συμβαλλόμενα μέρη υποχρεούνται να παρέχουν την ευρύτερη δυνατή αμοιβαία συνδρομή για την πραγματοποίηση ερευνών και την άσκηση διώξεων, ενώ άρνηση συνδρομής μπορούν να δικαιολογήσουν πολιτικά εγκλήματα ή εγκλήματα σχετιζόμενα με αυτά, καθώς επίσης λόγοι κυριαρχίας, ασφάλειας, δημόσιας τάξης ή άλλα ουσιαστικά δικαιώματα του κράτους που αρνείται τη συνδρομή. (άρθρο 27§4).

2.3.3 Ευρωπαϊκές Οδηγίες

Εστιάζοντας στις κυριότερες απειλές του ψηφιακού περιβάλλοντος, όπως τις κατατάσσει η Ευρωπαϊκή Επιτροπή διακρίνοντας σε εγκληματική δραστηριότητα παραδοσιακής μορφής με τη χρήση του Διαδικτύου, δημοσίευση παράνομου περιεχομένου και αξιόποινες πράξεις που μπορούν να διαπραχθούν μόνο μέσω ηλεκτρονικών δικτύων,[93] μεταξύ των οποίων τις υψηλότερες θέσεις καταλαμβάνουν οι επιθέσεις ransomware και DDoS σε δημόσιους και ιδιωτικούς φορείς και ακολουθούν τα εγκλήματα σεξουαλικής εκμετάλλευσης και απάτες τύπου skimming κυρίως (IOCTA 2018), οι κύριες ευρωπαϊκές οδηγίες που απευθύνονται ευθέως στο ηλεκτρονικό έγκλημα παρατίθεται ως κάτωθι:

i) Η Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών

Η οδηγία 2013/40/ΕΕ αντικατέστησε την απόφαση πλαίσιο 2005/222/ΔΕΥ[94] του Συμβουλίου για τις επιθέσεις κατά των συστημάτων πληροφοριών, κρινόμενης της τελευταίας ως ξεπερασμένης και ακατάλληλης πλέον να αντιμετωπίσει ευχερώς τις νέες μορφές επιθέσεων κατά των συστημάτων πληροφοριών, καθιερώνοντας ελάχιστους κανόνες σε αναφορά με τον ορισμό των ποινικών αδικημάτων και τις σχετικές κυρώσεις και επιπλέον, τη βελτίωση της συνεργασίας μεταξύ των αρμόδιων Αρχών. Στις αρμόδιες Αρχές συμπεριελήφθησαν η αστυνομία και άλλες συσταθείσες υπηρεσίες, καθώς επίσης, οργανισμοί και επιμέρους φορείς της Ένωσης (Eurojust, η Europol, AC3 και ENISA).[95] Επισημάνθηκε δε, η αυξανόμενη απειλή του οργανωμένου εγκλήματος και η αναγκαιότητα προστασίας των υποδομών ζωτικής σημασίας των κρατών μελών της Ένωσης έναντι των μαζικών επιθέσεων σε πληροφοριακά συστήματα με διασυνοριακό αντίκτυπο (επιθέσεις "Botnet").[96] Αναγκαία στο πλαίσιο αυτό κρίθηκε η κοινή προσέγγιση των στοιχείων της αντικειμενικής υπόστασης των ποινικών αδικημάτων της παράνομης πρόσβασης σε σύστημα πληροφοριών, της παράνομης παρεμβολής σε

[93] Διαθέσιμο εδώ: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14560&from=EN

[94] Η απόφαση προέβλεπε την ποινικοποίηση των αδικημάτων της παράνομης πρόσβασης σε δεδομένα, της παράνομης παρεμβολής σε σύστημα και της παράνομης παρεμβολής σε δεδομένα.

[95] Σκέψη 1

[96] Σκέψη 2, 3 και 5

συστήματα και δεδομένα και της υποκλοπής[97], καθώς επίσης, η προώθηση της συνεργασίας δημοσίων και ιδιωτικών φορέων των κρατών μελών.[98] Στην κατεύθυνση αυτή, η παρούσα οδηγία ενίσχυσε τη σημασία των δικτύων δράσης, όπως το δίκτυο των σημείων επαφής της ομάδας G8 και του Συμβουλίου της Ευρώπης, που είναι διαθέσιμο σε 24ωρη βάση, ενισχύοντας την αποτελεσματική παροχή βοήθειας δια της ανταλλαγής συγκριτικών δεδομένων, τεχνικών συμβουλών και νομικών πληροφοριών για έρευνες ή διαδικασίες σχετικές με ποινικά αδικήματα που συνδέονται με συστήματα πληροφοριών και συναφή δεδομένα των κρατών μελών.[99]

ii) Η οδηγία 2019/7313/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την καταπολέμηση της απάτης και της πλαστογραφίας πληρωμών με μέσα πλην των μετρητών σε αντικατάσταση της απόφασης-πλαισίου 2001/413/ΔΕΥ του Συμβουλίου για την online απάτη

Η Οδηγία εκδόθηκε σε αντικατάσταση της απόφασης-πλαισίου 2001/413/ΔΕΥ, έπειτα από τη διαπίστωση της αυξημένης απειλής που συνεπάγεται η απάτη στον κυβερνοχώρο, ορώμενης της τελευταίας ως παράγοντος περαιτέρω εγκληματικής δραστηριότητας και εμποδίου για την ενιαία αγορά που, από κοινού με την απομίμηση μέσων πληρωμής πλην των μετρητών, διαταράσσει την εμπιστοσύνη των καταναλωτών και προκαλεί άμεσες οικονομικές απώλειες.[100] Η οδηγία στοχεύει στην επικαιροποίηση των προϋφιστάμενων κανόνων, με σκοπό τη διαμόρφωση ενός σαφούς νομικού πλαισίου, ανταποκρινόμενου στις ανάγκες της σύγχρονης εποχής. Σε αυτό το πλαίσιο περιλαμβάνονται νέοι τύποι πληρωμών, όπως η μεταφορά ηλεκτρονικού χρήματος και

[97] Σκέψη 8

[98] Επιτακτική είναι η ανάγκη συλλογής συγκρίσιμων δεδομένων σχετικά με τα προβλεπόμενα αδικήματα, τα οποία θα πρέπει να τίθενται στη διάθεση των αρμόδιων ειδικευμένων οργανισμών και φορέων της Ένωσης, όπως η Europol και η ENISA, σύμφωνα με τα καθήκοντά τους και τις ανάγκες πληροφόρησης, ώστε να αποκτούν μια πιο ολοκληρωμένη εικόνα του προβλήματος της εγκληματικότητας στον κυβερνοχώρο συντελώντας στην ασφάλεια δικτύων και πληροφοριών στο επίπεδο της Ένωσης. Τα κράτη μέλη θα πρέπει να υποβάλλουν πληροφορίες σχετικά με το modus operandi που χρησιμοποιείται από τους δράστες δια μέσου των αρμόδιων φορέων, ώστε να προβαίνουν σε αξιολογήσεις επί των απειλών και στρατηγικές αναλύσεις του εγκλήματος στον κυβερνοχώρο σύμφωνα με την απόφαση 2009/371/ΔΕΥ του Συμβουλίου, της 6ης Απριλίου 2009, για την ίδρυση Ευρωπαϊκής Αστυνομικής Υπηρεσίας (Europol). Η παροχή πληροφοριών μπορεί να διευκολύνει την καλύτερη κατανόηση των σημερινών και μελλοντικών απειλών και να συμβάλει έτσι στη λήψη καταλληλότερων και στοχευμένων αποφάσεων για την καταπολέμηση και την πρόληψη των επιθέσεων κατά των συστημάτων πληροφοριών. Σκέψη 24.

[99] Σκέψη 22

[100] Σκέψεις 1 και 2

εικονικών νομισμάτων και η διατήρηση ηλεκτρονικών πορτοφολιών[101] στο μέτρο που τα τελευταία μπορούν να χρησιμοποιηθούν ευρέως στις πληρωμές. Τα κράτη μέλη ενθαρρύνονται να εντάξουν την παραγωγή εικονικών νομισμάτων σε ένα νόμιμο πλαίσιο με την έκδοση αυτών από κεντρικές Τράπεζες ή άλλες δημόσιες αρχές και τον έλεγχό τους, ώστε να διασφαλίζεται αντίστοιχη προστασία με την προβλεπόμενη για τα παραδοσιακά μέσα πληρωμή.[102] Οι δε σχετικές με την απάτη και παραχάραξη μέσων πληρωμής, πλην των μετρητών, κυρώσεις, προβλέπεται ότι πρέπει να είναι αποτελεσματικές, αναλογικές και να φέρουν αποτρεπτικό χαρακτήρα σε ολόκληρη την Ένωση.[103] Έμφαση δίνεται στη διεθνή συνεργασία και την ανταλλαγή πληροφοριών[104] προς την εξασφάλιση της καλύτερης αντιμετώπιση της διασυνοριακής απάτης. Περαιτέρω, εναρμονίζονται έννοιες όπως η παραβίαση υπολογιστή (hacking) και το ηλεκτρονικό «ψάρεμα» (phishing) και η αντιγραφή δεδομένων κάρτας (skimming), καθώς επίσης, θεσπίζεται ένα ελάχιστο επίπεδο αναφοράς για τις μέγιστες ποινές που μπορούν να επιβληθούν σε φυσικά πρόσωπα.[105] Σε κάθε δε περίπτωση, τα κράτη μέλη είναι ελεύθερα να θεσπίσουν αυστηρότερες ρυθμίσεις, στα οποία εναπόκειται η θέσπιση ή ενίσχυση πολιτικών για την πρόληψη της απάτης και τη μείωση του κινδύνου μέσω ενημερωτικών εκστρατειών και εκστρατειών ευαισθητοποίησης και έρευνας.

iii) Η Οδηγία 2011/92/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 2011σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαισίου 2004/68/ΔΕΥ του Συμβουλίου

Η Οδηγία εκδόθηκε προς τον σκοπό της πληρέστερης ανταπόκρισης σε νέες απειλές όπως το ‘grooming’ που αυξάνονται και εξαπλώνονται με τη χρήση νέων τεχνολογιών και του Διαδικτύου[106] αντικαθιστώντας την απόφαση-πλαίσιο 2004/68 /ΔΕΥ του Συμβουλίου για την καταπολέμηση της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας, μέσα από την ποινικοποίηση των σοβαρότερων μορφών τέτοιας φύσης αδικημάτων και τη διεύρυνση της δικαιοδοσίας των εθνικών δικαστηρίων

[101] Σκέψη 7
[102] Σκέψη 7α
[103] Σκέψη 10 και 29
[104] Σκέψεις 15 και 18
[105] Άρθρο 8
[106] Σκέψη 3

για την πρόβλεψη ενός ελάχιστου επιπέδου συνδρομής για τα θύματα. Οι νέες διατυπώσεις προβλέπουν την ποινικοποίηση της απόκτησης πρόσβασης σε υλικό παιδικής πορνογραφίας που καθίσταται προσβάσιμο μέσω της τεχνολογίας των πληροφοριών και επικοινωνιών, συντρεχουσών των προϋποθέσεων της επιδίωξης της πρόσβασης στον ιστότοπο όπου διατίθεται το σχετικό υλικό και της γνώσης της ύπαρξης τέτοιων εικόνων.[107] Ακούσιες επομένως πράξεις παραμένουν εκτός του πεδίου ευθύνης.[108] Διατηρουμένης της ανάγκης αντιμετώπισης του φαινομένου της προσέγγισης ενός παιδιού εκτός του πλαισίου του Διαδικτύου, τα κράτη μέλη υποχρεώνονται να διασφαλίσουν την ποινική δίωξη των υπαιτίων, λαμβάνοντας υπόψη τα ειδικά χαρακτηριστικά του Διαδικτύου, μεταξύ των οποίων, η ανωνυμία που επιτρέπει στους χρήστες την απόκρυψη της πραγματικής ταυτότητας και των προσωπικών χαρακτηριστικών τους, όπως, για παράδειγμα, το στοιχείο της ηλικίας τους.[109] Περαιτέρω, τα κράτη μέλη υποχρεώνονται σε διατήρηση των κατάλληλων ερευνητικών εργαλείων για τους σκοπούς της έρευνας και δίωξης, μεταξύ των οποίων, η ηλεκτρονική παρακολούθηση, η παρακολούθηση τραπεζικών λογαριασμών και η κατά περίπτωση απόκρυψη της ταυτότητας των αρχών επιβολής του νόμου στο Διαδίκτυο.[110] Επίσης, ορίζεται ότι οι κανόνες δικαιοδοσίας θα πρέπει να τροποποιηθούν κατά τρόπο που θα διασφαλίζει τη δίωξη δραστών που προέρχονται από την Ένωση σε περιπτώσεις διάπραξης των σχετικών εγκλημάτων εκτός Ένωσης.[111] Προς τον σκοπό αυτό τα κράτη υποχρεούνται σε ενίσχυση του ανοικτού διαλόγου, ο οποίος προωθείται περαιτέρω μέσω της δημιουργίας μηχανισμών συλλογής δεδομένων[112] και υπηρεσιών πληροφοριών για την ενημέρωση σχετικά με την αναγνώριση των ενδείξεων τέλεσης τέτοιων εγκλημάτων.[113]

iv) Η Οδηγία 2016/1148/ΕΕ σχετικά με τα μέτρα για ένα υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση ('NIS')

[107] Ενδεικτικό του εκούσιου χαρακτήρα αποτελεί ο κατ' επανάληψη χαρακτήρας της πράξης ή η επιδίωξη αυτής έναντι αμοιβής. Σκέψη 18
[108] Σκέψη 18
[109] Σκέψη 19
[110] Σκέψη 27
[111] Σκέψη 29
[112] Σκέψη 44
[113] Σκέψη 45

Με την Οδηγία[114] θεσπίζονται μέτρα για την επίτευξη υψηλού κοινού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών εντός της Ένωσης με σκοπό την καλύτερη λειτουργία της εσωτερικής αγοράς μέσα από την ενίσχυση της ασφάλειας των συστημάτων δικτύου και πληροφοριών και την ανάπτυξη εμπιστοσύνης και αξιοπιστίας μεταξύ των κρατών μελών. Προς τον σκοπό αυτό προβλέπεται η υποχρέωση θέσπισης εθνικής στρατηγικής για την ασφάλεια των συστημάτων δικτύου και πληροφοριών από όλα τα κράτη μέλη.[115] Περαιτέρω, στις κύριες ρυθμίσεις της Οδηγίας περιλαμβάνεται η δημιουργία ομάδων συνεργασίας με σκοπό την υποστήριξη και τη διευκόλυνση της στρατηγικής συνεργασίας και της ανταλλαγής πληροφοριών[116] και η δημιουργία δικτύου ομάδων απόκρισης συμβάντων που αφορούν την ασφάλεια των υπολογιστών (CSIRT)[117] για την προώθηση της ταχείας και αποτελεσματικής επιχειρησιακής συνεργασίας. Ακόμη, θεσπίζονται απαιτήσεις ασφάλειας και κοινοποίησης για τους φορείς εκμετάλλευσης βασικών υπηρεσιών (Operations of Essential Services), οι οποίοι θα πρέπει να λάβουν τα κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση κινδύνων, την αποτροπή και ελαχιστοποίηση του αντικτύπου συμβάντων και τη χωρίς αδικαιολόγητη καθυστέρηση κοινοποίηση στην αρμόδια αρχή ή στην CSIRT συμβάντων με σοβαρό αντίκτυπο[118] στη συνέχεια των βασικών υπηρεσιών.[119] Αντίστοιχες απαιτήσεις προβλέπονται για τους παρόχους ψηφιακών υπηρεσιών (Digital Service Providers),[120] στους οποίους περιλαμβάνονται τα ηλεκτρονικά καταστήματα, οι μηχανές αναζήτησης και οι υπηρεσίες νεφουπολογιστικής (cloud computing). Λαμβανομένου υπόψη ότι τα περισσότερα συστήματα δικτύου και πληροφοριών ανήκουν σε ιδιωτικούς φορείς προωθείται η συνεργασία μεταξύ ιδιωτικών και δημόσιων φορέων, καθώς επίσης, η διαμόρφωση άτυπων μορφών συνεργασίας από τους φορείς εκμετάλλευσης βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών.[121] Τέλος, προβλέπεται η δημιουργία ενιαίων κέντρων επαφής που θα πρέπει να συνεργάζονται με τις εθνικές αρμόδιες αρχές και τις CSIRT για τους σκοπούς της Οδηγίας.[122]

[114] Η Οδηγία κυρώθηκε από την ελληνική έννομη τάξη με τον Ν. 4577/2019.
[115] Σκέψη 29
[116] Σκέψη 33
[117] Σκέψη 34
[118] Η σοβαρότητα κρίνεται με γνώμονα τον αριθμό των χρηστών που επηρεάζονται από τη διατάραξη της βασικής υπηρεσίας, τη διάρκεια του συμβάντος και το γεωγραφικό εύρος της πληττόμενης περιοχής. Σε ό, τι δε αφορά στις βασικές υπηρεσίες, ως τέτοιες εννοούνται οι υπηρεσίες ενέργειας, μεταφορών, υγείας και οι χρηματοπιστωτικές υπηρεσίες.
[119] Άρθρο 14
[120] Σκέψη 49
[121] Σκέψη 35
[122] Άρθρα 8 και 10

2.4. Φορείς ευρωπαϊκής και διεθνούς συνεργασίας

Στο πλαίσιο της ενίσχυσης μιας ολοκληρωμένης πολιτικής αντιμετώπισης του ηλεκτρονικού εγκλήματος ιδιαίτερα σημαντική τυγχάνει η δράση πλειόνων φορέων που δραστηριοποιούνται σε διεθνές και ευρωπαϊκό επίπεδο. Η Interpol, σε επίπεδο διεθνούς εκπροσώπησης, αποτελεί το δεύτερο μεγαλύτερο οργανισμό μετά τα Ηνωμένα Έθνη, που ήδη από το έτος 1990, οπότε ίδρυσε το European Working Party of Information Technology Crime δραστηριοποιείται ενεργά στη μάχη κατά του ηλεκτρονικού εγκλήματος σε συνεργασία με ομάδες εργασίες στην Αμερική, την Ευρώπη, την Ασία και την Αφρική. Σκοπός της είναι η προώθηση της αμοιβαίας συνεργασίας των επιμέρους εθνικών αρχών και η αποτελεσματική πρόληψη της εγκληματικότητας σε παγκόσμιο επίπεδο. Μεταξύ των σημαντικότερων αδικημάτων που εμπίπτουν στο αντικείμενό της περιλαμβάνονται η τρομοκρατία, το οργανωμένο έγκλημα, τα εγκλήματα κατά της ανθρωπότητας, το λαθρεμπόριο όπλων και η παιδική πορνογραφία. Πρόκειται δε, για πολιτικά ουδέτερο οργανισμό κατά τα οριζόμενα στον καταστατικό της χάρτη.[123] Άλλο σημαντικό φορέα που δραστηριοποιείται στην καταπολέμηση του σοβαρού διεθνούς εγκλήματος και της τρομοκρατίας αποτελεί η Europol (European Police Office) με έδρα τη Χάγη, η οποία το 2013 ίδρυσε το Ευρωπαϊκό Κέντρο για το έγκλημα στον κυβερνοχώρο (European Cybercrime Center-AC3), στο πλαίσιο της ενίσχυσης της νομοθεσίας στη μάχη κατά του ηλεκτρονικού εγκλήματος στην ΕΕ με σκοπό την παροχή βοήθειας σε ευρωπαίους πολίτες, επιχειρήσεις και κυβερνήσεις. Από την ίδρυσή της, η EC3 έχει συμβάλει σημαντικά στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο έχουσα συμμετάσχει σε πλειάδα επιχειρήσεων (‘Operation Onymous’, ‘Operation Pachtou’, ‘Operation Koala’). Κάθε χρόνο, δημοσιεύει αναφορά με τις εκτιμήσεις των απειλών του Οργανωμένου Εγκλήματος (IOCTA 2019), η οποία αποτελεί την στρατηγική της έκθεση σχετικά με τα βασικά ευρήματα και τις αναδυόμενες απειλές και εξελίξεις σε αναφορά με το έγκλημα στον κυβερνοχώρο. Ειδικής μνείας χρήζει και η Eurojust, ιδρυθείσα το 2001 με έδρα επίσης τη Χάγη, η οποία αποτελεί την μονάδα δικαστικής συνεργασίας της ΕΕ και καθήκον το δικαστικό συντονισμό και τη συνεργασία μεταξύ των επιμέρους εθνικών αρχών για την καταπολέμηση του σοβαρού οργανωμένου εγκλήματος σε περισσότερες

[123] Δεν επιτρέπεται η ανάληψη δραστηριοτήτων στρατιωτικής, πολιτικής, θρησκευτικής ή φυλετικής φύσης ή η εμπλοκή σε θέματα ουσίας.

από μία χώρες της ΕΕ. Τέλος, στους σημαντικότερους φορείς, στο πλαίσιο της ενίσχυσης της ασφάλειας των δικτύων και πληροφοριών, συγκαταλέγεται η ENISA (European Network and Information Security System), η οποία συστάθηκε δυνάμει του Κανονισμού 460/2004 και αποτελεί το ευρωπαϊκό κέντρο εμπειρογνωσίας για την ασφάλεια στον κυβερνοχώρο. Στις αρμοδιότητές της ανήκει η προώθηση της συνεργασίας ανάμεσα σε ιδιωτικούς και δημόσιους φορείς και η ενίσχυση της αποτελεσματικής προετοιμασίας της Επιτροπής και των κρατών όσον αφορά στον εντοπισμό και την επίλυση προβλημάτων που σχετίζονται με την ασφάλεια των πληροφοριών.[124]

2.5 Ελληνική Έννομη Τάξη

2.5.1 Ν. 4411/2016

Η Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο και το Πρόσθετο Πρωτόκολλο για την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω συστημάτων υπολογιστών, καθώς επίσης, η Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών,[125] ενσωματώθηκαν στην ελληνική έννομη τάξη με το Ν. 4411/16 (ΦΕΚ Α΄ 142/3.8.2016),[126] δυνάμει του οποίου εισήχθησαν σημαντικές ρυθμίσεις προς το σκοπό της καταπολέμησης του ηλεκτρονικού εγκλήματος και οι οποίες αποτυπώνονται, ειδικότερα, στα άρθρα 13, $292^{Β}$, $292^{Γ}$, $348^{Β}$, $370^{Γ}$ -$370^{Ε}$, $381^{Α}$, $381^{Β}$ και $386^{Α}$ του Ποινικού Κώδικα (ΠΚ). Στο άρθρο 13 ΠΚ περιλήφθηκαν οι όροι «πληροφοριακό σύστημα» και «ψηφιακά δεδομένα» και επιπλέον, στο εικοστό δεύτερο κεφάλαιο του Ποινικού Κώδικα, όπου περιγράφονται οι προσβολές ατομικού απορρήτου και επικοινωνίας, ενσωματώθηκαν οι προβλέψεις της πρώτης ενότητας του

[124] Αξίζει να σημειωθεί σε εγχώριο επίπεδο η δράση του Διεθνούς Ινστιτούτου Κυβερνοασφάλειας (CSIi Institute), ιδρυθέντος το έτος 2017 από τον Αντιστράτηγο της Ελληνικής Αστυνομίας και επί σειρά ετών επικεφαλής της δίωξης ηλεκτρονικού εγκλήματος, Εμμανουήλ Σφακιανάκη, το οποίο εμφανίζει εξέχουσα δράση στο θέμα της αντιμετώπισης θεμάτων ασφαλείας στο Διαδίκτυο, προωθώντας παράλληλα την εκπαίδευση, ενεργοποίηση και τεχνολογική έρευνα στον τομέα των νέων τεχνολογιών και του Διαδικτύου.

[125] Η οποία ακολούθησε σε αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου («Οδηγία») καλώντας τα κράτη μέλη της ΕΕ να χρησιμοποιούν τα ίδια σημεία επαφής με τα χρησιμοποιούμενα στο Συμβούλιο της Ευρώπης και τους G8 προς την κατεύθυνση της ταχείας αντιμετώπισης της απειλής του ηλεκτρονικού εγκλήματος.

[126] «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».

δευτέρου κεφαλαίου της Σύμβασης σχετικά με τα εγκλήματα κατά της εμπιστευτικότητας, της ακεραιότητας και διαθεσιμότητας των δεδομένων και συστημάτων πληροφοριών, για τα οποία μέχρι τότε εφαρμόζονταν οι διατάξεις του Ν. 1805/1988.[127] Παρά ταύτα, δεν προβλέφθηκαν ιδιαίτερες τροποποιήσεις στην Ποινική Δικονομία σχετικά με τα μέσα εξιχνίασης ηλεκτρονικών εγκλημάτων και ιδίως την εξέταση ψηφιακών πειστηρίων Σημαντικές μεταρρυθμίσεις επήλθαν υπό τις μεταρρυθμίσεις του Ν. 4619/19 (ΦΕΚ Α΄ 95/11.6.2019) και του νέου Ποινικού Κώδικα, όπως ισχύει μετά την ψήφιση και θέση σε ισχύ του Ν. 4640/2019 (ΦΕΚ Α΄ 190/30.11.2019).

2.5.2 Εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων και πληροφοριών στην ελληνική έννομη τάξη

i) Προσβολές ατομικού απορρήτου και επικοινωνίας: άρθρα 370 επ. ΠΚ

Υπό το φως του νέου Ποινικού Κώδικα στο άρθρο 370 ΠΚ που τιτλοφορείται «Παραβίαση απορρήτου εγγράφων» προστίθεται η §2 που τιμωρεί με ποινή φυλάκισης έως 2 έτη ή χρηματική ποινή όποιον αθέμιτα αποκτά πρόσβαση σε ηλεκτρονικό μήνυμα ή ηλεκτρονική αλληλογραφία άλλου. Στην επόμενη παράγραφο (§3) προβλέπεται αυστηρότερο πλαίσιο ποινής τουλάχιστον 1 έως 3 έτη ή χρηματική ποινή στη διακεκριμένη μορφή του εγκλήματος, όταν το υποκείμενο δράσης φέρει μία από τις περιγραφόμενες ιδιότητες.[128] Πρόκειται δε για κατ' έγκληση διωκόμενο αδίκημα (§4).

Στο άρθρο 370^{A} ΠΚ περί παραβίασης του απορρήτου τηλεφωνικής επικοινωνίας και προφορικής συνομιλίας επιδιώκεται ο εξορθολογισμός του καθ' υπέρβαση της αρχής της αναλογικότητας νομοθετικού πλαισίου του Ν. 3674/2008 και προστίθεται η παρακολούθηση προφορικής συνομιλίας τρίτων που δε διεξάγεται δημόσια, όπως είχε υιοθετηθεί από το Ν. 2172/1993, και η αποτύπωση σε υλικό φορέα μη δημόσιας πράξης άλλου ή της συνομιλίας του δράστη με άλλον χωρίς τη συγκατάθεση του τελευταίου,

[127] Ο οποίος είχε εισαγάγει στα άρθρα 370Β, 370Γ, 386Α του Ποινικού Κώδικα τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές.
[128] Υπάλληλος οργανισμού ή επιχείρησης παροχής ταχυδρομικών, τηλεγραφικών ή ηλεκτρονικών υπηρεσιών.

οπότε απειλείται φυλάκιση τουλάχιστον 1 έτους (§2).[129] Προϋπόθεση πλήρωσης της νομοτυπικής υπόστασης των αδικημάτων της παραβίασης του απορρήτου τηλεφωνικής επικοινωνίας και προφορικής συνομιλίας, όπως περιγράφονται στις §§1, 2 και 3 αποτελεί ο αθέμιτος χαρακτήρας της ενέργειας, μη συντρέχοντος του οποίου αίρεται το κατ' αρχήν άδικο της πράξης. Περαιτέρω, απόκειται στο δικαστήριο ή την ανακριτική αρχή να κρίνει αν συντρέχει λόγος άρσης του αδίκου, ιδίως δε, στις περιπτώσεις που πρόκειται για το μοναδικό μέσο που αποδεικνύει την αθωότητα του κατηγορουμένου, οπότε διαπιστώνεται η ανάγκη διαφύλαξης δικαιολογημένου συμφέροντος που δε μπορούσε να διαφυλαχθεί διαφορετικά (Χαραλαμπάκης 2019: 110).

Στο άρθρο 370^{Β} ΠΚ τυποποιείται, υπό το καθεστώς του προϊσχύοντος Ποινικού Κώδικα προβλεπόμενο στο άρθρο 370^{Γ} ΠΚ, το αδίκημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα ή σε ηλεκτρονικά δεδομένα, που ποινικοποιήθηκε στο πλαίσιο προώθησης της αξίωσης ποινικοποίησης της εκ προθέσεως και άνευ δικαιώματος πρόσβασης στο σύνολο ή σε τμήμα συστήματος ηλεκτρονικών υπολογιστών (hacking).[130] Ειδικότερα, τυποποιείται η μη εξουσιοδοτημένη πρόσβαση, χωρίς να απαιτείται απαραιτήτως να συνοδεύεται από σκοπό δολιοφθοράς, καταστροφής ή αποκόμισης οικονομικού οφέλους,[131] αλλά αρκεί η άντληση ηθικής και μόνο ικανοποίησης του δράστη από την παράκαμψη των συστημάτων ασφαλείας και την επίδειξη των τεχνικών ικανοτήτων του (Δαλακούρας 2018: 8). Καίριας σημασίας είναι η «χωρίς δικαίωμα» πρόσβαση που συνιστά προϋπόθεση της αντικειμενικής υπόστασης του αδικήματος. Συνεπώς, στην περίπτωση αυτή, σε αντίθεση με τη διαπίστωση του «αθέμιτου» χαρακτήρα του προηγούμενου άρθρου που περιλαμβάνεται στα «ειδικά

[129] Η αθέμιτη χρήση της πληροφορίας ή του φορέα επί του οποίου έχει αποτυπωθεί κατά τα οριζόμενα στις §§2 και 3 τιμωρείται με φυλάκιση έως 3 έτη ή χρηματική ποινή, ενώ αυστηρότερες είναι οι κυρώσεις στις διακεκριμένες μορφές της §4 οπότε ο δράστης ως εκ της ιδιότητάς του απειλείται με τιμωρία τουλάχιστον 3 ετών και χρηματική ποινή σωρευτικά.

[130] Article 2 – Illegal access. *Each Party shall adopt such legislative and other measures as may be necessary to*
establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.

[131] Η ποινικοποίηση της απλής πρόσβασης σε ηλεκτρονικά δεδομένα ανεξάρτητα από την επέλευση ζημίας, δικαιολογείται από το δικαίωμα κάθε προσώπου στην προστασία του απορρήτου συγκεκριμένων δεδομένων του, καθώς επίσης, κατ' άλλη άποψη, από το έννομο αγαθό της περιουσίας π.χ. στην περίπτωση που νόμιμος κάτοχος του συστήματος είναι νομικό πρόσωπο (*Carr. I and William S.K.* (2002), Cybercrime Convention, Criminalization and the Council of Europe, Draft, *Computer Law & Security Report* 84, αναφέρεται στον Δαλακούρα (2018: 7). Σύμφωνο με τη διάταξη αυτή το υπ' αριθμόν 3204/1993 Βούλευμα του Συμβουλίου Πλημμελειοδικών Θεσσαλονίκης, έκρινε ότι: « Η διάταξη λοιπόν αυτή προστατεύει τα προγράμματα των υπολογιστών ως ένα ιδιαίτερο περιουσιακό αγαθό που εκφράζει κάποια οικονομική αξία ανάλογη με τη φύση του προγράμματος, το κόστος παραγωγής». Τρίτη άποψη προτάσσει την ασφάλεια του ηλεκτρονικού συστήματος (Βλαχόπουλος 2007: 137 σε Δαλακούρα 2018: 8).

στοιχεία του αδίκου» ελλείψει των οποίων ο άδικος χαρακτήρας αίρεται, αποκλείεται ήδη η πλήρωση της αντικειμενικής υπόστασης και το προστατευόμενο έννομο αγαθό δε θεωρείται ότι προσβάλλεται. Στην §2, η οποία διατηρείται ως περιγραφόταν στην §3 του προγενέστερου άρθρου 370^{Γ} ΠΚ, περιγράφονται οι περιπτώσεις 'white hacking;' ή 'ethical hacking' που αφορούν σε δοκιμές διείσδυσης (penetration tests), στις οποίες ο δράστης, κατόπιν εντολής του κατόχου του πληροφοριακού συστήματος, επιδιώκει να αποκτήσει πρόσβαση στο σύστημα με σκοπό τον έλεγχο του επιπέδου ασφαλείας του και τιμωρούνται μόνο αν απαγορεύονται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου. Αυξημένη ποινή προβλέπεται αν η πράξη αναφέρεται σε επιστημονικά ή επαγγελματικά απόρρητα επιχείρησης του ιδιωτικού ή δημοσίου τομέα (§3-φυλάκιση έως 3 έτη ή χρηματική ποινή διαζευκτικά έναντι της § που προβλέπει ανώτατο όριο φυλάκισης τα 2 έτη), καθώς και όταν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου και το απόρρητο είναι ιδιαίτερα μεγάλης αξίας επιβάλλεται σωρευτικά στερητική της ελευθερίας ποινή και χρηματική ποινή (§4). Με την εξαίρεση της §3 απαιτείται έγκληση για την άσκηση ποινικής δίωξης.

Στο άρθρο 370^{Γ} ΠΚ ποινικοποιείται η αθέμιτη αντιγραφή, αποτύπωση, χρήση, αποκάλυψη σε τρίτο ή παραβίαση στοιχείων ή προγραμμάτων υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα με ποινή φυλάκισης τουλάχιστον 3 μηνών, παρεκτός αν συντρέχει η επιβαρυντική περίσταση της §2, οπότε, στην περίπτωση που ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου και το απόρρητο είναι ιδιαίτερα μεγάλης αξίας επιβάλλεται ποινή τουλάχιστον 1 έτους. Τα αυτά προβλέπονταν αυτούσια στο άρθρο 370^{Β} ΠΚ του προϊσχύοντος Ποινικού Κώδικα διατηρουμένου του ίδιου πλαισίου ποινής. Πρόκειται επίσης για κατ' έγκληση διωκόμενο αδίκημα.

Υπό το πρίσμα του προϊσχύοντος Ποινικού Κώδικα, στο άρθρο 370^{Δ} ΠΚ τυποποιείτο ως αυτοτελές αδίκημα κακουργηματικού χαρακτήρα η παραβίαση του απορρήτου των επικοινωνιών μέσω πληροφοριακών συστημάτων υπό τις διατυπώσεις της §1 και η χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου η πληροφορία αποτυπώθηκε (§2), με επαπειλούμενη την ποινή της κάθειρξης έως 10 ετών. Υπό το νέο Ποινικό Κώδικα η διατύπωση του ανωτέρω αδικήματος μεταφέρεται στο άρθρο 370^{Ε}

ΠΚ,[132] δυνάμει του οποίου τιμωρείται όποιος αθέμιτα, με τη χρήση τεχνικών μέσων, παρακολουθεί ή αποτυπώνει σε υλικό φορέα μη δημόσιες διαβιβάσεις δεδομένων ή ηλεκτρομαγνητικές εκπομπές από, προς ή εντός πληροφοριακού συστήματος ή παρεμβαίνει σε αυτές με σκοπό την ίδια πληροφόρηση ή την πληροφόρηση άλλου για το περιεχόμενο αυτού, καθώς και όποιος κάνει χρήση αυτής ή του υλικού φορέα αυτής, πλην όμως, υπό τις νέες διατυπώσεις ο κακουργηματικός χαρακτήρας αίρεται και η ποινή της κάθειρξης αντικαθίσταται με φυλάκιση τουλάχιστον 3 ετών και χρηματική ποινή. Το άρθρο 370^{Δ} ΠΚ τιμωρεί με χρηματική ποινή ή παροχή κοινωφελούς εργασίας[133] τη χωρίς δικαίωμα αντιγραφή ή χρήση προγραμμάτων υπολογιστών (§1), ενώ αυστηρότερη ποινή επαπειλείται στην περίπτωση της §2, όπου, ωστόσο, επαναλαμβάνονται τα οριζόμενα στην §2 του άρθρου 370^{Β} ΠΚ, πλην όμως, με διαφορετικό πλαίσιο ποινής.[134]

ii) Παρακώλυση λειτουργίας πληροφοριακών συστημάτων: άρθρα 292^{Β}-292^{Γ} ΠΚ

Στο άρθρο 292^{Β} ΠΚ ενσωματώθηκε το άρθρο 4 της Οδηγίας 2013/40/Ε και ποινικοποιούνται οι επιθέσεις άρνησης εξυπηρέτησης τύπου DDoS και οι πράξεις παράνομης πρόσβασης τύπου hacking στις περιπτώσεις κατά τις οποίες η άνευ δικαιώματος παρεμπόδιση ή διακοπής της λειτουργίας του πληροφοριακού συστήματος δύναται να χαρακτηριστεί σοβαρή. Υπό το Νέο Ποινικό Κώδικα επέρχεται αυστηροποίηση του πλαισίου ποινής, καταργούμενου αφενός του κατ' έγκληση χαρακτήρα (§4 ως ίσχυε), υπό τη σκέψη ότι πρόκειται για διάταξη που αφορά ευρύτερο αριθμό ανθρώπων και πρέπει να διώκεται αυτεπαγγέλτως, και αφετέρου, αυξανόμενης της επαπειλούμενης ποινής για τους δράστες. Ειδικότερα, υπό το προϊσχύσαν καθεστώς προβλεπόταν ποινή έως 3 έτη, ενώ υπό το ισχύον καθεστώς η ποινή μπορεί να φτάσει έως 5 έτη, καθώς επίσης, προβλέπεται σωρευτικά επιβολή χρηματικής ποινής (§1). Στη δε §2 του άρθρου, στο πλαίσιο της προσπάθειας τήρησης της αρχής της αναλογικότητας

[132] Υπό το προισχύσαν νομικό πλαίσιο με τη διάταξη του άρθρου 370^{Ε} ΠΚ τιμωρούνταν οι προπαρασκευαστικές πράξεις.

[133] Η κοινωφελής εργασία προβλέπεται πλέον ως αυτοτελής ποινική κύρωση για μικρής βαρύτητας εγκλήματα (50 ΠΚ).

[134] Άξιο λόγου, όπως έχει παρατηρήσει ο Χρίστος Χ. Μυλωνόπουλος σε σχολιασμό του για το νέο Ποινικό Κώδικα, είναι ότι η διάταξη της §2 του άρθρου 370^{Δ} ΠΚ είναι όμοια με τη διάταξη της §1 του άρθρου 370^{Β} ΠΚ, πλην όμως, στην πρώτη περίπτωση απειλείται φυλάκιση έως 2 έτη ή χρηματική ποινή, ενώ στη δεύτερη περίπτωση η φυλάκιση μπορεί να ανέλθει σε έως 5 έτη.
Διαθέσιμο εδώ: https://www.kathimerini.gr/politics/1039677/christos-ch-mylonopoylos-meizona-provlimata-toy-neoy-poinikoy-kodika/

βάσει του είδους και της ένταση της προσβολής προβλέπονται αυστηρότερες ποινές, οι οποίες υπό την ισχύουσα νομοθεσία σχεδόν διπλασιάζονται ανάλογα με την υποπερίπτωση στην οποία υπάγεται η αξιόποινη συμπεριφορά.[135] Καίριας σημασίας είναι η περίπτωση της §2γ που αφορά στην παρέμβαση ή διακοπή της λειτουργίας συστημάτων πληροφοριών που αφορούν σε αγαθά ή υπηρεσίες ζωτικής σημασίας[136] η προστασία των οποίων κρίθηκε ότι έπρεπε όπως ενισχυθεί σημαντικά. Στο πλαίσιο αυτό η επαπειλούμενη ποινή ανέρχεται σε τουλάχιστον 3 έτη φυλάκισης[137] και χρηματική ποινή. Το άρθρο 292^{Γ} ΠΚ τιμωρεί τις προπαρασκευαστικές πράξεις για την τέλεση του ως άνω εγκλήματος.

iii) Παράνομη παρεμβολή σε δεδομένα κατ' άρθρον 381^{Α} ως ίσχυε

Το άρθρο 381^{Α} ΠΚ με τίτλο «φθορά ψηφιακών δεδομένων» όπως ενσωματώθηκε στην ελληνική έννομη τάξη με το Ν. 4411/16 αποτέλεσε μεταφορά του άρθρου 4 της Σύμβασης και του άρθρου 5 της Οδηγίας στο πλαίσιο της ποινικοποίησης της εκ προθέσεως και άνευ δικαιώματος πρόκλησης βλάβης, διαγραφής, καταστροφής, μεταβολής ή απόκρυψης των δεδομένων υπολογιστή προκειμένου η αυτοτελής προστασία των ψηφιακών δεδομένων να καταστεί δυνατή και ανάλογη με αυτή που απολαμβάνουν τα ενσώματα αντικείμενα (Δαλακούρας 2018: 170). Υπό το προ της θέσεως σε ισχύ του Ν. 4411/16 καθεστώς τα ψηφιακά δεδομένα μη ιδωμένα ως πράγμα ώστε να εμπίπτουν στο πραγματικό του άρθρου 381 ΠΚ περί φθοράς ξένης ιδιοκτησίας, παρέμεναν απροστάτευτα, ενώ η παρεχόμενη εκ περιτροπής προστασία αφορούσε αποκλειστικά και μόνο στον υλικό φορέα που πληττόταν, κενό που ενώ καλύφθηκε στον προϊσχύσαντα ΠΚ (Κιούπης 1999: 140) αξιοπερίεργα και όλως αδικαιολόγητα δημιουργείται εκ νέου με την κατάργηση του σχετικού άρθρου.

[135] Σύμφωνα με το άρ. 9 §5 της Οδηγίας επιβαρυντική περίσταση συνιστά η τέλεση του αδικήματος δια της υφαρπαγής δεδομένων (identity theft) προσωπικού χαρακτήρα άλλου ατόμου που στοχεύει στη δημιουργία εμπιστοσύνης με σκοπό την πρόκληση περιουσιακής ζημίας στον νόμιμο κάτοχο της ταυτότητας, ωστόσο, δεν ενσωματώθηκε στην ελληνική έννομη τάξη.

[136] Πρόκειται για την κριτική υποδομή της χώρας που αφορά σε υπηρεσίες απαραίτητες σε μία χώρα, όπως η υγεία, η ΔΕΗ, οι συγκοινωνίες, οι μεταφορές, η εθνική άμυνα κ.α. που αν διακοπεί η λειτουργία τους η χώρα βυθίζεται στο σκοτάδι. Τέτοιες ενέργειες δε, συνήθως σηματοδοτούν κυβερνοπόλεμο. Η εκ του πληροφοριακού πολέμου απειλή έχει εκτιμηθεί από τις ΗΠΑ και το ΝΑΤΟ και έχει αξιολογηθεί ως απειλή του συνόλου του κρατικού μηχανισμού, ενώ ένας εκ των τρόπων αντιμετώπισης αποτελεί η προσπάθεια απορρόφησης των κυβερνοεγκληματιών από τις Ειδικές Δυνάμεις των ΗΠΑ.

[137] Υπό το πρίσμα του προηγούμενου ΠΚ προβλεπόταν ποινή φυλάκισης τουλάχιστον 1 έτους.

2.5.3 Εγκλήματα σχετικά με υπολογιστές

i) Απάτη με υπολογιστή: άρθρο 386^{A} ΠΚ

Στο άρθρο 386^{A} προβλέπεται το αδίκημα της απάτης με υπολογιστή που προστέθηκε αρχικώς με το άρθρο 5 του Ν. 1805/1988 προκειμένου να καλυφθεί το κενό της ποινικής νομοθεσίας που είχε διαπιστωθεί στις περιπτώσεις που η περιουσιακή βλάβη λάμβανε χώρα ευθέως με κατάχρηση ενός συστήματος ηλεκτρονικής επεξεργασίας δεδομένων χωρίς την παραπλάνηση φυσικού προσώπου.[138] Στην αρχική διατύπωση του άρθρου τιμωρείτο «όποιος με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο».[139] Η δε διατύπωση με «οποιονδήποτε άλλο τρόπο» ήταν σκοπίμως ευρεία ώστε να περιλαμβάνει όλες εκείνες τις περιπτώσεις κατά τις οποίες ο δράστης επηρεάζει τα στοιχεία του υπολογιστή υπό την έννοια ότι το αποτέλεσμα της επεξεργασίας δεδομένων που επιτεύχθηκε με την μεσολάβηση της χωρίς δικαίωμα επεξεργασίας αυτών αποκλίνει από εκείνο που προσδοκάτο με την κανονική και σύννομη χρήση του.[140] Υπό τη θέση σε ισχύ του Ν. 4411/16, απαλείφθηκε η διατύπωση «με οποινδήποτε τρόπο» και προστέθηκαν οι συμπεριφορές της χωρίς δικαίωμα χρήσης ψηφιακών δεδομένων και της χωρίς δικαίωμα παρέμβασης σε πληροφοριακό σύστημα (13 η΄ και θ΄ του ΠΚ).[141] Σύμφωνα δε με την αιτιολογική έκθεση του Ν. 4411/16, «με τη νέα διάταξη περιλαμβάνεται πλέον ρητά στις περιπτώσεις απάτης με υπολογιστή και η χρήση (ορθών) δεδομένων που γίνεται χωρίς δικαίωμα, όπως π.χ. στην περίπτωση του δράστη που έχει αποκτήσει παράνομα το όνομα χρήστη και τον κωδικό χρήστη του δικαιούχου», ώστε, δυνάμει αυτού, προκύπτει ότι οποιαδήποτε μεταφορά χρημάτων λαμβάνει χώρα με υποκλοπή και χρήση ξένων (ορθών) κωδικών ή με παράνομη

[138] Ως εκ τούτου η εφαρμογή του άρθρου 386 ΠΚ θα αποτελούσε ανεπίτρεπτη αναλογία (Μυλωνόπουλος 2006: 597-597).
[139] Βασικό χαρακτηριστικό της διάταξης είναι η ομοιότητά της με την απάτη του άρθρου 386 ΠΚ. Προστατευόμενο έννομο αγαθό είναι η προστασία της περιουσίας ως συνόλου.
[140] Βλ. Μυλωνόπουλος 2006: 601 και παραπομπή σε BGHSt, 38, 121, ΠΧ ΜΒ/468 (απόδοση Α. Τζαννετή).
[141] Η έννοια της χωρίς δικαίωμα χρήσης ορθών δεδομένων προϋπήρχε στο άρθρο 263a του Γερμανικού Ποινικού Κώδικα.

διείσδυση του δράστη στα πληροφοριακά συστήματα Τραπεζών ή χρηματιστηριακών εταιρειών συνιστά απάτη με υπολογιστή κατ' άρθρον 386^{A} ΠΚ (Δαλακούρας 2018: 170). Στην παρούσα μορφή του άρθρου 386^{A} ΠΚ, μετά τις τελευταίες τροποποιήσεις, προστίθενται επιπλέον οι συμπεριφορές της χωρίς δικαίωμα εισαγωγής, αλλοίωσης, διαγραφής ή εξάλειψης δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας και της χωρίς δικαίωμα αξιοποίησης λογισμικού προορισμένου για τη μετακίνηση χρημάτων, στο πλαίσιο του εκσυγχρονισμού των νομοθετικών προβλέψεων προκειμένου να συμπεριληφθούν οι νέες προεκτάσεις της απάτης. Ως προς την υποκειμενική υπόσταση του αδικήματος πρόκειται για έγκλημα σκοπού και ιδίως για την θεμελίωση του κατ' αρχήν αδίκου απαιτείται ο σκοπός του δράστη[142] να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος. Υπό τις τελευταίες τροποποιήσεις το ποινικό πλαίσιο αυστηροποιείται προστιθέμενης της υποχρέωσης επιβολής χρηματική ποινής σωρευτικά με την ποινή φυλάκισης υπό τις ειδικότερες προϋποθέσεις του άρθρου.

2.5.4 Εγκλήματα σχετικά με το περιεχόμενο

i) Πορνογραφία και πορνογραφικές παραστάσεις ανηλίκων: άρθρα 348^{A}-348^{Γ} ΠΚ

Το άρθρο 9 του 3^{ου} κεφαλαίου της Σύμβασης της Βουδαπέστης καλύπτει τις απειλές που σχετίζονται με την παράνομη παραγωγή, κατοχή ή διανομή υλικού παιδικής πορνογραφίας ως ένα από τα πιο επικίνδυνα ηλεκτρονικά εγκλήματα,[143] ως εκ της ανωνυμίας που προσφέρει το Internet και των παιδιών που συνήθως επιζητούν προσοχή ή δεν έχουν αναπτυγμένες κοινωνικές ικανότητες με αποτέλεσμα να αποτελούν εύκολη βορά των παιδόφιλων. Τα σχετικά με τη γενετήσια ζωή αδικήματα εκσυγχρονίστηκαν για πρώτη φορά με το Ν. 3062/2002 ενώ έως το 2007,[144] τιμωρούνταν μόνο αυτός που

[142] Άμεσος δόλος α΄ βαθμού ως προς το περιουσιακό όφελος ενώ ως προς τα λοιπά πραγματικά περιστατικά που θεμελιώνουν το παράνομο αρκεί ενδεχόμενος δόλος.
[143] Σκέψη 36 της Αιτιολογικής Έκθεσης της Σύμβασης. Επισημαίνεται ότι η παιδική πορνογραφία έρχεται τρίτη σε ετήσιο τζίρο μετά το εμπόριο ναρκωτικών και όπλων με ετήσια κέρδη που ξεπερνούν τα 3 δισ., ενώ παρατηρείται το φαινόμενο, επιχειρηματίες που δεν έχουν καμία σχέση με την παιδική πορνογραφία να επενδύουν σε αυτή προκειμένου να εισπράξουν μερίσματα (επιχείρηση 'Storm', επιχείρηση'Purity, Σφακιανάκης 2016: 87).
[144] Κύρωση του προαιρετικού Πρωτοκόλλου της Σύμβασης για τα Δικαιώματα του Παιδιού σχετικά με την εμπορία παιδιών, την πορνεία και την παιδική πορνογραφία με τον Ν. 3625/2007.

κερδοσκοπούσε διακινώντας υλικό παιδικής πορνογραφίας, ώστε υπήρχε διάκριση σε δύο είδη παιδόφιλων, τον «καλό» που κατείχε το υλικό χωρίς να κερδοσκοπεί από αυτό, και τον «κακό» που κερδοσκοπούσε από αυτό (Σφακιανάκης: 35-36). Έκτοτε, το νομοθετικό πλαίσιο άλλαξε για να περιλάβει και τις δύο κατηγορίες (Δαλακούρας 2018: 15-16). Γενική στόχευση της Σύμβασης αποτέλεσε η ενίσχυση των μέτρων προστασίας της παιδικής ηλικίας μέσω της συστηματικής οριοθέτησης της χρήσης συστημάτων ηλεκτρονικών υπολογιστών και της αποτελεσματικής αποτροπής διάπραξης σεξουαλικών εγκλημάτων σε βάρος των παιδιών.[145] Έννομο αγαθό αποτελεί η ανηλικότητα που αξιώνει προστασίας από συμπεριφορές που τη διαφθείρουν. Κομβικό σημείο συνιστά η εξίσωση της συμβατικής με την εικονική πορνογραφία. Επισημαίνεται επίσης η αναγκαιότητα συσταλτικής ερμηνείας στην έννοια της κατοχής, ώστε να προϋποτίθεται αποθήκευση σε σκληρό δίσκο και όχι απλή θέαση, ενώ για το αιτιολογημένο της κρίσης οφείλει όπως προσδιορίζεται το επιλήψιμο του αρχείου.[146] Με τη διάταξη του άρθρου 348^{A} ΝΠΚ («πορνογραφία ανηλίκων») τιμωρείται όποιος παράγει ή εισάγει, διανέμει ή πωλεί κλπ υλικό παιδικής πορνογραφίας ενώ η ποινή αυξάνεται όταν η πράξη τελείται μέσω Διαδικτύου. Με το άρθρο 348^{B} ΝΠΚ («προσέλκυση παιδιών για γενετήσιους λόγους») τιμωρείται όποιος με πρόθεση, μέσω πληροφοριακών συστημάτων, προτείνει σε ανήλικο που δε συμπλήρωσε τα 15 έτη να συναντήσει τον ίδιο ή τρίτο με σκοπό τη διάπραξη του αδικήματος του άρθρου 348^{A} ΝΠΚ, όταν της πρότασης ακολουθούν περαιτέρω πράξεις που οδηγούν σε μια τέτοια συνάντηση, με φυλάκιση τουλάχιστον 2 ετών και χρηματική ποινή. Στη διάταξη του άρθρου 348^{Γ} ΝΠΚ («πορνογραφικές παραστάσεις ανηλίκων»), στη διαμόρφωση της οποίας έχουν συνυπολογιστεί οι προβλέψεις της Πρότασης Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την καταπολέμηση της σεξουαλικής κακοποίησης, της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας,[147]τιμωρείται σε βαθμό κακουργήματος όποιος εξωθεί ή παρασύρει ανήλικο σε πορνογραφικές παραστάσεις ή διοργανώνει αυτές (§1).

[145] Πρόσθετο Πρωτόκολλο της Σύμβασης του ΟΗΕ για τα δικαιώματα του παιδιού, Διεθνής Διάσκεψη για την καταπολέμηση της Παιδικής Πορνογραφίας στο Διαδίκτυο του 1999, Απόφαση-Πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου της 22ας.13.2003 για την καταπολέμηση της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας σε ΕΕΕΕ L 13/44, 20.1.2004.
[146] ΑΠ92/2017, ΠοινΧρ 2018, ΑΠ 1648/2016, ΑΠ 1517/2016.
[147] Κατήργησε την απόφαση-πλαίσιο 2004/68/ΔΕΥ.

2.5.5 Παρατηρήσεις

Η νομοθεσία αποτελεί αναμφίβολα τον ακρογωνιαίο λίθο στην αντιμετώπιση του εγκλήματος. Η ύπαρξη κατάλληλων να επιτύχουν το σκοπό αυτό νόμων είναι απαραίτητη σε επίπεδο καταστολής και πρόληψης εγκληματικών συμπεριφορών, οι οποίες, εν τη απουσία ισχυρού νομοθετικού πλαισίου, πολλαπλασιάζονται, απορρέουσες από την ανθρώπινη φύση. Κατά τη διατύπωση του Hobbes ο άνθρωπος είναι ένα εγωιστικό ον με μοναδικό του σκοπό το ατομικό του καλό και οτιδήποτε εξυπηρετεί αυτό ακόμη κι αν αυτό προϋποθέτει βλάβη των συμφερόντων τρίτων. Υπό το φόβο αυτής της παραδοχής δημιουργήθηκε το κράτος και το κράτος δημιούργησε το νόμο για να οριοθετήσει τους αναγκαίους περιορισμούς της ελευθερίας (Tatarkiewicz 2001: 68). Συνδυαζόμενης της σκέψης αυτής με την παρατήρηση του Mill ότι ο νόμος στοχεύει στην εγγύηση ότι η ελευθερία ενός ατόμου δε θα παραβιαστεί από τη δράση ενός άλλου ατόμου, επιβεβαιώνεται η αναγκαιότητα της παρουσίας του Ποινικού Δικαίου σε όλες τις εκφάνσεις της παρεκκλίνουσας δράσης. Αντιστοίχως, τα αυτά διαλαμβάνονται στο χώρο του Διαδικτύου, όπου η δημιουργία κατάλληλου νομοθετικού πλαισίου οφείλει να είναι μια δυναμική διαδικασία (deliberation forcing) (Meares, Katyal & Kahan 2004: 1171). Σημαντικός, στο πλαίσιο αυτό, είναι ο ακριβής καθορισμός των δραστηριοτήτων που το Δίκαιο αντιμετωπίζει ως αποδοκιμαζόμενες από την έννομη τάξη. Οι Κανόνες Δικαίου δεν πρέπει να περιβάλλονται από ασάφεια και αοριστία, αλλά πρέπει να είναι ακριβείς και συγκεκριμένοι προκειμένου να είναι ικανοί να επιτύχουν τον σκοπό τους και να ανταποκριθούν ευχερώς στις αναδεικνυόμενες απειλές.

Η ταχύτητα στην εξέλιξη της τεχνολογίας, ωστόσο, και η διαρκής εμφάνιση νέων απειλών καθιστούν προκριτέα τη χρήση τεχνολογικά ουδέτερης γλώσσας προς αποφυγή του ενδεχομένου να καταστεί η νομοθεσία απαρχαιωμένη, όπως επιχειρεί η Σύμβαση της Βουδαπέστης. Περαιτέρω, απαραίτητος τυγχάνει ο εκσυγχρονισμός των ποινικών νομοθεσιών, προκρινόμενου ενός συνδυασμού προσαρμογής της υπάρχουσας νομοθεσίας, απεκδυόμενης αυτής από στενές ερμηνευτικές προσεγγίσεις του παρελθόντος,[148] και νέων νομοθετικών προβλέψεων. Η ουσιαστική εναρμόνιση των εθνικών ποινικών νομοθεσιών και η προώθηση της αποτελεσματικής συνεργασίας

[148] Χαρακτηριστική είναι η διατύπωση του Ανδρουλάκη (1995: 682, 686) περί «απελευθέρωσης του ποινικού Δικαίου από την αστικολογική σκέψη, σε σχέση ιδίως με την υπεξαίρεση λογιστικού χρήματος» αναφερόμενος στις έννοιες του πράγματος και της κατοχής (ΟλΑΠ 1093/1991).

απαιτούν δράση σε πλείονα επίπεδα. Στην κατεύθυνση αυτή η Σύμβαση της Βουδαπέστης ως το κύριο διεθνές νομοθετικό κείμενο επιδιώκει την εναρμόνιση του Ουσιαστικού και Δικονομικού Ποινικού Δικαίου των συμβαλλόμενων κρατών και την αμοιβαία συνεργασία. Παρόλα αυτά, πολλά κράτη εξακολουθούν να μην έχουν θεσπίσει σχετικές διατάξεις για το ηλεκτρονικό έγκλημα με αποτέλεσμα την ατιμωρησία των δραστών.[149] Μολονότι τα τελευταία χρόνια έχουν γίνει σημαντικά βήματα, ο δρόμος προς μια πραγματική εναρμόνιση εννοιών και διαδικασιών σε διεθνές επίπεδο είναι ακόμη μακρύς, πόσο μάλλον που η νομοθεσία είναι καταδικασμένη να βρίσκεται πάντοτε ένα βήμα πίσω από τις τεχνολογικές εξελίξεις.

[149] Ο δράστης του 'I Love You' virus δεν τιμωρήθηκε ποτέ εξαιτίας της απουσίας σχετικών νομοθετικών διατάξεων στις Φιλιππίνες.

ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ

ΤΑ ΕΡΓΑΛΕΙΑ ΤΗΣ ΟΙΚΟΝΟΜΙΚΗΣ ΑΝΑΛΥΣΗΣ ΤΟΥ ΔΙΚΑΙΟΥ ΩΣ ΜΕΣΟ ΠΕΡΙΣΤΟΛΗΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

3.1 Εισαγωγικές Παρατηρήσεις

Στο προηγούμενο κεφάλαιο, έγινε προσπάθεια καταγραφής σημαντικών νομοθετικών προβλέψεων που αποσκοπούν στην καταστολή των επιμέρους μορφών του ηλεκτρονικού εγκλήματος ως κοινωνικού προβλήματος μέσα από τον ποινικό κολασμό των δραστών, πληρουμένης της νομοτυπικής υπόστασης του εγκλήματος.[150] Διερευνώντας, περαιτέρω, τον σκοπό της ποινής, όπως πρεσβεύουν οι απόλυτες θεωρίες, αυτός εντοπίζεται στον ανταποδοτικό χαρακτήρα, αδιάφορης της κοινωνικοπροληπτικής διάστασης, με τους υποστηρικτές της νεοκλασικής σχολής να εστιάζουν στην αναλογία σε σχέση με το άδικο της πράξης και την εξατομικευμένη ενοχή του δράστη ('punishement appropriate to the backround of the offender') (Grabosky 2016: 114, Μανωλεδάκης & Παρασκευόπουλος 1999: 176). Οι σχετικές θεωρίες εστιάζουν στην προστασία της κοινωνικής ειρήνης αντιμετωπίζοντας την ποινή ως μέσο πρόληψης (Jescheck 1978: 55), ως αντίδρασης στις προσβολές των εννόμων αγαθών, που θα έπρεπε να στοχεύει στην εξουδετέρωση του δράστη, μερική ή ολική, στην επαναφορά της κοινωνικής ειρήνης και της ισορροπίας στη συνείδηση των κοινωνών και στην προσπάθεια αποτροπής νέων προσβολών στο μέλλον (Μανωλεδάκης & Παρασκευόπουλος 1999: 2). Αυτό επιτάσσει η προληπτική λειτουργία του Ποινικού Δικαίου, στην οποία υπάγονται γενικο-προληπτικοί και ειδικο-προληπτικοί σκοποί. Κατά μία άποψη, η προσφυγή στην ποινική καταστολή πρέπει να συνιστά το ultimum refugium της εννόμου τάξεως (Χωραφάς), πολλώ δε μάλλον, που στην πράξη σε μεγάλο μέρος η προσοχή στρέφεται στον τιμωρητικό σκοπό του Ποινικού Δικαίου, συνοδευόμενου από μια επίφαση γενικο-προληπτικής λειτουργίας[151]. Στο πλαίσιο αυτό και υπό τη σκέψη ότι, σύμφωνα με τη γενική αρχή της αναλογικότητας (proportionality), τα ηπιότερα μέσα της έννομης τάξης που σκοπούν στη διασφάλιση των εννόμων αγαθών, οφείλουν όπως προηγούνται της ποινικοποίησης μιας συγκεκριμένης συμπεριφοράς μέσω των θεσμών

[150]Αυτό προϋποθέτει ότι για να επιβληθεί η ποινή πρέπει να διαπιστωθεί πράξη άδικη και καταλογιστή (Μανωλεδάκης & Παρασκευόπουλος 1999: 173).

[151] Οι σκοποί της ποινής μπορούν να είναι πολλοί και αρκετές φορές αντικρουόμενοι. Μεταξύ άλλων περιλαμβάνουν την αποτροπή, την επανένταξη του δράστη, την καταγγελία του εγκλήματος, τη τιμωρία, την αποδυνάμωση του δράστη, την αποκατάσταση ή αποζημίωση του θύματος (Grabosky 2016: 112).

του Ποινικού Δικαίου,[152] σκόπιμη είναι, κατά τη γνώμη της γράφουσας, η εξέταση μεθοδολογικών εργαλείων που θα εστιάζουν στο κοινωνικά βέλτιστο (social optimum) και θα συνεπικουρούν την προληπτική λειτουργία του Ποινικού Δικαίου στη βάση της αναζήτησης των κινήτρων που θεωρούνται πιο αποτελεσματικά για τη διαμόρφωση βέλτιστων συμπεριφορών στο μέλλον.[153]

3.2 Αναζητώντας τα κίνητρα των δραστών

Στο απαύγασμα των δυνατοτήτων του Διαδικτύου αναδείχθηκαν νέες μορφές εγκληματικών συμπεριφορών, οι οποίες, ωστόσο, δεν παύουν να ερείδονται στους ήδη γνωστούς προσδιοριστικούς παράγοντες της ανθρώπινης συμπεριφοράς. Φαινόμενα cyber-bullying για παράδειγμα ανάγονται σε πρόσωπα-θύτες με στρατηγικές τάσεις, συσσωρευμένο θυμό και χαμηλή συναισθηματική νοημοσύνη που στον πραγματικό κόσμο θα επιδίδονταν σε αντίστοιχες μορφές κατ' εξακολούθηση παρενόχλησης, με τη διαφορά ότι στις περιπτώσεις εκείνες θα γινόταν λόγος για bullying. Σε ό, τι αφορά επομένως στη μετάλλαξη των παραδοσιακών εγκλημάτων τα κίνητρα είναι ήδη γνωστά μέσα από τα παραδείγματα του πραγματικού κόσμου. Πιο σύνθετη, ωστόσο, εμφανίζεται η ανίχνευση των κινήτρων στο πεδίο των αμιγώς νέων μορφών, όπου όμοιες συμπεριφορές μεταξύ των δραστών απηχούν ανόμοιες κινητήριες δυνάμεις. Κατά συνέπεια, η πρόθεση διείσδυσης σε συστήματα πληροφοριών μπορεί να ανάγεται άλλοτε στην περιέργεια της ανθρώπινης φύσης που επιθυμεί να ερευνήσει το άγνωστο ('electronic voyeurism')[154] ή άλλοτε στη θεώρηση του Διαδικτύου ως χώρου που θα έπρεπε να είναι ανοιχτός προς όλους μέσα από την ελεύθερη πρόσβαση στα περιεχόμενά του (Stallman 1990: 25-26).

[152] «Η προστασία των εννόμων αγαθών δεν πραγματώνεται σε πρώτο βαθμό από τους θεσμούς του Ποινικού Δικαίου, αλλά από όλο το οικοδόμημα της έννομης τάξης και το Ποινικό Δίκαιο πρέπει να επεμβαίνει τελευταίο, κι αφού πρωτύτερα έχουν ενεργοποιηθεί και έχουν αποτύχει τα άλλα μέσα επίλυσης κοινωνικών προβλημάτων» (Roxin 1992: 17).

[153] Στόχο και τομέα του Ποινικού Δικαίου αποτελεί άλλωστε η 'de lege ferenda' έρευνα, συνώνυμη της «αντεγκληματικής πολτικής» που ερευνά τη διαμόρφωση του ορθού Ποινικού Δικαίου και την αποτελεσματική προστασία της έννομης τάξης.

[154] Χαρακτηριστική είναι η φράση του Mitnick, ενός από τους πιο διάσημους Αμερικανούς hackers: "Our favorite was the National Security Agency computer because it was supposed to be so confidential. It was like a big playground once you got into it."
Διαθέσιμη εδώ: https://apnews.com/article/b83c6ccc6411f742195296ef7937cc59

Μια πρώτη γενική κατηγοριοποίηση των δραστών του κυβερνοεγκλήματος με αφετηρία τις έρευνες που εμφανίζουν ως σημαντική απειλή τους δυσαρεστημένους εργαζομένους εταιρειών και επιχειρήσεων,[155] διακρίνει ανάμεσα α) σε αυτούς που δρουν από τα έσω (insiders), οι οποίοι διαπράττουν το έγκλημα υπερβαίνοντας εξουσιοδοτημένη πρόσβαση,[156] και β) σε αυτούς που δρουν από έξω (outsiders), οι οποίοι αποκτούν και εκμεταλλεύονται μη εξουσιοδοτημένη πρόσβαση. Σύμφωνα με μια εύστοχη παρατήρηση, η διαφορά μεταξύ των δύο έγκειται στο ότι ο πρώτος δράστης θα αφήσει ίχνη, παρεκτός αν είναι πολύ καλός, ενώ ο δεύτερος όχι, παρεκτός αν είναι πολύ κακός (Shackelford 1992: 482-483).

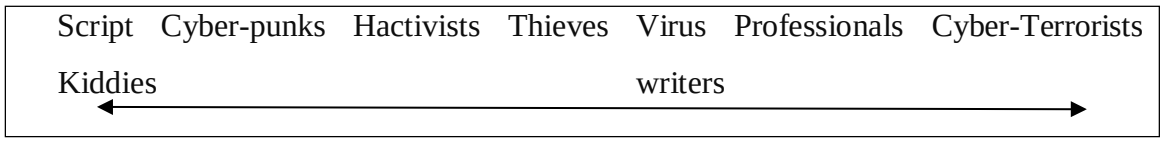
Άλλη ταξινόμηση που αφορά στις τεχνικές ικανότητες των δραστών διακρίνει ανάμεσα σε 'sophisticated' και 'recreational' hackers. Η έννοια του 'sophisticated' αναπτύχθηκε με την πάροδο των χρόνων για να περιγράψει τις πιο σύνθετες μεθόδους που επιστράτευαν δράστες με εξειδικευμένες γνώσεις σε σχέση με τους πρώιμους δράστες που χρησιμοποιούσαν πιο απλές μεθόδους. Στον αντίποδα, ο όρος 'recreational' που χαρακτηρίζει αρκετά σύγχρονα παραδείγματα δραστών, απευθύνεται σε όσους δε διαθέτουν τις εξειδικευμένες γνώσεις που εντοπίζονται στους πρώτους, αλλά προσφεύγουν σε διαθέσιμα εργαλεία και τεχνικές που κυκλοφορούν στο Διαδίκτυο, πολλά εκ των οποίων είναι προσβάσιμα στο ευρύ κοινό.

Από κοινωνιολογική σκοπιά οι δράστες μπορούν να υπαχθούν σε πέντε κατηγορίες: 1) άτομα που διαπράττουν τέτοιες ενέργειες για λόγους διασκέδασης ή προσωπικής ικανοποίησης, 2) άτομα που υποκινούνται από το υλικό όφελος, 3) άτομα που ενεργούν για ιδεολογικούς σκοπούς, 4) πνευματικά άρρωστα άτομα και 5) επαγγελματίες εγκληματίες. Η κοινή συνισταμένη είναι ίδια και εντοπίζεται στη βλαπτική ενέργεια στην οποία σκοπίμως οδηγήθηκαν για να επιτύχουν το στόχο τους (Simundic, Brbaric & Franjic 2016: 168).

[155] Σύμφωνα με έρευνα της δικηγορικής εταιρείας Michael G. Kessler & Associates Ltd του 1999 τη μεγαλύτερη απειλή αποτελούσαν οι δυσαρεστημένοι εργαζόμενοι, κάτι που επιβεβαιώνουν οι αναφορές του FBI. Αξίζει να αναφερθεί η περίπτωση υπεξαίρεσης 21,3 εκατ. σε συνεργαζόμενη με την εταιρεία Wells Fargo Τράπεζα που διαπράχθηκε από υπάλληλο της Τράπεζας (ACLR 1986: 409).

[156] Σύμφωνα με έρευνα του Harvard Business Review τα τέσσερα από τα πέντε στελέχη εταιρειών θεωρούν τις πρακτικές των εταιρειών τους ως ανήθικες και τα τέσσερα από τα επτά ότι η συμπεριφορά άλλων στελεχών θα παραβίαζε τους ηθικούς κώδικες αν ήξεραν ότι δεν θα αποκαλυφτούν.

Μια ακόμη πιο αναλυτική κατηγοριοποίηση που εστιάζει στα κίνητρα και αφορά στις συνηθέστερες κατηγορίες δραστών διαβαθμίζει την εγκληματική συμπεριφορά από πλευράς τεχνικής γνώσης, κινήτρου και ηθικής ανάπτυξης σε επτά κατηγορίες (Rogers 2006: 97-102, σε Ghosh & Turrini 2010: 218-223):



1) Script Kiddies: Άτομα με περιορισμένη τεχνική γνώση, ανώριμα συνειδησιακά και ηθικά, που δε συνειδητοποιούν τις πιθανές συνέπειες της πράξης τους. Υποκινούνται από ενθουσιασμό και διάθεση να ξεχωρίσουν στο σύνολο, γι' αυτό και αποτελούν εύκολα εντοπίσιμη κατηγορία. Ευθύνονται για την πλειοψηφία των εγκλημάτων του κυβερνοχώρου (Kesan & Hayes 2015: 440).
2) Cyber-punks: Διακατέχονται από αντίδραση προς τις κοινωνικές νόρμες και τάση για δημόσια αναγνώριση. Παρότι συνειδητοποιούν τις συνέπειες, το μη αναπτυγμένο αίσθημα κοινωνικής ευθύνης υποκινεί τη δράση τους. Η σκέψη της τιμωρίας δε συνιστά αποτρεπτικό παράγοντα, καθώς πιστεύουν ότι ενδεχόμενη σύλληψη θα τους μετατρέψει σε ήρωες.
3) Hacktivists (Political Activists): Μοιραζόμενοι κοινά στοιχεία με άλλες κατηγορίες, αιτιολογούν τις ενέργειές τους με όρους πολιτικής και ηθικής ορθότητας. Κύριο κίνητρό τους είναι η πολιτική αντίσταση και δευτερευόντως η εκδίκηση, η δύναμη, η απληστία, η διαφήμιση και η προσοχή των ΜΜΕ.[157]
4) Thieves: Κοινοί εγκληματίες που κινητοποιούνται από το υλικό όφελος. Συνήθως δε διαθέτουν εξειδικευμένες γνώσεις και ελκύονται από αριθμούς καρτών και λογαριασμών. Στις συνήθεις δράσεις τους συγκαταλέγεται η κλοπή ταυτότητας.
5) Virus writers: Αυτή η κατηγορία περιλαμβάνει τόσο άτομα με ειδικές γνώσεις όσο και άτομα της πρώτης κατηγορίας που ξεκινούν ως έφηβοι και εξελίσσονται χρονολογικά και συνειδησιακά. Ο βαθμός πνευματικής προσήλωσης στο έργο τους ποικίλλει, ενώ στοχεύουν στην προσοχή και την ωμή συγκίνηση χωρίς να αποτρέπονται από την τιμωρία.

[157] Πρόκειται για κατηγορία με αυξανόμενη δυναμική. Το 1999 δέχθηκαν επιθέσεις πολιτικού ακτιβισμού ταυτόχρονα οι ιστοσελίδες του Λευκού Οίκου, του Υπουργείου Εσωτερικών, της Greenpeace και της Γερουσίας.

6) Professionals: Αποτελούν την ελίτ των δραστών και διακρίνονται για την ανταγωνιστική τους ευφυΐα και εκπαίδευση. Συχνά αναμειγνύονται σε επιτηδευμένες απάτες και εταιρική κατασκοπεία πουλώντας πληροφορίες και προϊόντα πνευματικής ιδιοκτησίας στους σπουδαιότερους πλειοδότες. Θεωρούν τη δραστηριότητά τους εργασία και τον εαυτό τους επαγγελματία.[158]
7) Cyber-terrorists: Ιδωμένοι ως στρατιώτες ή πολεμιστές της ελευθερίας χρησιμοποιούν τους υπολογιστές ως εργαλεία διακίνησης πληροφοριών. Στοχεύουν στην επίθεση για να ανακόψουν τη δράση του εχθρού και να επιτύχουν την προστασία του δικού τους κεκτημένου.

Η απαρίθμηση των προτεινόμενων κατηγοριοποιήσεων των δραστών δεν είναι εξαντλητική, αφορά, ωστόσο, στις κυριότερες, κατά τη γνώμη της γράφουσας, προσπάθειες ταξινόμησης των δραστών σε μοντέλα συμπεριφοράς. Οι κυριότερες στρατηγικές αντιμετώπισης του ηλεκτρονικού εγκλήματος, μέχρι στιγμής, εστιάζουν σε τεχνικές λύσεις, πλην όμως, αμελούν, σε μεγάλο βαθμό, τα αίτια της ανθρώπινης συμπεριφοράς. Κατά τη διατύπωση της Susan Brenner (2007: 783), οι κανόνες που συνοδεύουν την κακή χρήση της τεχνολογίας είναι ποινικοί κανόνες και οι ποινικοί κανόνες απευθύνονται σε ανθρώπους και όχι συσκευές. Η εύρεση, επομένως, αποτελεσματικών λύσεων προϋποθέτει προηγουμένως την κατανόηση του *ποιος* και του *γιατί* στην εγκληματική δραστηριότητα (Ghosh & Turrini 2010: 234-235).

3.3 Η συμβολή της οικονομικής ανάλυσης

Κοινή συνισταμένη της νομικής επιστήμης και των οικονομικών αποτελεί η τοποθέτηση κινήτρων στο κεντρικό τμήμα της ανάλυσής τους. Τα οικονομικά αποτελούν την κοινωνική επιστήμη που μελετά την ορθολογική επιλογή ('rational choice') και τη συμπεριφορά των ατόμων κατά την παραγωγή και κατανάλωση αγαθών που είναι πεπερασμένα. Στο πλαίσιο αυτό, η οικονομική ανάλυση καλείται να αποδείξει ότι τόσο τα μεμονωμένα άτομα όσο και το κράτος λειτουργούν ορθολογικά επιδιώκοντας τη μεγιστοποίηση της ωφελιμότητάς τους (utility) και τούτο, προϋποθέτοντας, ότι γνωρίζουν καλά τις προτιμήσεις τους και λειτουργούν ορθολογικά προκειμένου να τις

[158] Υπάγονται σε τρεις επιμέρους κατηγορίες: α) εκείνους που έχουν εγκληματική πρόθεση, β) εκείνους που επιδιώκουν να εξελίξουν τις δυνατότητές τους και γ) εκείνους που επιδιώκουν να εισβάλουν σε συστήματα για να βελτιώσουν τις αδυναμίες τους (Branscomb 1990: 28).

ικανοποιήσουν. Από την αρχή αυτή, απορρέει η παραδοχή ότι τα άτομα δεν πράττουν, παρεκτός αν το προσδοκώμενο όφελος από τη δράση τους υπερβαίνει το προσδοκώμενο κόστος, παραδοχή που διαπιστώνεται τόσο σε συνθήκες αγοράς όσο και στα ανθρώπινα περιβάλλοντα ως εξωτερικά της αγοράς (σιωπηρές αγορές). Βασική προϋπόθεση της αρχής της ορθολογικής μεγιστοποίησης ('rational maximization') συνιστά η αντίδραση των ορθολογικών δρώντων ('rational maximizers'), στους οποίους, στο πλαίσιο που ενδιαφέρει το νόμο, περιλαμβάνονται οι υποψήφιοι θιγόμενοι, δυνητικοί εγκληματίες, οι πιθανοί διάδικοι και τα υποψήφια θύματα, σε κίνητρα και νομικούς κανόνες που καθορίζουν τις επιλογές τους. Όταν η νομική κύρωση για μια ενέργεια αυξάνεται, η οποία σε συνθήκες αγοράς ισοδυναμεί με αύξηση της τιμής, διατηρουμένων των υπόλοιπων δεικτών αμετάβλητων και δοθέντος ότι η (σιωπηρή) αγορά αναπόφευκτα θα οδηγηθεί σε ισορροπία, οι δυνητικοί δράστες αποθαρρύνονται να εμπλακούν σε αυτή τη δραστηριότητα υπό την έννοια ότι «καταναλώνουν λιγότερο» (Fisher 2014: 38-41). Υπό το πρίσμα αυτό, η συμπεριφορά των ατόμων είναι προβλέψιμη. Βέβαια, η ίδια η κεντρική αφετηρία της ορθολογικής επιλογής ανατρέπεται από την πραγματικότητα στην οποία οι άνθρωποι υποφέρουν από γνωστικές προκαταλήψεις αποκλίνοντας από την ορθολογική συμπεριφορά, όπως για παράδειγμα όταν καταβάλλονται από υπερβολική αισιοδοξία κατά την αξιολόγηση των προοπτικών τους ή όταν από την άλλη, μένουν προσδεδεμένοι σε άγκυρες του παρελθόντος (McAdams & Ulen 2008: 4-5), εμφανίζοντας έτσι οριοθετημένη ορθολογικότητα, περιορισμένη δύναμη θέλησης και ιδιοτέλεια (Sunstein, Cash R., Christina Jolls & Richard H. Thaler 1998: 1477-1478). Στο πλαίσιο αυτό, εξετάζεται ο ρόλος πρόσθετων μηχανισμών που δύνανται να συμβάλουν στην οριοθέτηση της ανθρώπινης συμπεριφοράς με απώτερο σκοπό την ένταξή της σε ένα νομίμως αποδεκτό και κοινωνικά λειτουργικό πλαίσιο.

3.4.1 Η θεωρία του Gary Becker

Στη βάση της υπόθεσης ότι το έγκλημα αποτελεί κοινωνική επιλογή ('social choice'), ο Gary Becker (1968) ανέπτυξε ένα μοντέλο για την ορθή εκτίμηση και τον περιορισμό του κοινωνικού κόστους του εγκλήματος ('social cost'). Σύμφωνα με τον Becker η απόφαση της διάπραξης του εγκλήματος αποτελεί το προϊόν της στάθμισης κόστους και οφέλους, δύο παραγόντων που υποκινούν την εγκληματική στάση του δράστη υπό την προϋπόθεση ότι ο υποψήφιος δράστης συνιστά ένα ορθολογικά σκεπτόμενο ον που λειτουργεί με σκοπό την μεγιστοποίηση της ωφελιμότητάς του. Στο

πλαίσιο αυτό, η επιλογή τυγχάνει συνάρτηση των εσόδων που θα απορρεύσουν από την εγκληματογόνο δράση, της πιθανότητας σύλληψης, της σοβαρότητας και του είδους της τιμωρίας. Με μια μαθηματική αποτύπωση, η σχέση ανάμεσα στο προσδοκώμενο όφελος (b) που περιλαμβάνει όλα τα υλικά και άυλα οφέλη της εγκληματικής πράξης, της σοβαρότητας της ποινής (c) και της πιθανότητας επιβολής (p) προκύπτει από τη σχέση (b - pc) > 0. Η εγκληματική δραστηριότητα αυξάνει όσο αυξάνει το b και μειώνεται όσο αυξάνονται το p και το c, δηλαδή όσο ενισχύεται η τιμωρία είτε, άλλως, όσο μειώνονται τα προσδοκώμενα οφέλη. Διαπιστώνει δε, ότι η εγκληματική δραστηριότητα προκαλεί κοινωνικά κόστη, στα οποία περιλαμβάνεται η προκαλούμενη βλάβη στην κοινωνία, το κόστος της σύλληψης και καταδίκης και το κόστος της τιμωρίας.

Σκοπός του Becker είναι η ελαχιστοποίηση του παραγόμενου κοινωνικού κόστους που καταλήγει να επιβαρύνει τα θύματα και το νομικό σύστημα αποσταθεροποιώντας την οικονομία μέσω της ανάδειξης ενός κοινωνικού σχεδιασμού ικανού να μειώσει την εγκληματικότητα (Fisher 2014: 45-47). Εισάγεται ακόμη η ιδέα ότι οι προσπάθειες σύλληψης και καταδίκης αποτελούν υποκατάστατα (substitutes) της επιβολής του νόμου, ώστε η μείωση του κοινωνικού κόστους μπορεί να επέλθει με την αύξηση της επιβαλλόμενης ποινής είτε πρόκειται για επιβολή υψηλότερων χρηματικών προστίμων είτε για αύξηση του χρόνου φυλάκισης. Εξετάζοντας περαιτέρω την ενίσχυση των κοινωνικών εσόδων ως τρόπο αντιστάθμισης του κοινωνικού κόστους και αποφυγής της οικονομικής αποσταθεροποίησης, ο Becker προτείνει τη δημιουργία ενός μοντέλου εστιαζόμενου στις χρηματικές ποινές λαμβάνοντας αυτές ως πιο αποτελεσματικές και λιγότερο δαπανηρές. Υπό αυτή τη σκέψη, η επιβολή χρηματικών προστίμων έναντι της στερητικής της ελευθερίας ποινής που επιφέρει πρόσθετο κόστος για την κοινωνία, εμφανίζεται περισσότερο αποτελεσματική.[159] Τούτο περιλαμβανομένου του κόστους συντήρησης των καταστημάτων κράτησης και περίθαλψης των κρατουμένων και επιπλέον του υπαρκτού κινδύνου δημιουργίας εγκληματικών δικτύων μέσω της ανταλλαγής τεχνογνωσίας των δραστών στους χώρους κράτησης, ώστε τελικώς το

[159] Ο Becker εστιάζει τη βασική οικονομική θεωρία του στην αλληλεπίδραση μεταξύ ατόμου και επιβολής του νόμου υποστηρίζοντας ότι οι άνθρωποι προβαίνουν σε εγκληματική δραστηριότητα όχι εξαιτίας διαφορετικών κινήτρων από αυτά που εντοπίζονται στους νομοταγείς πολίτες αλλά λόγω της διαφορετικής στάθμισης κόστους-οφέλους. Υποστηρίζει ότι το νομοθετικό πλαίσιο πρέπει να είναι διαρθρωμένο με τρόπο ώστε να ελαχιστοποιείται το καθαρό κόστος του εγκλήματος προσφέροντας μια θεωρία εσωτερικοποίησης ('Pigouvian Tax'). Υπό τη διατύπωση του Posner (1985 ''An Economic Theory of the Criminal Law'' Columbia LR 1195) η ποινική κύρωση πρέπει να υπερβαίνει το αναμενόμενο κέρδος για να αποτρέπει τους παραβάτες από την συμμετοχή σε πράξεις στις οποίες το αντλούμενο κέρδος υπερβαίνει το επίπεδο της βλάβης (Fisher 2014: 51).

θεωρητικώς σωφρονιστικό μέσο της φυλάκισης δύναται να έχει αντίθετα των επιδιωκόμενων αποτελέσματα συντείνοντας στην καλλιέργεια κακόβουλων τάσεων (Sah 1991: 1272-1295).

Ενδεικτικά παραδείγματα είναι αυτό του διάσημου cracker John Draper που συνελήφθη στις ΗΠΑ το 1972 για απάτες μέσω συστημάτων τηλεπικοινωνιών, ο οποίος, ενόσω εξέτιε την ποινή του στη φυλακή, μοιράστηκε τις μεθόδους του περί πρόσβασης στα συστήματα τηλεπικοινωνιών με αποτέλεσμα, μετά την συμβολή του, οι εταιρείες τηλεπικοινωνιών να παρατηρήσουν υψηλότερες απώλειες (Monteiro 2011: 5) και του Max Butler ο οποίος αφότου καταδικάστηκε για εισβολή στα συστήματα πληροφορικής του Πενταγώνου, κατά τον εγκλεισμό του στη φυλακή έκανε γνωριμίες που τον μύησαν στις εισβολές σε τραπεζικά συστήματα και στις απάτες με πιστωτικές κάρτες (Poulsen 2011). Θεμελιώδη επιρροή στο μοντέλο της μαθηματικής στάθμισης των πιθανοτήτων που αναδεικνύει την υπεροχή των χρηματικών προστίμων ως καλύτερου μέσου αποτροπής του εγκλήματος, φαίνεται πως ασκούν επιπλέον εξωγενείς-κοινωνικοί παράγοντες καθότι επηρεάζουν τα ποσοστά του εγκλήματος μέσα στην κοινωνία. Ιδίως, χρησιμοποιούμενου ενός δείκτη κοινωνικών αλληλεπιδράσεων προκύπτει ότι το ποσοστό των κοινωνικών επιδράσεων, όπως επηρεάζεται από εξωγενείς παράγοντες, είναι υψηλότερο στα εγκλήματα ήσσοντος απαξίας ή μικροεγκλήματα, μέτριο σε πιο σοβαρά εγκλήματα και αμελητέο σε εγκλήματα αυξημένης απαξίας (Glaeser 1996: 507-548).

Το θεώρημα του Becker έχει δεχθεί κριτικές επειδή αποτυγχάνει να εξηγήσει βασικές συνισταμένες του Ποινικού Δικαίου, όπως ο δόλος (‘mens rea’) (Dau-Scmidt 1990: 27). Έτερη προβληματική αναπτύχθηκε από τον Stigler (1970: 526-536 σε Mookherjee & Png 1994: 1039-1066)[160] σε σχέση με την έννοια της οριακής αποτροπής (‘marginal deterrence’),[161] που επηρεάζει τη δημιουργία των κατάλληλων κινήτρων στα άτομα ώστε να απέχουν από σοβαρότερες παραβάσεις ή από τη διάπραξη ομοίων εγκλημάτων σε μεγαλύτερη κλίμακα.[162] Παρά ταύτα, η προσέγγιση του Becker αποτελεί

[160] Άλλη προβληματική στο μοντέλο του Becker είναι η επίδραση της πιθανότητας σύλληψης αθώων.
[161] Οι παραβάσεις διαφέρουν ως προς τη σοβαρότητά τους και οι μέγιστες επιβαλλόμενες τιμωρίες για όλες τις παραβάσεις δε μπορούν να παράσχουν οριακό εμπόδιο για έναν παραβάτη ώστε να μην προβεί σε διάπραξη μιας σοβαρότερης παράβασης.
[162] Η παραδοσιακή θεώρηση ερωτά αν η τιμωρία για το Χ αποτρέπει το Χ, ενώ η οριακή αποτροπή ερωτά αν η τιμωρία για Χ αποτρέπει Χ+1.

σημαντική αφετηρία στην εξέταση των τρόπων διαμόρφωσης κοινωνικά βέλτιστων οικοδομημάτων, όπου οι άνθρωποι ανταποκρίνονται σε κίνητρα.

3.4.2 Τα συστατικά της ανάλυσης κόστους-οφέλους

Ακολουθώντας την οικονομική προσέγγιση και προσαρμόζοντάς τη στο πεδίο του ηλεκτρονικού εγκλήματος, η απόφαση τέλεσης του εγκλήματος από μερίδα των υποψήφιων δραστών λαμβάνεται δυνάμει του μοντέλου: $Mb + Pb > Ocp + OcmPaPc$ (Clark & Davis 1995), όπου το *Mb* ισούται με τα οικονομικά οφέλη από τη διάπραξη του εγκλήματος, το *Pb* ισούται με τα ψυχολογικά οφέλη, το *Ocp* με το ψυχολογικό κόστος, το *Ocm* με το κόστος ευκαιρίας, το *Pa* με την πιθανότητα σύλληψης και το *Pc* με την πιθανότητα καταδίκης. Η ύπαρξη οικονομικών κινήτρων γίνεται αντιληπτή από τα τεράστια χρηματικά ποσά που αποσπώνται από εγκλήματα που λαμβάνουν χώρα στον κυβερνοχώρο. Σύμφωνα με έρευνα της εταιρείας IDC περισσότερο από το 60% των hackers επιτέθηκαν σε οικονομικούς οργανισμούς το 2003, ενώ μόνη η συνολική απώλεια από επιθέσεις phishing το ίδιος έτος ανήλθε στα 1,6 δισ. (RSA 2014). Τα ψυχολογικά οφέλη εξηγούνται με όρους εγγενών κινήτρων που ενεργοποιούν τα άτομα και τα ωθούν σε δραστηριότητες από τις οποίες αντλούν ικανοποίηση, η οποία, ανάλογα με την κατηγορία-προφίλ στην οποία εντάσσεται ο δράστης λαμβάνει την αντίστοιχη μορφή (π.χ. στην περίπτωση των script-kiddies το κίνητρο εντοπίζεται στην περιέργεια και την ευαρέσκεια των τεχνικών γνώσεων ενώ στην περίπτωση των hacktivists στη διασπορά μιας πολιτικής ιδέας). Τα ψυχολογικά κόστη συνδέονται με την ψυχική και διανοητική ενέργεια που απαιτείται για τη διάπραξη του εγκλήματος και καταλήγει στο φόβο της τιμωρίας.

Στο πλαίσιο αυτό, σημαντική είναι η διαπίστωση του κοινωνικού υποβάθρου των δραστών και της ηθικής διαδρομής που ακολουθούν (Kshetri 2006: 33-39). Στο κόστος σύλληψης περιλαμβάνονται οι πιθανότητες σύλληψης αξιολογούμενες στην οικονομική τους διάσταση.[163] Ελλείπουσας της σχετικής νομοθεσίας σε πολλά κράτη ή ακόμη ληφθέντος του κινδύνου σκόπιμης διατήρησης νομοθετικών αδυναμιών ή κενών, σε κάποιες περιπτώσεις, το κόστος σύλληψης μπορεί να είναι μηδενικό.[164] Το κόστος

[163] Για παράδειγμα αν ένας hacker καταδικαστεί σε τριετή στερητική της ελευθερίας ποινή εκτιόμενη και υποθέσουμε ότι οι ετήσιες απολαβές του ανέρχονται σε 20.000, η καταδίκη θα του κοστίσει 60.000.
[164] Με κίνητρο την προσέλευση κονδυλίων για την καταπολέμηση του ηλεκτρονικού εγκλήματος.

σύλληψης ελαχιστοποιεί, περαιτέρω, η συχνή δυσκολία συνεργασίας μεταξύ δημοσίου και ιδιωτικού τομέα και η περιορισμένη εκπαίδευση των αστυνομικών αρχών ή άλλων φορέων επιφορτισμένων με τα καθήκοντα της εξιχνίασης και της αποτροπής των δραστών. Τέλος, το κόστος καταδίκης σχετίζεται με τις πραγματικές πιθανότητες επιβολής καταδικαστικής ποινής και έκτισης αυτής, η οποία δυσχεραίνεται από τη συχνή μη καταγγελία σχετικών παραβάσεων και την προσφυγή σε αρκετές περιπτώσεις σε ίδιες λύσεις (π.χ. σε περιστατικά κλοπής ταυτότητας συνηθέστερη είναι η επικοινωνία με τον φορέα).

3.5 Η έννοια της αποτροπής

3.5.1 Το μοντέλο της αγοράς και η διαμόρφωση του κόστους αποτροπής

Προέκταση της θεωρίας του Becker αποτελεί το μοντέλο της αγοράς (‘model of offenses’) που στηρίζεται στην ισορροπία ανάμεσα: α) στην προσφορά των προσβολών (‘supply of offenses’) ή αλλιώς το ποσοστό του εγκλήματος, β) τη ζήτηση (‘demand’) ως την παροχή παράνομων αγαθών και υπηρεσιών και γ) την αρνητική ζήτηση (‘negative demand’) που προέρχεται από την τάση των δυνητικών θυμάτων να επιζητούν δημόσια και ιδιωτική προστασία (Monteiro 2011: 1-2). Στο πρώτο σκέλος, η προσφορά επηρεάζεται από τις πιθανότητες κέρδους, την προσωπική απέχθεια για το έγκλημα και την αντίληψη του δράστη σχετικά με τις πιθανότητες σύλληψης, περιλαμβανομένων των εξωτερικών αλληλεπιδράσεων ως παράγοντα επηρεασμού του ποσοστού εγκληματικότητας (Glaeser, Sacerdote & Scheinkman 1996: 507-548), το οποίο, επηρεάζεται, περαιτέρω, από την εισοδηματική ανισότητα με δύο τρόπους. Πρώτον, οι ευρισκόμενοι σε μειονεκτικότερη οικονομικά θέση έχουν μικρότερο κόστος ευκαιρίας για τη διάπραξη του εγκλήματος[165] και δεύτερον, οι κάτοχοι υψηλών εισοδημάτων αποτελούν προσφιλείς στόχους. Η διανομή των πόρων επηρεάζει, επομένως, τη ζήτηση. Αυτό εξηγεί την εκκίνηση πολλών μοντέλων από έναν κοινωνικό σχεδιασμό που βασίζεται στην ύπαρξη ενός εξωτερικού και ιδίως κρατικής προέλευσης οργάνου-φορέα,

[165] Νοούμενο ως το κόστος που προκύπτει από τη θυσία ενός αγαθού για την παραγωγή κάποιου άλλου αγαθού, ήτοι της θυσίας των εναλλακτικών εκείνων αγαθών που θα μπορούσαν να παραχθούν με τη χρήση των ίδιων παραγωγικών συντελεστών και δη της εναλλακτικής επιλογής που στις ασθενέστερες οικονομικά τάξεις εμφανίζεται λιγότερο κερδοφόρα.

επιφορτισμένου με τη διόρθωση των ατελειών-αδυναμιών της αγοράς που συντείνουν στην αύξηση του εγκλήματος.

Στη βάση της αναζήτησης κινήτρων και με γνώμονα τη μεταβολή του σημείου ισορροπίας, η αποτελεσματική λειτουργία του Ποινικού Δίκαιου οφείλει να εμπεριέχει τη δημιουργία πρότερων αποτρεπτικών παραγόντων στη βάση της έννοιας της αποτροπής που θεμελιώνεται σε δύο στοιχεία: α) τη τιμωρία των δραστών με την αύξηση του κόστους στην κλίμακα κόστους-οφέλους και β) την αποτροπή της επιτυχίας της επίθεσης (Kesan & Hayes 2012: 431-434). Σε ό, τι αφορά στο πρώτο στοιχείο κόστους αποτροπής ('cost deterrence'), ρόλος του κρατικού μηχανισμού είναι να αυξήσει το κόστος αποτροπής, το οποίο στο χώρο του Διαδικτύου είναι χαμηλό, λαμβανομένης της χαμηλής επένδυσης σε κεφάλαιο και ανθρώπινο δυναμικό ('perpetration cost') και του υψηλού προσδοκώμενου οφέλους, συγκρινόμενου του τελευταίου με το προσδοκώμενο κόστος. Πρόσθετο ρόλο σε αυτό δύνανται να επιτελέσουν οι πάροχοι υπηρεσιών ως εμπλεκόμενα τρίτα μέρη ανάμεσα στο δράστη και την εγκληματική ενέργεια, η κατανομή ευθυνών στους οποίους αυξάνει το κόστος αποτροπής. Τούτο βέβαια στο βαθμό που δε θίγεται η διασύνδεση ('interconnectivity') και η αξία του Διαδικτύου. Με οικονομικούς όρους, οι εξωτερικές επιδράσεις ('network effects') μπορούν να οδηγήσουν σε υπερβάλλουσα αδράνεια, οπότε μια νέα τεχνολογία ανακόπτεται παρότι η υιοθέτησή της θα λειτουργούσε προς όφελος των περισσότερων. Από την άλλη, μεταξύ των παρόχων υπηρεσιών και των χρηστών παρεμβάλλονται πληροφοριακές ασυμμετρίες ('asymmetric incentives') με αποτέλεσμα οι πάροχοι υπηρεσιών ως ιδιωτικές οντότητες να φέρουν την ευθύνη της απομάκρυνσης των «επικίνδυνων» χρηστών, θυσιαζομένων έτσι, των ευεργετημάτων του δικτύου. Πρωτεύοντα ρόλο στην αποφυγή της υπονόμευσης των πλεονεκτημάτων του Διαδικτύου ('negative externalities') (Katyal 2001: 1006-1008) και στην ανάπτυξη των μηχανισμών εκείνων που θα εξουδετερώσουν τα διαδικτυακά μειονεκτήματα οφείλει να έχει το Δίκαιο.[166]

[166] Προβληματική αυτού αποτελεί το καλούμενο 'dual use problem' που αφορά στα μέτρα εκείνα τα οποία έχουν και θετικό και αρνητικό αντίκτυπο και τα οποία πρέπει να αξιολογούνται προσεκτικά. Για παράδειγμα η κρυπτογραφία λειτουργεί ως μέσο προώθησης της ασφάλειας στις επικοινωνίες και της ελευθερίας αλλά λειτουργεί επίσης και ως μέσο προαγωγής της τρομοκρατίας.

3.5.2 Η εσωτερική υπακοή ως έτερος παράγοντας αποτροπής

Οι περισσότερες θεωρίες αποτροπής εστιάζουν τη συμμόρφωση στο νόμο στο φόβο των επερχόμενων συνεπειών, της τιμωρίας. Αντίθετα με το φόβο της τιμωρίας, οι κοινωνικοί ψυχολόγοι προτάσσουν την έννοια της εθελοντικής υπακοής ('internal obligation'), ως εσωτερικής υποχρέωσης συμμόρφωσης στο Δίκαιο[167], η οποία διαφοροποιείται στα άτομα ανάλογα με τον τρόπο που αντιδρούν στα ερεθίσματα, τυγχάνει, όμως, συνυφασμένη, κατά τρόπο ομοιογενή στις συνειδήσεις των κοινωνών, με την πεποίθηση ότι οι αρχές έχουν το δικαίωμα να ρυθμίζουν την ανθρώπινη συμπεριφορά. Η θεωρία του 'Group-Value Model' (Smith, Tyler et al. 1998: 470-493) διατείνεται υπέρ του μεγαλύτερου αντικτύπου που μπορεί να έχει η ανάπτυξη ενός μοντέλου εθελοντικής υπακοής, ερειδόμενου στην αποδοχή αυτού που θεωρείται ως Δίκαιο, από όλα τα μέλη και που συντείνει στη διατήρηση της κοινωνικής σταθερότητας. Κατά την παρατήρηση του Harcourt (2001 σε Link, Nathan W., James M. Kelly & al. 2017: 661) η «διαταραχή», ερμηνευόμενη ως παρέκκλιση, δεν αντιπροσωπεύει ένα σταθερό και αδιαμφισβήτητο χαρακτηριστικό που συνοδεύει τα άτομα, αλλά ορισμένα άτομα, αποδεικνύονται απλώς πιο επιρρεπή από άλλα σε αρνητικές επιρροές, ενώ με τους όρους του Hipp, όσοι ζουν σε προβληματικά περιβάλλοντα εμφανίζουν συχνότερα «προκατάληψη» στις αντιλήψεις τους για την αλήθεια, επηρεαζόμενοι, με την πάροδο του χρόνου, από τις τοπικές ασταθείς συνθήκες. (2010 σε Link, Nathan W., James M. Kelly & al. 2017: 660-661) Με άλλη διατύπωση, κατά τον κοινωνιολόγο Rob Sampson, εμπειρικά διαπιστώνεται ότι τα καλύτερα οργανωμένα δίκτυα συνοδεύονται από χαμηλότερα επίπεδα θυματοποίησης και προσβολών (Meares, Katyal & Kahan 2004: 1190). Αντιστρέφοντας τα ευρήματα της θεωρίας των σπασμένων παραθύρων ('broken windows theory', Wilson & Kelling 1982, Green 2015: 265-276)[168] και συσχετίζοντάς τα με το 'group value model' υποθέτουμε ότι η εστίαση της προσοχής στη δημιουργία κοινωνικών μοντέλων προσαρμοσμένων στους παράγοντες διαμόρφωσης της ανθρώπινης συμπεριφοράς εμφανίζει μεγαλύτερες πιθανότητες να οδηγήσει σε

[167] Το Δίκαιο νοούμενο ως το σύνολο των δεσμευτικών κανόνων που ρυθμίζουν κατά τρόπο εξαναγκαστικό την ανθρώπινη συμπεριφορά και εμπεριέχει την έννοια του ηθικά ορθού στην αντίληψη των κοινωνών.
[168] Αφήνοντας για πολύ καιρό άλυτο ένα μικρότερο πρόβλημα βρισκόμαστε τελικώς αντιμέτωποι με ένα μεγαλύτερο και τελικώς δισεπίλυτο πρόβλημα. Τούτο διότι η παράβλεψη της ανομίας σε μικρότερη κλίμακα δε δίνει κίνητρο για μη διαιώνισή της σε μεγαλύτερη κλίμακα. 'If you take care of the little things then you can prevent a lot of the big things' (Bratton, Police Commissioner, 2014). Διαθέσιμο εδώ: https://www.nytimes.com/2014/03/05/nyregion/bratton-says-street-stops-and-fighting-low-level-crime-will-remain-crucial.html

κοινωνικά βέλτιστα αποτελέσματα. Δεν παραβλέπεται, επίσης, ότι η διατήρηση μηχανισμών συμμόρφωσης από τις Αρχές είναι δαπανηρή και οι πόροι πεπερασμένοι. Αντιθέτως, η καλλιέργεια μιας νοοτροπίας νομιμότητας, στην κατεύθυνση σχηματισμού κοινωνικών νορμών ('social norms'), ως μέσου συμμόρφωσης προς την έννομη τάξη δεν επηρεάζεται από το πεπερασμένο των πόρων, καθότι το θεμιτό πλαίσιο νομιμότητας μπορεί να επιτευχθεί μέσα από την αλλαγή των ακολουθούμενων πρακτικών με τρόπο που δεν απαιτεί την κατανάλωση επιπρόσθετων πόρων. Εκκινώντας από το απλό παράδειγμα του τρόπου αντιμετώπισης των δραστών, έρευνες έχουν δείξει ότι στις περιπτώσεις που τα αστυνομικά όργανα συμπεριφέρονται με ευγένεια και μεγαλύτερο σεβασμό η συμμόρφωση επιτυγχάνεται με δαπάνη λιγότερων πόρων, καθώς επίσης αναμένεται μεγαλύτερη συμμόρφωση (Meares, Katyal & Kahan 2004: 1196).

3.6 Η πρόταση του Lessig

Η πρόταση εστιάζει στα φυσικά και ηλεκτρονικά εμπόδια που μπορούν να αποτρέψουν τις επιβλαβείς ενέργειες ('harmful acts') ως εργαλεία οριοθέτησης της ανθρώπινης συμπεριφοράς. Η θεωρία των τεσσάρων τρόπων οριοθέτησης της ανθρώπινης δράσης, όπως διατυπώθηκε από τον Lessig ('Pathetic Dot Theory' ή 'New Chicago School Theory') και μεταφέρεται στο χώρο του Διαδικτύου υποστηρίζει ότι η ανθρώπινη συμπεριφορά μπορεί να ρυθμιστεί από τέσσερις συντελεστές ('four modalities of constraint'): α) το νόμο, β) τους κανόνες κοινωνικής συμπεριφοράς, γ) την αγορά και δ) την αρχιτεκτονική της τεχνολογίας, καθένας εκ των οποίων επισύρει ένα διαφορετικό κόστος στο δράστη (Jiow 2013). Οι τέσσερις αυτές παράμετροι δεν είναι ανεξάρτητες η μία από την άλλη, αλλά αλληλεπιδρούν μεταξύ τους (Lessig 1999, 2006).

Ο νόμος υποδεικνύει ποιες συμπεριφορές δεν πρέπει να τελεστούν προκειμένου να αποφευχθεί η ποινική τιμωρία, η οποία για να είναι αποτελεσματική πρέπει να τελεί σε εύλογη αναλογία με την αποδοκιμαζόμενη πράξη, υπό την έννοια ότι τα αξιοποιούμενα μέσα προς αποτροπή πρέπει να είναι πρόσφορα και αναγκαία για την επίτευξη του επιδιωκόμενου σκοπού και συνάμα, να μην υπάρχουν λιγότερο ήπια μέσα δυνάμενα να επιφέρουν το επιδιωκόμενο αποτέλεσμα (αρχή της αναλογικότητας stricto sensu). Οι παραδοσιακές προσεγγίσεις αγνοούν το αντίστροφο αποτέλεσμα ιδιαίτερα υψηλών ποινών που στην πράξη ενέχουν τον κίνδυνο της μη εφαρμογής ('Inverse sentencing effect'), ακριβώς λόγω του δυσανάλογου χαρακτήρα τους, που ενδέχεται να

καταστήσει τα όργανα επιβολής διστακτικά στην εφαρμογή της, τη δε ενδεχόμενη επιβολή, άδικη. Αντιθέτως, πολύ σημαντικότερη κρίνεται η συνέπεια στην εφαρμογή μιας ποινής στο βαθμό που συμπορεύεται με κανόνες κοινωνικής συμπεριφοράς. Σε αντίθετη περίπτωση, η πρόταξη ενός νομοθετικού πλαισίου ανεξάρτητου από τα κοινωνικά πρότυπα μπορεί τελικώς να δυσχεράνει την αποτροπή αντί να την προαγάγει.[169]

Οι κανόνες κοινωνικής συμπεριφοράς περιορίζουν μέσα από το στίγμα που επιβάλλει η κοινωνία. Βασική υπόθεση της αποτροπής είναι η ενημέρωση των δυνητικών δραστών για το επαπειλούμενο πλαίσιο ποινής, η οποία επιτυγχάνεται μέσω μιας σύνθετης διαδικασίας κοινωνικής αλληλεπίδρασης. Κατά τον Andenaes (*Punishment and Deterrence* 1974) οι ποινές στέλνουν μηνύματα στην κοινωνία τα οποία μηνύματα καταλήγουν να δημιουργούν κανόνες κοινωνικής συμπεριφοράς ('social norms') που ενθαρρύνουν την υποσυνείδητη αποχή από το έγκλημα ('unconscious deterrent effect')[170] μεταθέτοντας την προβληματική από τη σχετική τιμή στην κοινωνική τιμή ('social price'). Σε ευρύτερη κλίμακα, η προσφυγή στην εγκληματική δραστηριότητα σχετίζεται με το στίγμα, το οποίο, από ψυχολογική σκοπιά, οδηγεί σε εσωτερικοποίηση του αρνητικού αντικτύπου του στίγματος και διαιώνιση της παρεκκλίνουσας συμπεριφοράς.[171] Εν τη απουσία δομών ένταξης ή επανένταξης δρώντων υποκειμένων που παρεκκλίνουν από την κοινωνική ορθότητα, οι παραβάτες είναι πιθανό να στραφούν εκ νέου σε εγκληματικές δραστηριότητες[172] και συναναστροφή με άτομα αντίστοιχων (παρεκκλινουσών) προτιμήσεων με τα οποία ομοιάζουν (Meares, Katyal & Kahan 2004: 1184). Υπό αυτή τη σκέψη λαθεμένες στρατηγικές μπορούν να επιφέρουν πρόσθετα κόστη στην κοινωνία.

Οι δυνάμεις τη αγοράς καθορίζουν το οικονομικό κόστος μιας συμπεριφοράς μέσα από τον καθορισμό της τιμής, η οποία στην προκειμένη περίπτωση ισοδυναμεί με την επιβολή του νόμου. Στη αγορά συναντώνται, ωστόσο, φαινόμενα υποκατάστασης

[169] Meares, Katyal & Kahan (2004: 1185-1186) – με αναφορά σε Blumstein, Cohen & Nagin (1978)
[170] Κατά τη διατύπωση του Βρετανού δικαστή James Fitzjames Stephen *'some people abstain from murder because they fear that, if they commited murder, they would be hung. Hundreds of thousands abstain from it because they regard it with horror. One great reason why they regard it with horror is, that murderers are hung with the hearty approbation of all reasonable men'* (Stephen 1863).
[171] Ο Goffman (1963, *Stigma: Notes on the Management of Spoiled Identity*) ορίζει ως άτομα φέροντα το στίγμα όλα όσα παρεκκλίνουν από τους κανόνες κοινωνικής συμπεριφοράς.
[172] Αν αισθάνονται ότι άλλες επιλογές δεν είναι διαθέσιμες για αυτούς είτε αν άλλες επιλογές εμφανίζονται λιγότερο κερδοφόρες (π.χ. η μαύρη εργασία ενισχύεται από τους χαμηλούς μισθούς της νόμιμης εργασίας)

('substitution effects'). Η θεωρία της υποκατάστασης επεκτεινόμενη στο πεδίο του Ποινικού Δικαίου και του σχηματισμού προτιμήσεων στην κοινωνία οδηγεί στη σκέψη ότι η αύξηση της τιμής ενός αδικήματος, νοούμενης της τιμής ως της επαπειλούμενης ποινής, θα οδηγήσει στη ζήτηση ενός άλλου συμπληρωματικού αδικήματος (Stigler 1970: 526-536).[173] Μόνη επομένως η αύξηση της ποινής ενός αδικήματος δεν συντείνει απαραίτητα στην μείωση της εγκληματικότητας είτε αυτή εξετάζεται στο πραγματικό κόσμο είτε στον ψηφιακό, αντιμετωπιζόμενου έκαστου πεδίου ως αγοράς (Meares, Katyal & Kahan 2004: 1176-1180). Στο πλαίσιο αυτό, σκόπιμη είναι η τοποθέτηση σημείων αναφοράς στο κέντρο της ανάλυσης. Έτερος παράγοντας που μπορεί να στρέψει την προσοχή σε άλλα εγκλήματα έναντι της συνολικής μείωσης της εγκληματικότητας είναι η σύγκριση μεταξύ των διαθέσιμων επιλογών, οπότε η προσθήκη μιας υποδεέστερης εναλλακτικής ανάμεσα σε δύο προϊόντα μπορεί να καταστήσει ελκυστική μια ορισμένη επιλογή.[174] Την τάση να προτιμούν οι καταναλωτές το προϊόν Α έναντι του Β με αυξανόμενο ρυθμό προστιθέμενης μιας εναλλακτικής Γ κατώτερης του Α αλλά ανώτερης του Β, οι ψυχολόγοι ονομάζουν αποτέλεσμα ασύμμετρης κυριαρχίας ('asymmetric dominance effect') (Meares, Katyal & Kahan 2004: 1180-1181), μέσα από την οποία καταδεικνύεται ότι πέρα από τη στάθμιση κόστους οφέλους και τη μεταβολή των συστατικών του ποινικού πλαισίου, η αποτελεσματικότατα των επιβαλλόμενων μέτρων αποτελεί συνάρτηση περισσότερων παραγόντων[175]

Τέλος, ο σχεδιασμός της τεχνολογίας και η διαθεσιμότητά της, συναπαρτίζουν το οικοδόμημα της τεχνολογίας, το οποίο επηρεάζει ευθέως την προσέλκυση των χρηστών. Για παράδειγμα η ενεργοποίηση μηχανισμών ανίχνευσης της τοποθεσίας από τις εταιρείες κατασκευής λογισμικού αυξάνει την πιθανότητα σύλληψης και κατ' επέκταση το κόστος τέλεσης του εγκλήματος (perpetration cost) (Katyal 2001: 1012).

3.7 Στρατηγική τριών μερών

[173] Στον πραγματικό κόσμο, αν π.χ. αυξηθεί η τιμή ενός ναρκωτικού (κρακ), είναι πολύ πιθανό να αυξηθεί η ζήτηση ενός άλλου συμπληρωματικού ναρκωτικού (ηρωίνη).
[174] Ανάμεσα σε δύο προϊόντα, ένα προϊόν Α υψηλότερης τιμής και ποιότητας και ένα προϊόν Β χαμηλότερης τιμής και ποιότητας, ο καταναλωτής είναι αδιάφορος. Αν όμως εμφανιστεί ένα προϊόν Γ με τιμή αντίστοιχη του Β αλλά ακόμη χαμηλότερη ποιότητα το προϊόν Β φαίνεται ελκυστική επιλογή.
[175] Τα άτομα τελικώς εξετάζουν τη διάπραξη ενός εγκλήματος σε σχέση με τα κόστη και οφέλη άλλων εγκληματικών δραστηριοτήτων.

Παράλληλα προς την επιβολή του νόμου[176], η ενίσχυση του οποίου είναι επιβεβλημένη, η ελαχιστοποίηση των αρνητικών συνεπειών του ηλεκτρονικού εγκλήματος απαιτεί τρόπους δράσης, που θα συμπορεύονται και θα συνεπικουρούν την ποινική νομοθεσία, οριοθετούμενους από τις αρχές της έννομης τάξης. Στο πλαίσιο αυτό, παρουσιάζονται i) στρατηγικές πρώτου μέρους ('first party') που στοχεύουν στην αποτροπή των δραστών που, υπό την αποδοχή της σκέψης του ορθολογικά δρώντος υποκειμένου, αποφασίζουν τη δράση τους έπειτα από μια ορθολογική στάθμιση επιμέρους στοιχείων, στα οποία, η προσθήκη θετικών κινήτρων αντισταθμίζει τα προσδοκώμενα οφέλη από τη διάπραξη του εγκλήματος, ii) στρατηγικές δευτέρου μέρους ('second party') που θα ενθαρρύνουν τα δυνητικά θύματα να αναπτύξουν μηχανισμούς προστασίας νομιμοποιούμενα να ασκήσουν ήπιας μορφής αυτοάμυνα με σκοπό την αύξηση του κόστους αποτροπής και iii) στρατηγικές τρίτου μέρους ('third party') (Katyal 2001: 1038-1114) βασιζόμενες στη δράση των παρόχων υπηρεσιών ως φορέων διαμεσολάβησης στο ψηφιακό περιβάλλον και άλλων ιδιωτικών οντοτήτων που θα παρακολουθούν τις επικίνδυνες δραστηριότητες και θα προλαμβάνουν τις επιθέσεις μέσω τεχνολογικών λύσεων.

3.7.1 Η ευθύνη των ενδιάμεσων μερών

Το ζήτημα της ευθύνης ενδιάμεσων μερών όπως των παρόχων υπηρεσιών, των ιδιοκτητών υπολογιστών zombie ή των εταιρειών κατασκευής λογισμικού έχει απασχολήσει την επιστήμη και έχει εγείρει συζητήσεις γύρω από τις προβληματικές θεμελίωσής της στη βάση των στοιχείων του δόλου, της αμέλειας ή της αντικειμενικής ευθύνης (Kesan & Hayes 2012: 496). Καίριο είναι, ακόμη, το ζήτημα του αιτιώδους συνδέσμου ανάμεσα στη ζημιογόνο δράση και το ζημιογόνο αποτέλεσμα, για το οποίο έχουν διατυπωθεί διαφορετικές θεωρίες, καθώς επίσης, της διακοπής της αιτιώδους διαδρομής μεσολαβούντων περισσότερων μερών. Ιδιαίτερη βαρύτητα, μεταξύ των περισσότερων μερών, παρουσιάζουν οι πάροχοι υπηρεσιών χωρίς τη μεσολάβηση των οποίων, αδικήματα, όπως η εκβίαση, η δυσφήμιση, η απάτη, οι παραβιάσεις δικαιωμάτων

[176] Μόνη δε η ενίσχυση της ποινικής νομοθεσίας θα μπορούσε να ισχυριστεί κανείς ότι ενέχει τον κίνδυνο του αποτελέσματος υποκατάστασης και εισοδήματος ('income effect') υπό την έννοια ότι η υψηλή ποινή για ένα έγκλημα ίσως ευνοήσει τη διάπραξη άλλων, ενδεχομένως και πιο καταστροφικών κοινωνικά εγκλημάτων ('substitution analysis').

πνευματικής ιδιοκτησίας ή η πορνογραφία, καθώς και φαινόμενα όπως τα fake news[177] και το hate speech που βρήκαν πρόσφορο έδαφος αναπαραγωγής μέσω των ενδιάμεσων φορέων, δε θα ήταν τεχνικά εφικτό να τελεστούν. Οι πάροχοι υπηρεσιών αποτελούν επομένως, ακρογωνιαίο λίθο του ψηφιακού περιβάλλοντος φέροντας έναν ρόλο καθοριστικό στη διακίνηση των πληροφοριών. Ενόψει αυτών, το ερώτημα που έχει απασχολήσει τη διεθνή βιβλιογραφία ήδη από τις απαρχές της λειτουργίας του Internet και εξακολουθεί να απασχολεί είναι το ζήτημα της νομικής ευθύνης των παρόχων υπηρεσιών για εγκληματικές πράξεις που διαπράττονται από τους χρήστες τους.[178] Τα διάφορα νομικά συστήματα έχουν προτείνει διαφορετικές λύσεις με μεγαλύτερη ομοιογένεια να εντοπίζεται στον περιορισμό της ευθύνης σε περιπτώσεις στις οποίες ο πάροχος λαμβάνει γνώση του παράνομου περιεχομένου που βρίσκεται σε ιστοσελίδες που τελούν υπό τον έλεγχό του και αρνείται να αναλάβει δράση (Viano 2017: 12). Στη Γαλλία για παράδειγμα, οι πάροχοι υπηρεσιών απαιτείται να καλούν τους χρήστες να τους ειδοποιούν για απαγορευμένο περιεχόμενο όπως η παιδική πορνογραφία, πρόκληση σε βία ή προσβολή της ανθρώπινης αξιοπρέπειας και πρέπει να αναλαμβάνουν άμεσα δράση για μετακίνηση περιεχομένου εμφανώς παράνομου ('manifestly illegal') (COE 2007, Weigend 2013:63).

Στην κατεύθυνση της θεσμοθέτησης ευθύνης, ιδιαίτερα σημαντική είναι η Οδηγία 'E-Commerce Directive 2000' (Directive 2000/31/EC) για το ηλεκτρονικό εμπόριο,[179] μέσω της οποίας σκοπείται η περιστολή των εννόμων συνεπειών σε βάρος των παρόχων υπηρεσιών ως ενδιάμεσων φορέων και η οριοθέτησή τους σε έλλογα πλαίσια. Η Οδηγία ρυθμίζει το νομικό πλαίσιο των μεσαζόντων στην εσωτερική αγορά για το περιεχόμενο που διαχειρίζονται, θωρακίζοντάς τους έναντι των κινδύνων της online διακίνησης. Θεσπίζοντας συγχρόνως ένα καθεστώς ασυλίας κατά οριζόντιο τρόπο υπέρ των παρόχων

[177] Κλασικό παράδειγμα της αυτής δυναμικής αποτελούν οι προεδρικές εκλογές των ΗΠΑ και η άσκηση επιρροής στο εκλογικό αποτέλεσμα μέσα από δίκτυα λογαριασμών ανύπαρκτων προσώπων που έλεγχαν Ρώσοι hackers (social bots).

[178] Η Σύμβαση της Βουδαπέστης μολονότι ορίζει στο άρθρο 1 την έννοια του παρόχου υπηρεσιών, περιλαμβάνουσα φορείς δημοσίου και ιδιωτικού Δικαίου, δεν περιέχει ειδικές ρυθμίσεις για την ποινική ευθύνη των παρόχων υπηρεσιών Διαδικτύου, σχετικά με το περιεχόμενο των μηνυμάτων που αποστέλλονται από χρήστες του Διαδικτύου ή τους συνδρομητές τους. Για τους παρόχους υπηρεσιών Διαδικτύου σε ό,τι αφορά τις αξιόποινες πράξεις που τελούνται από τους υπαλλήλους τους για λογαριασμό τους, εφαρμόζονται οι κείμενες διατάξεις. Ειδικότερα, σε ό,τι αφορά στα Συμβαλλόμενα Μέρη που είναι ταυτόχρονα κράτη μέλη της Ευρωπαϊκής Ένωσης (ΕΕ), εφαρμόζονται οι διατάξεις της Οδηγίας 2000/31/ΕΚ σχετικά με το ηλεκτρονικό εμπόριο και οι αρχές της ποινικής ευθύνης όπως θεσπίζονται από την ποινική νομοθεσία εκάστου κράτους.

[179] Η Οδηγία ακολούθησε τον προϋφιστάμενο γερμανικό Teledienstgestz (TDG). Διαθέσιμο εδώ: https://ec.europa.eu/digital-single-market/en/e-commerce-directive

προς διασφάλιση της έλλογης περιστολής του καταλογισμού ευθυνών για όλα τα είδη παράνομων δραστηριοτήτων από τρίτα μέρη[180] ειδικώς, η ευθύνη των παρόχων αποκλείεται αν α) μετακινήσουν ή δυσχεράνουν την πρόσβαση σε παράνομο περιεχόμενο του οποίου τον παράνομο χαρακτήρα γνωρίζουν το ταχύτερο δυνατό μόλις λάβουν γνώση αυτού, καθώς επίσης β) στις περιπτώσεις υπηρεσιών που διαδραματίζουν ουδέτερο, απλώς τεχνικό και παθητικό ρόλο προς το φιλοξενούμενο περιεχόμενο. Τα διαλαμβανόμενα δεν μπορούν σε καμία περίπτωση να επηρεάζουν την ανώνυμη χρήση ανοικτών δικτύων όπως το Διαδίκτυο (άρθρο 14). Σύμφωνα δε με την Οδηγία, τα κράτη μέλη δε μπορούν να επιβάλουν καμία γενική υποχρέωση παρακολούθησης περιεχομένου στους μεσάζοντες (άρθρο 15§1) και τούτο προς αποτροπή φαινομένων προληπτικής λογοκρισίας έναντι της ελεύθερης κυκλοφορίας της πληροφορίας (CTD 2012), ωστόσο, δύνανται να υποχρεώσουν τους φορείς παροχής υπηρεσιών της κοινωνίας της πληροφορίας να ενημερώνουν πάραυτα τις αρμόδιες κρατικές αρχές για τυχόν υπόνοιες περί χορηγούμενων παράνομων πληροφοριών ή δραστηριοτήτων που επιχειρούν αποδέκτες των υπηρεσιών τους ή να ανακοινώνουν στις αρμόδιες αρχές, κατ' αίτησή τους, πληροφορίες που διευκολύνουν τον εντοπισμό των αποδεκτών των υπηρεσιών τους με τους οποίους έχουν συμφωνίες αποθήκευσης (άρθρο 15§2).

i) Η ποινική ευθύνη των ενδιάμεσων παρόχων και ιδίως των μέσων κοινωνικής δικτύωσης υπό το πρίσμα της Οδηγίας 2000/31/ΕΚ και του ΠΔ 131/2003

Σκοπός του κοινοτικού νομοθέτη μέσα από τη θέσπιση της Οδηγίας 2000/31/ΕΚ ήταν ο περιορισμός των ευθυνών των ενδιάμεσων φορέων σε έλλογο πλαίσιο ανεξάρτητα από την κατάταξη των επαπειλούμενων κυρώσεων σε αστικές, διοικητικές ή ποινικές (Δαλακούρας 2018: 103). Η Οδηγία ενσωματώθηκε στην ελληνική έννομη τάξη με το ΠΔ 131/2003, το οποίο κινούμενο σε αυτό το πλαίσιο, στα άρθρα 11-14 ρυθμίζει συλλήβδην την ευθύνη των ενδιάμεσων φορέων σε αστικό, διοικητικό και ποινικό επίπεδο, διακρίνοντας, περαιτέρω, τριών ειδών φορείς ανάλογα με τη λειτουργία τους: α) απλή μετάδοση δεδομένων, β) αποθήκευσης σε κρυφή μνήμη, γ) φιλοξενία. Για την ποινική ευθύνη του παρόχου περιεχομένου, που ταυτίζεται με το δημιουργό τον ψηφιακών δεδομένων – οι χρήστες συνεπώς αποτελούν παρόχους περιεχομένου –

[180] Έκθεση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή – Πρώτη έκθεση σχετικά με την εφαρμογή της οδηγίας 2000/31 COM(2003), 702 τελικό, σημείο 4.6.

ισχύουν τα γενικώς προβλεπόμενα. Ειδικότερα, σε ό, τι αφορά στα μέσα κοινωνικής δικτύωσης, η λειτουργία των οποίων στηρίζεται στην παροχή στους χρήστες της δυνατότητας ψηφιακής επικοινωνίας και αποθήκευση των αναρτώμενων πληροφοριών στα πληροφοριακά συστήματα, ανήκουν στη τρίτη κατηγορία (host-service providers), η ευθύνη τους δε, ρυθμίζεται ειδικά στο άρθρο 13, το οποίο ως lex specialis απωθεί τον γενικό κανόνα που εφαρμόζεται στους παρόχους περιεχομένου. Στη διάταξη του άρθρου 13 τίθενται τα προστατευτικά όρια που καταλαμβάνουν την άγνοια του φορέα για το παράνομο του περιεχομένου της πληροφορίας και συγχρόνως εγκαθιδρύεται ευθύνη του παρόχου προς άμεση απόσυρση ή δυσχέρεια της πρόσβασης μόλις υποπέσει στην αντίληψή του το παράνομο περιεχόμενο. Απαιτείται, επομένως, πραγματική γνώση για να ενεργοποιηθεί η διαδικασία της Ειδοποίησης και Απόσυρσης (Notice and Take Down) (Κακαβούλης 2015: 317 σε Δαλακούρα 2018: 104). Η νομική φύση των παραπάνω ρυθμίσεων έχει δεχθεί αμφισβήτηση και έχει τροφοδοτήσει σημαντικές διατυπώσεις για τη θεμελίωση της ευθύνης. Στη Γερμανία, γεννήτορα της ρύθμισης (Teledienstgestz-TDG), ως κρατούσα προτάσσεται η «λύση της ενσωμάτωσης» κατά την οποία οι προϋποθέσεις αποκλεισμού της ποινικής ευθύνης θα πρέπει να δύνανται να υπαχθούν σε μία από τις τρεις βαθμίδες διάκρισης του εγκλήματος (ειδική υπόσταση, άδικο, ενοχή), κυρίως δε, υποστηρίζεται η εξέταση στο πλαίσιο της πλήρωσης της ειδικής υπόστασης.[181] Όσον αφορά στα εγκλήματα ενέργειας, η απαίτηση της γνώσης του ενδιάμεσου παρόχου αποτελεί ειδική ρύθμιση αποκλεισμού του ενδεχόμενου δόλου – η δε ταχεία απόσυρση συνιστά λόγο εξάλειψης του αξιοποίνου και ειδικώς μορφή έμπρακτης μετάνοιας – και τοποθετείται στην υποκειμενική υπόσταση, ενώ διαφορετική είναι η αντιμετώπιση των τελούμενων δια παραλείψεως εγκλημάτων, για τη διαπίστωση των οποίων η γνώση της ανάγκης ενεργείας, υπό την έννοια της απαίτησης για αφαίρεση του παράνομου περιεχομένου ή παρακώλυση της πρόσβασης σε αυτό, τοποθετείται στην αντικειμενική υπόσταση (Μυλωνόπουλος 2007: 113-116). Στη θεμελίωση της δια παραλείψεως ποινικής ευθύνης προσανατολίζεται η θεωρία ήδη από τις πρώτες αναλύσεις (Κιούπης 1998: 714-720).

[181] Κατά την αντίθετη άποψη η εξέταση προηγείται του ελέγχου της ειδικής υπόστασης (προληπτικό φίλτρο), ωστόσο, αδυνατεί να εξηγήσει τη διαφορετική ποινική αντιμετώπιση των ενδιάμεσων παρόχων.

ii) Ποινική ευθύνη των μέσων κοινωνικής δικτύωσης για εγκλήματα εξωτερίκευσης δυνάμει του κοινού Ποινικού Δικαίου

Ειδικότερα σε ό, τι αφορά στα εγκλήματα εξωτερίκευσης και την ποινική ευθύνη των μέσων κοινωνικής δικτύωσης η ποινική ευθύνη συνδέεται με τη λειτουργία της πλατφόρμας και την παράλειψη διαγραφής του επιλήψιμου περιεχομένου.[182] Κρίσιμος επομένως στη δόμηση της ποινικής ευθύνης είναι ο προσδιορισμός του βαθμού συμμετοχής του ενδιάμεσου φορέα στην αξιόποινη πράξη. Μία θεωρία που έχει υποστηριχθεί είναι αυτή των ουδέτερων συμμετοχικών πράξεων δυνάμει της οποίας η δημιουργία και λειτουργία μιας πλατφόρμας κοινωνικής δικτύωσης συνιστά πράξη ουδέτερη, η οποία, υπό το πρίσμα αυτό, δε μπορεί να γίνει δεκτή ως ποινικά κολάσιμη πράξη (Δαλακούρας 2018: 107). Κατ' άλλη άποψη, η ποινική ευθύνη εδράζεται στην αντιμετώπιση του ενδιάμεσου παρόχου ως αυτουργού ή εν στενή έννοια συμμετόχου στη δια παραλείψεως τελούμενη εγκληματική πράξη, θεωρία που επίσης εμφανίζεται προβληματική και τούτο, διότι η δια παραλείψεως θεμελίωση ποινικής ευθύνης προϋποθέτει ιδιαίτερη νομική υποχρέωση[183] που στην περίπτωση των ενδιάμεσων παρόχων δεν μπορεί να θεωρηθεί ότι υφίσταται ως γενική υποχρέωση αποτροπής παντός μελλοντικού εγκλήματος εξωτερίκευσης[184] Έτι περαιτέρω, η ιδιαίτερη νομική υποχρέωση που θεμελιώνει ευθύνη για μη αποτροπή του επελθόντος κινδύνου απαιτεί δράση πριν την επέλευση του αποτελέσματος, ήτοι προ της εξωτερίκευσης της ζημιογόνου συμπεριφοράς του δράστη. Τρίτη θεωρία που αποπειράται να θεμελιώσει την ειδική υποχρέωση που απαιτεί η αποδοχή του δια παραλείψεως τελούμενου εγκλήματος είναι αυτή περί «εγγυητικών θέσεων», δυνάμει της οποίας ο ενδιάμεσος πάροχος έχει υπό την κυριαρχία του μια πηγή κινδύνου από την οποία απορρέει μια εγγυητική θέση επαγρύπνησης, ερμηνευόμενη ως υποχρέωσης αποτροπής των επαπειλούμενων για τα έννομα αγαθά κινδύνων. (Überwachungsgarant) (Δαλακούρας 2018: 109). Και αυτή η θεωρία, ωστόσο, αποτυγχάνει να τεκμηριώσει επαρκώς τη θεμελίωση ποινικής ευθύνης

[182] Το στάδιο της δημιουργίας βρίσκεται σε απώτερο προστάδιο τέλεσης της πράξης του χρήστη, ώστε η δημιουργία πλατφόρμας αντιμετωπίζεται ως μια κατ' αρχήν κοινωνικά αποδεκτή συμπεριφορά εντός του πλαισίου της έννομης τάξης και δεν μπορεί να γίνει δεκτό ότι καλύπτεται από δόλο του παρόχου κατά το στάδιο της δημιουργίας της πλατφόρμας.

[183] Είτε πρόκειται για αυτουργική συμπεριφορά είτε απλή συνδρομή στο δια παραλείψεως τελούμενο έγκλημα.

[184] Κατά δε το άρθρο 14 ΠΔ 131/2003 οι φορείς παροχής υπηρεσιών φιλοξενίας δε φέρουν γενική υποχρέωση ελέγχου των πληροφοριών που αποθηκεύουν ή δραστήριας αναζήτησης γεγονότων ή περιστάσεων που δείχνουν πως πρόκειται για παράνομες δραστηριότητες (Κακαβούλης 2015: 328-329).

προϋποθέτουσα αφενός έγκλημα αποτελέσματος και αφετέρου πράξη πριν την επέλευση αυτού. Ενόψει τούτων, πιο δόκιμη φαίνεται η λύση που προκρίνει την αναζήτηση της ευθύνης στη βάση της κάθε φορά εκδηλούμενης αξιόποινης συμπεριφοράς με υπαγωγή στις διατάξεις του κοινού Ποινικού Δικαίου, εκεί όπου κρίνεται ότι χωρούν εφαρμογής οι παραδοσιακές διατάξεις, είτε με υπαγωγή σε νέα καθεστώτα προβλέποντα νέες ειδικές υποστάσεις και νέα δικονομικά εργαλεία, εκεί όπου κρίνεται απαραίτητο.

3.7.2 Αυτοάμυνα ('Self-defense')

i) Από την παθητική ('passive defense') στην ενεργητική αυτοάμυνα ('active defense')

Σε επίπεδο διαδικτυακών επιθέσεων η πρώτη μέθοδος πρόληψης εμφανίζεται με τη μορφή της αυτοάμυνας και συγκεκριμένα της παθητικής άμυνας ('passive-defense'), η οποία επιτυγχάνεται ως εξής: α) με ελέγχους στην πρόσβαση του συστήματος, β) με ελέγχους στα δεδομένα πρόσβασης, γ) με ασφαλή διαχείριση και δ) με ασφαλή σχεδιασμό περιλαμβανομένης της σε κάθε περίπτωση εκπαίδευσης των χρηστών ως προς τους τρόπους ανάκαμψης στο ενδεχόμενο δυνητικής επίθεσης και με τελικό στόχο τη θωράκιση των ηλεκτρονικών στόχων (Sklerov 2009: 6-10). Τέτοια παραδείγματα αποτελούν η χρήση ασφαλών κωδικών εισόδου και αριθμών PIN, η ανάπτυξη λογισμικών ασφαλείας, π.χ. virus scanners, η εδραίωση τεχνολογιών όπως το βιομετρικό σύστημα ταυτοποίησης (αναγνώριση προσώπου, φωνής, δακτυλικών αποτυπωμάτων), η κρυπτογράφηση και η αυτοματοποιημένη αποτροπή (Condron). Στην τελευταία, ωστόσο, περίπτωση, ενώ συμφωνείται ότι ενισχύεται η αποτροπή, η δυνητική ζημία που προκαλείται από την εξάλειψη του ανθρώπινου στοιχείου δύναται να υπερβεί τελικώς το όφελος (Grabosky 2016: 466). Τόσο τα μεμονωμένα άτομα όσο και οι επιχειρήσεις επενδύουν σε μηχανισμούς ασφαλείας, οι επιχειρήσεις δε, αρκετές φορές καταφεύγουν και σε μεθόδους ασφάλισης ('hacker insurance'). Υπό την παραδοχή, άλλωστε, ότι η ευημερία στο Διαδίκτυο εξαρτάται σημαντικά από τις δυνάμεις της αγοράς, είναι εύλογη η υπόθεση του Grabosky (2016: 112) ότι οι επιχειρήσεις που παρέχουν ασφαλείς πλατφόρμες υπηρεσιών (π.χ. online banking) και επενδύουν στην ανάπτυξη φιλικών και ασφαλών λειτουργικών συστημάτων είναι εκείνες που θα επιβιώσουν. Τα υποψήφια θύματα επομένως έχουν κίνητρο να λαμβάνουν μέτρα. Επιπλέον, η ενίσχυση των

κινήτρων λήψης τέτοιων μέτρων εικάζεται ότι μπορεί να εδραιώσει μια κουλτούρα.[185] Παρόλα αυτά, τέτοια μέτρα εμφανίζουν αδυναμίες. Ο Katyal εντοπίζει την αδυναμία τους, το πρώτον, στο ότι απευθύνονται σε μικρό εύρος δεκτών, υποθέτοντας ταυτόχρονα, ότι αν αυτές οι μέθοδοι ήταν περισσότερο διάχυτες θα εμφάνιζαν μεγαλύτερη αποτελεσματικότητα, και, δεύτερον, στο ότι δεν είναι σχεδιασμένες να απευθύνονται σε δράστες με πιο εξειδικευμένες ικανότητες ('sophisticated'). Επιπλέον, η ανεπάρκεια αυτών των μέτρων αποδεικνύεται στις περιπτώσεις των zero-days (Kesan & Hayes 2012: 431-542) καθώς επίσης, δεν καταφέρνουν να εξηγήσουν τη συμβολή τους στο επίπεδο της αποτροπής του δράστη, ο οποίος διατηρεί το αρχικό του κίνητρο που τον ωθεί να ξαναπροσπαθήσει. Από την άλλη πλευρά, ενδεχόμενες προσπάθειες ισχυροποίησης των σχετικών μεθόδων σχετίζονται με αύξηση του επιπέδου ασφαλείας που μπορεί να επιτευχθεί με την κάμψη της ανωνυμίας και την ταυτοποίηση των χρηστών, πλην όμως, ενέχουν κινδύνους για την ιδιωτικότητα και το ηλεκτρονικό εμπόριο (Nojeim) (Grabosky 2016: 473). Υπό τις σκέψεις αυτές, αναπτύχθηκε από ορισμένους θεωρητικούς η θεωρία της ενεργητικής άμυνας ('active defense'), η οποία εδράζεται σε τρία επίπεδα: α) τη διαπίστωση μιας εισβολής, β) την εξιχνίαση του εισβολέα και γ) την ενεργοποίηση κάποιας μορφής διαδικτυακών αντιποίνων,[186] νοούμενου του τρίτου επιπέδου ως μορφή επιτρεπόμενης διαδικτυακής αυτοδικίας ('cyber vigilantism')[187] μέσω ανταποδοτικών επιθέσεων[188] ('retributive counterstriking').

ii) 'Mitigative counterstriking' και 'Socially optimal hackback'

Τις προβληματικές της ex post αντιμετώπισης της εκδηλούμενης απειλής και των πιθανών αρνητικών προεκτάσεων της ενίσχυσης των μέτρων παθητικής άμυνας ενδέχεται να προσπελάσει η θεωρία του 'mitigative counterstriking' ή 'socially optimal

[185] Ας σκεφτούμε μια αναλογία πατερναλισμού που υποχρεώνει σε χρήση ζώνης. Αργά ή γρήγορα θα αναγκάσει τους δέκτες της υποχρέωσης, στην πλειοψηφία τους τουλάχιστον, σε συμμόρφωση (Grabosky 2016: 123).

[186] Το νομότυπο των αντιποίνων σχετίζεται αφενός με την εξιχνίαση των δραστών και αφετέρου με τη διασφάλιση ότι τα θιγόμενα μέρη δε θα αποστερηθούν του δικαιώματος υπεράσπισης του εαυτού τους και της ιδιοκτησίας τους.

[187] Στο Διαδίκτυο συναντάται πληθώρα αυτόδικων συμπεριφορών όπως π.χ. σε περιπτώσεις εξιχνίασης αδικημάτων παιδικής πορνογραφίας ή στις λαϊκές «δίκες» των social media που εκφράζουν την τάση του όχλου (mob mentality) να επιδίδεται στη διαδικτυακή καταδίκη ατόμων. Σε κάποιες περιπτώσεις μπορούν να επιφέρουν θετικά αποτελέσματα, πλην όμως, συνιστούν απειλή για τα δικαιώματα τρίτων ενέχοντας τον κίνδυνο να πλήξουν ανεπανόρθωτα την τιμή και την υπόληψη των εκτιθέμενων σε δημόσιο διασυρμό, καθώς επίσης, βάλλονται ευθέως κατά του τεκμηρίου αθωότητας.

[188] Οι διαδικτυακές επιθέσεις πλήττουν σε σημαντικό βαθμό ιδιωτικές επιχειρήσεις και ιδιοκτήτες των δομών που περιλαμβάνονται στην κριτική υποδομή.

hackback' (Kesan & Majuca 2009), όπως εμφανίζεται στη διεθνή βιβλιογραφία, που ενέχει την έννοια της ενεργητικής επανάληψης μιας ήπιας και αναλογικής διαδικτυακής αντεπίθεσης, εντοπιζόμενης στον πυρήνα της ενεργητικής άμυνας ως του μηχανισμού εκείνου που στοχεύει να αμβλύνει τον κίνδυνο, ήτοι να εξουδετερώσει την απειλή ('active threat neutralization') (Kesan & Hayes 2012: 474-485). Υπό το πρίσμα αυτό, τρία είναι τα στάδια που συνθέτουν το μηχανισμό ενεργητικής άμυνας αυτής της μορφής και αναλύονται α) στη χρήση της κατάλληλης τεχνολογίας για τον εντοπισμό του ηλεκτρονικού ίχνους (Intrusion Detection Systems-IDS), β) τεχνολογία για την ανίχνευση της επίθεσης στην πηγή της ('traceback') και γ) την ανάπτυξη δυνατοτήτων αντεπίθεσης τέτοιων που να περιλαμβάνουν τρόπους ανακατευθυνσης δεδομένων στο δράστη ώστε να ανακόπτεται η δρομολογημένη πορεία της επίθεσης και οι προς τούτο ενέργειες να ανακατευθύνονται στον πομπό (π.χ. STRATCOM) (Kesan & Hayes 2012: 474). Αυτά δε, με σκοπό την πρόληψη της ζημίας ex ante και συγχρόνως την καθιέρωση ενός σταθερού μοντέλου προστασίας που μπορεί να εφαρμοστεί σε περισσότερα συστήματα κατά το προληπτικό στάδιο (Majuca & Kesan 2009: 1-69).Οι επικριτές, ωστόσο, επισημαίνουν τους κινδύνους της νομιμοποίησης μιας καταστροφικής αυτοδικίας, η οποία εγείρει πολλαπλά ζητήματα όπως η βλάβη τρίτων μερών και ζητήματα Διεθνούς Δικαίου στο βαθμό που τέτοιες ενέργειες δύνανται να σηματοδοτήσουν κυβερνοπόλεμο. Επιπλέον προβληματική εγείρει το ερώτημα, του ποια θα είναι το νομιμοποιούμενα να εφαρμόσουν τέτοιες μεθόδους μέρη μεταξύ του κράτους και των ιδιωτικών φορέων.[189] Η πραγματικότητα, ωστόσο, δείχνει, ότι, παρά τις πολλαπλές προβληματικές, τέτοιες τεχνικές έχουν χρησιμοποιηθεί στην πράξη τόσο από κυβερνητικούς όσο και από ιδιωτικούς φορείς.[190] Δοθέντος, συνεπώς, του ήδη συμβαίνοντος, αντί της εθελοτυφλίας, η θεσμοθέτηση ενός νομικού πλαισίου που θα οριοθετεί τις επιτρεπόμενες ενέργειες από τους νομιμοποιούμενες φορείς, έχει υποστηριχθεί ως πιο αποτελεσματική λύση,[191] προλαμβάνοντας τη ζημία και

[189] Εκτιμάται ότι το 2012 περίπου το 80% των υποδομών κριτικής σημασίας των ΗΠΑ ανήκε στον ιδιωτικό τομέα.

[190] Όταν το 1998 το ακτιβιστικό γκρουπ Electronic Disturbance Theater επιτέθηκε στο Πεντάγωνο (DDoS), το Πεντάγωνο ανακατεύθυνε τις δεχόμενες εντολές στους αποστολείς τους (Biegel 2003: 242). Το 2002 ο Mullen, υπεύθυνος ανάπτυξης λογισμικού, ανέπτυξε μια τεχνολογία εξουδετέρωσης της επίθεσης που δέχθηκε στο σύστημα πληροφοριών ανακόπτοντας τον πολλαπλασιασμό του Code Red και των Nimda worms (Kesan & Hayes 2012: 476).

[191] Σε πρακτικό επίπεδο δεν πρέπει να παραβλέπεται η υπάρχουσα διάσταση ανάμεσα στην αδυναμία της αστυνομίας και των νομιμοποιούμενων φορέων να πράξουν άμεσα και της τεχνικής πραγματικότητας που προϋποθέτει χρόνο για την εξιχνίαση της επίθεσης, δοθείσης της ταχύτητας, ώστε ένα νομοθετικό πλαίσιο που θα λαμβάνει υπόψη τις υπάρχουσες ανάγκες και τις τεχνικές δυσκολίες, να είναι ικανότερο και

καθιερώνοντας συγχρόνως ένα σταθερό μοντέλο προστασίας ικανό να εφαρμοστεί σε επίπεδο πρόληψης. Στις περιπτώσεις, άλλωστε, ανεπαρκών νομοθετικών προβλέψεων, το ρίσκο χρησιμοποίησης παράνομων και δυνητικά επιβλαβών μεθόδων από τα εμπλεκόμενα μέρη μεγιστοποιείται (Karnow 2005: 89, 94, Katyal 2005: 61-62, Sklerov 2009: 7, 73). Σε κάθε περίπτωση τα μέσα που κρίνονται αναγκαία και αναλογικά[192] προς την επίτευξη του επιδιωκόμενου σκοπού, μπορούν να αποτελέσουν κοινωνικά προκρινόμενη λύση (Karnow 2005: 96-97, Katyal 2005: 43-54), εν τη απουσία πρακτικών εναλλακτικών λύσεων, δυνάμενων να προλάβουν την επαπειλούμενη δράση (Kesan & Majuca 2009).

iii) Η αυτοάμυνα υπό το πρίσμα του άρθρου 51 του Χάρτη Η.Ε.

Σε επίπεδο κρατών το δικαίωμα αυτοάμυνας και εφαρμογής αντιποίνων εντοπίζεται στο άρθρο 51 του Χάρτη των Ηνωμένων Εθνών[193] που νομιμοποιεί την ατομική ή συλλογική αυτοάμυνα[194] σε περιπτώσεις ένοπλης επίθεσης ('armed attack').[195] Ενδιαφέρον παρουσιάζει το ζήτημα του κατά πόσο στην έννοια της ένοπλης επίθεσης μπορούν να υπαχθούν, υπό προϋποθέσεις, κατηγορίες διαδικτυακών επιθέσεων τελούμενων από δράστες εκτός της επικράτειας του πληττόμενου κράτους, με στόχευση στις υποδομές κριτικής σημασίας του τελευταίου (Graham 2010: 93 σε Kesan 2012: 478-481). Ορισμένοι μελετητές επισημαίνουν την αναγκαιότητα ύπαρξης μιας ανώτερης

προτιμότερο έναντι κεκτημένων και σπασμωδικών κινήσεων που ενέχουν τον κίνδυνο να εκφύγουν των νομίμως επιτρεπόμενων ενεργειών (Katyal 2005).

[192] Η αρχή της αναλογικότητας εντοπίζεται στο άρθρο 22 ΠΚ που ορίζει ότι στο πλαίσιο της νόμιμης άμυνας είναι επιτρεπόμενη η αναγκαία προσβολή του επιτιθέμενου στην οποία προβαίνει το άτομο προς υπεράσπιση του εαυτού του ή άλλου από παρούσα και άδικη επίθεση που στρέφεται εναντίον του, ώστε το αναγκαίο μέτρο άμυνας πρέπει να τελεί σε εύλογη αναλογία με την επικινδυνότητα της επίθεσης, τον τρόπο και την έντασή της και το επαπειλούμενο έννομο αγαθό.

[193] *"Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."*

[194] Η νόμιμη αυτοάμυνα δύναται να δικαιολογηθεί όταν α) η απειλή ένοπλης επίθεσης είναι άμεση, β) όταν υπάρχει επιτακτική ανάγκη για αμυντική δράση, γ) όταν δεν υπάρχει άλλη ηπιότερη εναλλακτική επιλογή και δ) όταν η πράξη αυτοάμυνας περιορίζεται στα επιτρεπόμενα όρια αυτής (Jennings et al. 2008).

[195] Ο όρος 'armed attack' γίνεται δεκτός ως υποκατηγορία του όρου 'use of force' που χρησιμοποιείται στο άρθρο 24 του Χάρτη των Ηνωμένων Εθνών η οποία περιλαμβάνει μια σειρά από ενέργειες επίθεσης ('acts of aggression') με τις ένοπλες επιθέσεις να είναι οι εντονότερες. Σύμφωνα με τη Γενική Αμνηστία ο όρος «επίθεση» περιλαμβάνει τη χρήση ένοπλης δύναμης από ένα κράτος ενάντια στην κυριαρχία, την εδαφικότητα και την κυριότητά του ή την πολιτική του ανεξαρτησία ή οτιδήποτε άλλο έρχεται σε αντίθεση με το Χάρτη των Ηνωμένων Εθνών.

αρχής επιφορτισμένης με τον χαρακτηρισμό των εισβολών ως «ένοπλων επιθέσεων» (Sklerov 2009: 1-85). Το άρθρο 51 κατοχυρώνει το εγγενές δικαίωμα αυτοάμυνας, η χρήση του οποίου, ωστόσο, βρίσκει τα όριά της, στην αρχή της αναλογικότητας,[196] η οποία αναλύεται σε τρεις επιμέρους αρχές: την αρχή της αναγκαιότητας του ληφθέντος μέτρου για την επίτευξη του επιδιωκόμενου σκοπού, την αρχή της προσφορότητας στην επέλευση του αποτελέσματος και την αρχή της αναλογικότητας strict sensu[197] που πρεσβεύει ότι δεν υπάρχουν άλλα μέτρα λιγότερα ήπια και περισσότερο ικανά να οδηγήσουν στον επιδιωκόμενο σκοπό, άλλως, δεν υπάρχουν άλλα αποτελεσματικά ειρηνικά μέσα επίλυσης, αντλούμενα από τη φύση της επίθεσης, τις αντιρρήσεις των κρατών και την πιθανότητα αποτελεσματικής παρέμβασης της διεθνούς κοινότητας (Kesan 2012: 526). Σε ό, τι αφορά στο προληπτικό στάδιο, έχει υποστηριχθεί η προληπτική αυτοάμυνα στις περιπτώσεις που κρίνεται πως υπάρχει άμεση και επείγουσα ανάγκη και δε διαπιστώνεται άλλος τρόπος απάντησης ούτε χρόνος διαβούλευσης (‘Caroline doctrine’). Άλλη άποψη υποστηρίζει ότι το άρθρο 51 πρέπει αυστηρά να εφαρμοστεί ως απάντηση σε εκδηλούμενη ένοπλη επίθεση και όχι προληπτικά, οπότε σε επίπεδο διαδικτυακών επιθέσεων, όπου εξετάζεται η αναλογική εφαρμογή, η ζημιά θα έχει ήδη συντελεστεί (Kesan 2012: 528). Τέλος, ενδιαφέρουσα είναι η άποψη του Schmitt που υποστηρίζει την προληπτικά επιτρεπόμενη αυτοάμυνα πληρουμένων τριών προϋποθέσεων: α) η επίθεση αποτελεί μέρος ενός συνολικού σχεδιασμού που κατατείνει σε ένοπλη επίθεση, β) η επίθεση κρίνεται αναπόφευκτη (‘irrevocable step’) και γ) η προληπτική απάντηση στην επίθεση λαμβάνει χώρα την τελευταία δυνατή στιγμή που χωρεί αντιμετώπιση.

3.7.3 Διαμόρφωση προτιμήσεων (‘Preference-shaping Theory’)

i) ‘Hacker Ethic’

Η έννοια της διαμόρφωσης προτιμήσεων (‘Preference-shaping Theory’) περιγράφει τη δημιουργία ενός μοντέλου παροχής θετικών κινήτρων που συντείνει στην προσαρμογή μιας υφιστάμενης δράσης εντός ενός κοινωνικώς αποδεκτού πλαισίου, ενός

[196] Προς τον σκοπό αποφυγής της ανταποδοτικής ή τιμωρητικής αντεπίθεσης που εκφεύγει από τα όρια του θεμιτού.
[197] Η αναγκαιότητα (‘necessity’) και η αναλογικότητα (‘proportionality’) συναντώνται στο jus in bello, ενώ υπό την ισχύ του jus ad bellum απαιτείται και η προϋπόθεση της αμεσότητας (‘immediacy’)

πλαισίου νομιμότητας (Dau-Schmidt 1990: 17-24). Πρόκειται για μια ιδέα εμπνευσμένη από την πρώιμη ηθική των hackers ('hacker ethic') που βασίζεται στη περιορισμένη και υπό συγκεκριμένες προϋποθέσεις αποποινικοποίηση του hacking – ορισμένοι μελετητές, ωστόσο, έχουν υποστηρίξει ότι η αποποινικοποίηση θα ήταν αναποτελεσματική, καθώς πιθανώς να αποσταθεροποιούσε την έννομη τάξη, γι' αυτό και μπορεί να γίνει λόγος μόνο για μετριασμένη αποποινικοποίηση- εντός ενός διαυγούς πλαισίου που θα οριοθετεί τα επιτρεπόμενα όρια δράσης και θα συνοδεύεται από την παροχή ανταμοιβών. Εξετάζοντας τη σημασία της ανταμοιβής από φιλοσοφική σκοπιά, φαίνεται πως, περισσότερο ίσως και από την τιμωρία, η ανταμοιβή μπορεί να διαδραματίσει καθοριστικό ρόλο στο σχηματισμό κοινωνικής συνείδησης, ως έτερος αποτρεπτικός παράγοντας που ενθαρρύνει το σχηματισμό μιας κοινωνικοηθικά αποδεκτής νοοτροπίας.[198] Το ζητούμενο, επομένως, εντοπίζεται στην παροχή θετικών κινήτρων μέσω ανταμοιβών που εντείνουν το αίσθημα ελευθερίας και αυτοβελτίωσης οδηγώντας σε υψηλότερα ποσοστά συμμόρφωσης χάρη στην υπεισέλευση θετικών στοιχείων (Eisenberger & Rhoades 2001). Μόνη δε η τιμωρία, εμπειρικά αποδεικνύεται πως δεν είναι πάντοτε ικανή να διορθώσει την παρεκκλίνουσα συμπεριφορά. Οι κοινωνικές επιστήμες παρατηρούν ότι η τιμωρία δε λειτουργεί ως ισχυρός αποτρεπτικός παράγοντας στην περίπτωση των φερόντων εγκληματική προδιάθεση (Lombroso: *The criminal Man*. 1876) ή των «ηθικά αδέσμευτων» (Piliavin 1986: 101, 117), καθώς επίσης, σε ορισμένες περιπτώσεις δεν αποκλείεται η όξυνση παρεκκλινουσών συμπεριφορών,[199] κατά τη γενική παραδοχή ότι όταν κάποια/ος ζει σε ένα περιβάλλον που την/ον αντιμετωπίζει ως εγκληματία είναι περισσότερο πιθανό να παρανομήσει. Εστιάζοντας, επομένως, στην ανθρώπινη συμπεριφορά, η προσπάθεια διαμόρφωσης μιας σύγχρονης κουλτούρας, μέσω της συνύπαρξης του ποινικού πλαισίου και των θετικών κινήτρων, μπορεί να εξεταστεί ως ένας πιθανός τρόπος απαλοιφής ή έστω περιορισμού των αρνητικών προεκτάσεων του Διαδικτύου (Wible 2003: 1590-1592).

[198] Κατά τον άγγλο φιλόσοφο Jeremy Bentham (σε Draper 2002: 1-17) το μεγαλύτερο ρίσκο έγκειται σε μια ποινική απαγόρευση ανεπαρκώς τιμωρητική παρά υπερβολικά τιμωρητική.
[199] Αυτό μπορεί να επιτύχει για παράδειγμα ο στιγματισμός με την περιθωριοποίηση του δράστη και την αναγκαστική προσφυγή του σε γνώριμες μεθόδους δράσης μέσω των οποίων αυτοολοκληρώνεται.

ii) 'Hack-in' διαγωνισμοί

Μια πρόταση που ήδη εφαρμόζεται, στο πλαίσιο αυτής της προσέγγισης, είναι η ενίσχυση διαγωνισμών 'hack-in' (Black Hat, DEFCON)[200] διεξαγόμενων από παρόχους υπηρεσιών Διαδικτύου και εταιρείες παροχής λογισμικού ή εξοπλισμού υπολογιστών με διττό σκοπό: α) τον εντοπισμό των αδυναμιών των συστημάτων ασφαλείας προ της θέσης τους σε κυκλοφορία και β) τη δημιουργία μιας θετικής αγοράς για την ανάπτυξη ικανοτήτων hacking προς αποτροπή ή μείωση της επιβλαβούς δραστηριοποίησης. Οι διαγωνισμοί αυτοί, συνοδευόμενοι από χρηματικά έπαθλα[201] και αναγνωρισιμότητα στο ευρύ κοινό, στοχεύουν στην εκτόνωση των hackers, οι οποίοι έτσι εμφανίζουν ένα ισχυρό κίνητρο να συμμετάσχουν, αποκαλύπτοντας, συγχρόνως, τα στοιχεία τους και συνδράμοντας, παράλληλα, στην αξιοποίηση των ειδικών ικανοτήτων τους προς το συλλογικό όφελος. Για δε τις διοργανώτριες εταιρείες, άλλοτε λειτουργούν ως τρόπος διαφήμισης του απαραβίαστου των υπηρεσιών τους (Morris 2018) και άλλοτε διαδραματίζουν καταλυτικό ρόλο στην ενίσχυση του λογισμικού των προσβαλλόμενων συστημάτων και την ισχυροποίηση των μηχανισμών ασφαλείας των φορέων παροχής υπηρεσιών ζωτικής σημασίας απέναντι στις απειλές του κυβερνοχώρου. Η ομαλή διεξαγωγή προϋποθέτει βέβαια επαρκή μέτρα για τη διασφάλιση των εμπιστευτικών πληροφοριών και την αποφυγή της αποκάλυψης των ευπαθειών στο ευρύ κοινό.[202] Ενδεικτικά μέτρα που έχουν προταθεί είναι η αποσύνδεση των εμπιστευτικών πληροφοριών από τα προσβάσιμα δεδομένα και η συμβολαιογραφική δέσμευση των νικητών να αποκαλύψουν τις διαπιστωθείσες αδυναμίες αποκλειστικά στους διενεργούντες το διαγωνισμό με παράλληλη εξασφάλιση της επωνυμίας του συμμετέχοντα (Lewis 2004: 1369-1370). Επιτακτική καθίσταται και η διασφάλιση της βελτίωσης των διαπιστωθεισών αδυναμιών. Στην πράξη τέτοιοι διαγωνισμοί λαμβάνουν χώρα ήδη επί μακρόν, πολλοί εκ των οποίων διεξάγονται σε ετήσια βάση αποσκοπώντας στην εύρεση νέων ταλέντων που θα αξιοποιηθούν στην μάχη κατά του

[200] Στην ιστοσελίδα hackaday.com για παράδειγμα καλούνται πάντες ενδιαφερόμενοι να μοιραστούν τις γνώσεις τους σε σχέση με το hacking και να ενημερωθούν για τους εν εξελίξει διαγωνισμούς, όπου μπορούν να συμμετάσχουν. Αναλυτικά: https://hackaday.com/about/

[201] Το 2019 η Google ανακοίνωσε ότι θα προσέφερε 1,5 εκατ. δολάρια σε όποιον επιτύγχανε να χακάρει συστήματα Android (Holmes 2019). Το 2013 ανακοίνωσε έπαθλο άνω των 3 εκατ. δολαρίων σε όποιον κατάφερνε να παραβιάσει τα συστήματα του Chrome (Greenberg 2013).

[202] Το 2002 ο καθηγητής του Princeton Edward W. Felten κέρδισε έναν διαγωνισμό παρακάμπτοντας τα συστήματα προστασίας ψηφιακής μουσικής. Λίγο αργότερα δημοσίευσε εργασία στην οποίο εξηγούσε πώς έσπασε τον κώδικα.

κυβερνοεγκλήματος ('European Cyber Security Challenge').[203] Η διοργάνωση διαγωνισμών αυτού του είδους, επομένως, είναι πραγματικότητα, πλην όμως, ελλείψει σχετικού νομοθετικού πλαισίου, ελλοχεύουν οι κίνδυνοι εμπλοκής σε αυθαίρετο hacking, το οποίο, μπορεί μεν σε ορισμένες περιπτώσεις να αποδειχθεί καλόηθες, δεν αποκλείεται, ωστόσο, σε ορισμένες άλλες περιπτώσεις, να αποδειχθεί επιζήμιο, δημιουργώντας επιπρόσθετα κόστη ασφάλειας και παρακολούθησης (Wible 2003: 1594).

iii) Το μοντέλο

Ο σχεδιασμός ενός διαγωνισμού κατάλληλου να διαμορφώσει προτιμήσεις, χωρίς να ενέχει τους ανωτέρω κινδύνους, πρέπει να πληροί ορισμένες προϋποθέσεις, διακρίνοντας, κατ' αρχήν, ανάμεσα στο κοινωνικώς αποδεκτό hacking και εκείνο που βρίσκεται εκτός του πλαισίου νομιμότητας. Δεύτερον, για να προσελκύσει ενδιαφερόμενους πρέπει να διαφημίζεται με τέτοιο τρόπο που να εστιάζει την προσοχή στην παροχή θετικών κινήτρων, βασιζόμενης της επιτυχίας του μοντέλου στη συμμετοχή της μεγαλύτερης κατά το δυνατόν μερίδας hackers και λοιπών φορέων[204], οι οποίοι αναμένεται να ωφεληθούν αμοιβαία από την ανταλλαγή πληροφοριών. Στη διαμόρφωση θετικών κινήτρων μέσα από τη δημιουργία των κατάλληλων συνθηκών, ο ρόλος του κράτους είναι σημαντικός.[205] Στη βάση της αναζήτησης θετικών κινήτρων, μια πρόταση είναι κάθε διαγωνισμός να χωρίζεται σε επιμέρους δοκιμασίες για τις οποίες θα δημοσιεύεται ένα σύστημα αξιολόγησης (π.χ. top 100), ώστε όλοι οι συμμετέχοντες να έχουν το κίνητρο της αναγνωρισιμότητας,[206] ενώ η ανταμοιβή των νικητών πέρα από χρηματικά έπαθλα μπορεί να συνίσταται σε εργασιακές ευκαιρίες (Wible 2003: 1604). Σε ό, τι αφορά στους συμμετέχοντες φορείς, τα θετικά κίνητρα μπορούν να λάβουν τη μορφή φορολογικών ελαφρύνσεων ή μείωσης των ασφαλιστικών εισφορών τους προκειμένου να ελαχιστοποιηθεί το κόστος συμμετοχής (Wible 2003: 1597). Πέρα από

[203] Βλ. https://europeancybersecuritychallenge.eu/ και https://e-estonia.com/cyber-exercise-for-private-sector-tallinn/

[204] Οι φορείς μπορούν να αναφέρονται ονομαστικά είτε να παραμένουν ανώνυμοι. Για να αποφευχθεί το πρόβλημα της ενδεχόμενης προσβολής μη συμμετέχοντος φορέα, οι φορείς που δε θα συμμετέχουν στο διαγωνισμό θα μπορούσαν να εμφανίζουν στις ιστοσελίδες τους προειδοποιήσεις ότι τυχόν παραβίαση επισύρει κυρώσεις.

[205] 'Because cybercrime is so easy to commit and much of the knowledge needed to make it more difficult resides in private hands, government must devise methods to extract such information from criminals.' (Katyal σε Wible 2003: 1595).

[206] Έρευνα του Boston Consulting Group του 2002 σχετικά με τα κίνητρα των hackers έδειξε ότι τα διανοητικά ερεθίσματα και η βελτίωση των τεχνικών ικανοτήτων ήταν τα κύρια κίνητρα της εγκληματικής δράσης.

τη μείωση του κόστους συμμετοχής, καταλυτικός πρέπει να είναι ο ρόλος του κράτους στη δημιουργία κατευθυντηρίων οδηγιών προς τις οποίες πρέπει να συμμορφώνονται όλοι οι διαγωνιζόμενοι, οριοθετώντας το πλαίσιο νομότυπης δράσης των συμμετεχόντων ιδιωτικών φορέων, διασφαλίζοντας, ως εκ τούτου, την τιμωρία των παραβατών. Μόνη η διεξαγωγή τέτοιων διαγωνισμών δε μπορεί να γίνει δεκτό ότι θα εξαλείψει φαινόμενα όπως το αθέμιτο hacking,[207] είναι πολύ πιθανό κοινωνιολογικά, ωστόσο, υπό την εποπτεία του κράτους και τη δημιουργία ενός νομοθετικού πλαισίου ανταποκρινόμενου σε αυτό το μοντέλο, να οδηγήσει στη διαμόρφωση προτιμήσεων για τους επίδοξους hackers[208] όσο και στην ισχυροποίηση των συστημάτων των συμμετεχόντων φορέων.[209] Σίγουρα τα ακριβή αποτελέσματα αυτών των μεθόδων είναι αμφισβητούμενα, καθώς επίσης, αυτού του είδους οι στρατηγικές περιορίζονται σε συγκεκριμένες κατηγορίες εγκλήματος ούσες αδόκιμες σε περιπτώσεις άλλων κατηγοριών εγκλήματος, όπως π.χ. η παιδική πορνογραφίας ή η απάτη (Grabosky 2016: 120-122). Παρά ταύτα, ακόμη και υπό αυτή τη σκέψη, αν γίνουν δεκτά πιθανά ευεργετικά αποτελέσματα σε αυτά περιλαμβάνεται η αποδέσμευση πόρων που χρησιμοποιούνται στην καταπολέμηση αδικημάτων αυτής της μορφής και αναδιανομή τους με γνώμονα την αντιμετώπιση λοιπών μορφών αδικημάτων.

3.8 Στην κατεύθυνση μιας ορθής κουλτούρας

3.8.1 Δημόσια αφύπνιση

Οι προκλήσεις που φέρνει στο προσκήνιο η τεχνική βελτίωση των δραστών απαιτεί τόσο τα μεμονωμένα άτομα όσο και οι επιχειρήσεις να βρίσκονται σε διαρκή ενημέρωση για τους κινδύνους που αντιμετωπίζουν, διατηρώντας την ικανότητά τους να αποτρέψουν τις προσβολές όπου είναι εφικτό και ταυτόχρονα να απαντήσουν στις

[207] Θα μπορούσε να ειπωθεί ότι η αλληλεπίδραση κόστους και ανταμοιβής που καθορίζει την ανθρώπινη συμπεριφορά στο επίπεδο του ανωτέρω μοντέλου αποτελεί υποκατάστατο (substitute) των ποινικών κυρώσεων. Και υπό τη σκέψη ότι μέρος των hackers είναι εθισμένο στη διάπραξη τοιαύτων ενεργειών, η προσφορά ενός αβλαβούς υποκατάσταστου (harmless substitute) είναι προτιμότερη λύση έναντι του ακώλυτου παράνομου hacking (Wible 2003: 1620)

[208] Ανάλογη προσέγγιση εφαρμόστηκε στη Φιλαδέλφεια των ΗΠΑ με σκοπό τον περιορισμό των graffiti. Με τη διοργάνωση προγραμμάτων ενίσχυσης της τοιχογραφίας και εξεύρεσης νέων καλλιτεχνών, δόθηκε κίνητρο στους συμμετέχοντες να καλύψουν τα υπάρχοντα graffiti με τοιχογραφίες και να συμφωνήσουν να απέχουν από αυθαίρετους σχεδιασμούς σε βάρος της ιδιοκτησίας τρίτων (Brown 2000).

[209] Πέραν της διαπίστωσης των τρωτών σημείων τους, έρευνες αποδεικνύουν ότι η ίδια η συμμετοχή σε διαγωνισμούς που περιλαμβάνουν πληροφορίες για συστήματα ασφαλείας καθιστά τους συμμετέχοντες λιγότερο επιρρεπείς σε κακόβουλες επιθέσεις (Hafner & Biggs 2003 σε Wible 2003: 1597).

προσβολές που λαμβάνουν χώρα. Με όρους προσφοράς και ζήτησης, οι προοπτικές μείωσης των διαθέσιμων παραβατών είναι περιορισμένες δοθέντος ότι τα κίνητρα πολλών μορφών ηλεκτρονικού εγκλήματος είναι βαθιά εδραιωμένα στην ανθρώπινη συμπεριφορά. Από την άλλη, ο περιορισμός της πρόσβασης στην τεχνολογία αποτελεί μη ρεαλιστική υπόθεση και σαφώς μη θεμιτή. Στο πλαίσιο αυτό και ενόψει της νέας πραγματικότητας, κρίνεται επιβεβλημένη η προώθηση μιας κουλτούρας ορθής χρήσης του Διαδικτύου από τους χρήστες και η αναμόρφωση των αξιών της κοινωνίας σε επίπεδο Διαδικτύου, στόχοι που μέχρι στιγμής προωθήθηκαν στο πλαίσιο ανεπίσημων διαδικασιών. Καταλυτικό ρόλο σε αυτό οφείλει να έχει το κράτος χωρίς να παραβλέπεται η αναγκαιότητα συνεργασίας επιμέρους φορέων. Το ρόλο της στη μάχη κατά του ηλεκτρονικού εγκλήματος έχει η αναγκαιότητα δημόσιας αφύπνισης σχετικά με τους κινδύνους που εγείρει ο διαδικτυακός χώρος. Κοινή διαπίστωση αποτελεί άλλωστε το πεπερασμένο της ικανότητας του κράτους να ελέγξει το χώρο του Διαδικτύου. Η ενημέρωση επομένως των χρηστών για τη σωστή χρήση του Διαδικτύου και τους ελλοχεύοντες κινδύνους είναι αναγκαία και θέτει τις πρώτες βάσεις στη δημιουργία της κουλτούρας του Διαδικτύου και τον περιορισμό των επιπτώσεων φαινομένων εγκληματικής συμπεριφοράς. Φαινόμενα grooming για παράδειγμα μπορούν να ελαχιστοποιηθούν με την ορθή εκπαίδευση των υποψήφιων θυμάτων, τα οποία οι γονείς είναι δύσκολο να ελέγχουν κατά την πλοήγησή τους, αλλά και με την ενημέρωση των γονέων για τη σωστή γαλούχηση των παιδιών τους.[210] Άλλη μορφή που μπορεί να λάβει η ζητούμενη αφύπνιση είναι αυτή της ειδοποίησης των Τραπεζών για ύποπτες συναλλαγές (Grabosky 2016: 122-124). Η έννοια της επιδιωκόμενης αφύπνισης, συνεπώς, εκτείνεται σε πλείονα επίπεδα συσχετιζόμενη με την εκπαίδευση, τη δημιουργία σχετικών προγραμμάτων και ενημερωτικών δράσεων από εξειδικευμένους φορείς.

3.8.2 Παροχή κινήτρων στα υποψήφια θύματα

Μέθοδο εδραίωσης κοινωνικά θεμιτών συμπεριφορών και πρόληψης μπορεί να αποτελέσει η παροχή κινήτρων σε δυνητικά θύματα προκειμένου να αποτρέψουν ή να

[210] Παράδειγμα η ΜΚΟ SafetyGroup στη Ν. Ζηλανδία που παρέχει πληροφορίες σε παιδιά και γονείς.

περιορίσουν τον επαπειλούμενο κίνδυνο.[211] Σύμφωνα με μια πρόταση οι αρμόδιες αρχές θα μπορούσαν να ασκούν κατά προτεραιότητα διωξη για τα εγκλήματα στα οποία τα θύματα έλαβαν τα πρόσφορα για την προστασία τους μέτρα, παρά ταύτα, αυτά απέβησαν ατελέσφορα. Το επιχείρημα υπέρ της άποψης αυτής είναι η αξιοποίηση των λιγότερων δυνατών πόρων από την πλευρά του κρατικού μηχανισμού – έχει ήδη επισημανθεί το πεπερασμένο των πόρων και η αναγκαιότητα αποτελεσματικής κατανομής τους στην παραγωγική διαδικασία και ειδικότερα στην αποτελεσματική λειτουργία του ποινικού μηχανισμού (Katyal 2001: 1080) – και η ευσυνειδησία των δυνητικών θυμάτων σχετικά με τη διασφάλιση της ατομικής τους προστασίας έναντι μελλοντικών προσβολών. Από την άλλη πλευρά, είναι αμφίβολο το αν η τακτική αυτή δύναται να ενθαρρύνει πράγματι τους χρήστες να προβούν στη λήψη των αναγκαίων προληπτικών μέτρων, στους οποίους, κατά τους επικριτές της αυτής πρότασης, μετατίθεται το βάρος που παραδοσιακά ανήκει στο κράτος.[212] Πρόσθετα, η από τους χρήστες πιστή υπακοή στις απαιτήσεις του δικτύου, ήτοι στις κρατικές προβλέψεις που στοχεύουν στην αναγωγή της προστασίας των υποψήφιων θυμάτων σε δημόσιο αγαθό, συνεπάγεται έναν έτερο κίνδυνο. Η ίδια η γενικευμένη αίσθηση προστασίας ενέχει ταυτόχρονα τον κίνδυνο ορισμένοι χρήστες να εφησυχάσουν και να αρκεστούν στις ευεργετικές επιπτώσεις των ληφθέντων από τους άλλους χρήστες μέτρων (‘free rider problem’).[213] Φυσικά πιθανή τέτοια εξέλιξη είναι αυτονόητο ότι δεν εξασφαλίζει τον επιθυμητό βαθμό προστασίας και προσθέτει επιπλέον διαχειριστικά κόστη (Lewis 2004: 1363-1364). Η δημόσια αφύπνιση και η σωστή εκπαίδευση διαδραματίζουν τον κύριο ρόλο στην καλλιέργεια μιας ορθής κουλτούρας ασφαλούς χρήσης.

[211] Στον πραγματικό κόσμο μια αναλογία είναι η παροχή κινήτρων στα υποψήφια θύματα προκειμένου να κλειδώνουν τις πόρτες της οικίας τους και να υποχρεωθούν σε εγκατάσταση συστήματος συναγερμού προς αποτροπή των κλοπών.

[212] Η μετάθεση του βάρους γεννά σειρά από ηθικούς προβληματισμούς που αφορούν στην επίρριψη ευθυνών στο θύμα (‘blame-the-victim-strategy’).

[213] Η έννοια αναφέρεται στο οικονομικό και πολιτικό φαινόμενο ορισμένοι να επωφελούνται από δημόσια αγαθά χωρίς, όμως, να καταβάλλουν το μερίδιο που τους αναλογεί, με αποτέλεσμα την πρόκληση του μη βέλτιστου τελικώς αποτελέσματος για το σύνολο, το οποίο ανακόπτεται από την παρείσφρηση ατομικών συμφερόντων έναντι του συλλογικού συμφέροντος.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Αναμφίβολα οι νέες τεχνολογικές δυνατότητες και η εισχώρηση του Διαδικτύου στις περισσότερες εκφάνσεις της καθημερινότητας εγκαινίασαν μια νέα εποχή που στα μάτια παλαιότερων θα φάνταζε σενάριο επιστημονικής φαντασίας. Ουδόλως πρέπει να απαρνηθούμε τα αδιαμφισβήτητα πλεονεκτήματα της τεχνολογίας από την οποία σκοπός πρέπει να είναι η άντληση του μεγαλύτερου δυνατού οφέλους σε ατομικό και κοινωνικό επίπεδο. Παρά ταύτα, η ψηφιακή εποχή ανέδειξε και αρνητικά τεχνολογικά φαινόμενα με σημαντικότερο το ηλεκτρονικό έγκλημα, ο ευρύς οικονομικός και κοινωνικός αντίκτυπος του οποίου, το ανήγαγε σε κοινωνικό φαινόμενο που δε γνωρίζει σύνορα. Ο όρος «ηλεκτρονικό έγκλημα» καταλαμβάνει πολλές επιμέρους μορφές εγκληματικής δραστηριότητας, κάποιες εκ των οποίων συνιστούν μετάλλαξη των παραδοσιακών εγκλημάτων, η διάπραξη των οποίων κατέστη πρόσφορη χάρη στα μοναδικά χαρακτηριστικά του Διαδικτύου, και άλλες αποτελούν ολότελα νέες μορφές εγκληματικής δράσης, οι οποίες γεννήθηκαν στο χώρο του Διαδικτύου. Τόσο δε τα εγγενή χαρακτηριστικά του ψηφιακού χώρου όσο και η εφευρετικότητα των δραστών, αναδεικνύουν διαρκώς νέες προεκτάσεις της εγκληματικής δράσης επισύροντας νομοθετικές και τεχνολογικές προκλήσεις στη μάχη ενάντια στην καταπολέμησή τέτοιων φαινομένων.

Ο τεράστιος οικονομικός και κοινωνικός αντίκτυπος και ο διασυνοριακός χαρακτήρας του ηλεκτρονικού εγκλήματος, όπως αποδεικνύουν τα εμπειρικά παραδείγματα, είναι γεγονός, απαιτεί δε, συντονισμένες προσπάθειες σε πολλά επίπεδα. Προς τούτο συνηγορεί ο ίδιος ο χαρακτηρισμός του ως κοινωνικού φαινομένου συνώνυμου της σύγχρονης εποχής που τροφοδοτείται από την εξέλιξη της τεχνολογίας. Δοθέντος ότι η τεχνολογία δε θα πάψει να εξελίσσεται είναι εύλογη η υπόθεση ότι και το ηλεκτρονικό έγκλημα, κατά συνέπεια, δε θα πάψει να εξελίσσεται, αντιθέτως, θα εμφανίζεται ακόμη πιο σύνθετο και απειλητικό εξακολουθώντας να εκπλήσσει. Το ζήτημα που επιχειρήθηκε να απαντηθεί με την παρούσα μελέτη αφορά στους τρόπους με τους οποίους θα κατορθώσουμε να μεγιστοποιήσουμε τις αντλούμενες ωφέλειες και ταυτόχρονα να ελαχιστοποιήσουμε τις αρνητικές-δηλητηριώδεις επιδράσεις δικτύου. Στο πλαίσιο αυτό, πρέπει να επισημανθεί ότι το Δίκαιο τείνει να μην προσαρμόζεται άμεσα και αποτελεσματικά στην κοινωνική αλλαγή, ατενίζοντας τα νέα φαινόμενα με αργούς και προσεκτικούς ρυθμούς, πλην όμως, οι ιδιαίτερες δυσκολίες στην αντιμετώπιση του

ηλεκτρονικού εγκλήματος, τόσο σε επίπεδο εξιχνίασης των δραστών όσο και πρόληψης νέων εγκληματικών δράσεων, απαιτούν ταχείες και στοχευμένες ενέργειες από περισσότερους φορείς με παράλληλη ανάπτυξη των κατάλληλων νομοθετικών εργαλείων και πρακτικών.

Υπό τις σκέψεις αυτές, η γράφουσα φρονεί ότι, η εναρμόνιση των νομικών συστημάτων είναι αναγκαία συνθήκη, όχι όμως επαρκής για την καταπολέμηση του φαινομένου. Πρώτο προαπαιτούμενο είναι η ολοκληρωμένη διεθνής εναρμόνιση σε ουσιαστικό και δικονομικό επίπεδο και η ενίσχυση των αρμόδιων αρχών με τα κατάλληλα νομοθετικά και τεχνολογικά εργαλεία για την εξιχνίαση και την έρευνα, οι οποίες μολονότι, μοιράζονται κοινά στοιχεία με τις διαδικασίες που ακολουθούνται στα παραδοσιακά εγκλήματα, εμφανίζουν ιδιαιτερότητες που χρήζουν ειδικής μεταχείρισης. Πολλές ποινικές υποθέσεις στηρίζονται στη βάση των ψηφιακών αποδείξεων, πλην όμως, οι τελευταίες, σε αντίθεση με τις αποδείξεις του πραγματικού κόσμου αποτελούν ευμετάβλητα και φθαρτά στοιχεία επιρρεπή στη διαγραφή ή τροποποίηση. Στον ψηφιακό κόσμο, οι δράστες μπορούν εύκολα να αποκρύψουν την ταυτότητά τους μέσα από ανώνυμες υπηρεσίες και τεχνικές κρυπτογράφησης τελώντας την αξιόποινη πράξη από την οικία τους. Το δε αξιόποινο αποτέλεσμα μπορεί να επέλθει και σε άλλη ήπειρο. Εύκολα γίνεται αντιληπτό ότι πρόκειται για κατ' εξοχήν έγκλημα εξ αποστάσεως. Ως εκ τούτου, ο τόπος εκδήλωσης της συμπεριφοράς του δράστη διαφέρει από τον τόπο εκδήλωσης του αξιόποινου αποτελέσματος. Η ιδιαιτερότητα του τόπου τέλεσης του εγκλήματος στον ψηφιακό χώρο είναι επομένως μια βασική προβληματική που εγείρει ζητήματα δικαιοδοσίας μεταξύ των εμπλεκόμενων κρατών και καθιστά περισσότερο επιτακτική την αναγκαιότητα συνεργασίας και αποτελεσματικής ανταλλαγής πληροφοριών πέρα από τα στενά όρια των μεμονωμένων κρατών μέσα από την παράλληλη δράση δημόσιων και ιδιωτικών φορέων, μεταξύ των οποίων οι δεύτεροι συνήθως υπερέχουν σε τεχνολογικές γνώσεις και τεχνικές ασφαλείας συστημάτων. Η προώθηση της συνεργασίας μεταξύ δημοσίων και ιδιωτικών φορέων, συνεπώς, είναι ουσιώδους σημασίας εφόσον δύναται να ενισχύσει τόσο το έργο της εξιχνίασης των δραστών όσο και να συντείνει στην πρόληψη εγκληματικών φαινομένων.

Στην κατεύθυνση της συλλογικής αντιμετώπισης και με όραμα τη θεμελίωση ενός παγκόσμιου εγχειρήματος εναρμόνισης των επιμέρους εθνικών νομοθεσιών στη μάχη ενάντια σε έναν ισχυρό εχθρό, τα κράτη μέλη της Ευρωπαϊκής Ένωσης και τέσσερις

χώρες παρατηρητές προχώρησαν το 2001 στην υπογραφή της Σύμβασης της Βουδαπέστης που αποτελεί το μοναδικό διεθνές κείμενο που επιχειρεί να ρυθμίσει καίρια ζητήματα Ουσιαστικού και Δικονομικού Δικαίου με σκοπό την ενίσχυση της αποτελεσματικής συνεργασίας σε ευρύτερο επίπεδο, παρέχοντας χρήσιμα εργαλεία ειδικά προσαρμοσμένα στις νέες απαιτήσεις. Μολονότι η Σύμβαση έχει πλέον επικυρωθεί από αρκετά κράτη, τα οποία έχουν εισαγάγει σχετικές ρυθμίσεις στο εγχώριο νομοθετικό τους σύστημα, η προβληματική παραμένει, εδραζόμενη αφενός στις διαφοροποιήσεις των εθνικών νομικών συστημάτων των συμβαλλόμενων κρατών και αφετέρου, στην απουσία σχετικών νομοθετικών προβλέψεων ή ύπαρξη ατελών νομοθετικών ρυθμίσεων σε σημαντικό τμήμα του χάρτη. Σύμφωνα με τα επικαιροποιημένα στοιχεία της UNCTAD όσον αφορά στη σχετική με το ηλεκτρονικό έγκλημα νομοθεσία σε παγκόσμια εμβέλεια, το 73% το χωρών παγκοσμίως διαθέτουν νομοθετικές προβλέψεις και το 9% επεξεργάζονται τη θέσπιση σχετικών προβλέψεων, πλέον τούτου όμως, διαπιστώνεται η ολική ανυπαρξία ρυθμίσεων σε ένα διόλου αμελητέο ποσοστό του 18%, ενώ για το 1% δεν υπάρχουν καθόλου στοιχεία.

Τα στατιστικά δεδομένα δημιουργούν πολύ μεγαλύτερη ανησυχία σε ό, τι αφορά την οικονομική και κοινωνική αποτύπωση της συνολικής βλάβης που προκαλείται σε ευρύτερο επίπεδο από το ηλεκτρονικό έγκλημα, πολλώ δε μάλλον, εκ του γεγονότος ότι τα στοιχεία δεν είναι ακριβή, καθότι τα θύματα, στα οποία περιλαμβάνονται μεμονωμένα άτομα, επιχειρήσεις, ιδιωτικοί και κρατικοί φορείς εμφανίζονται συχνά διστακτικά στην καταγγελία των σχετικών περιστατικών στρεφόμενα συχνά σε λύσεις αυτοδικίας. Συνεπώς, προκρίνεται η σκέψη ότι η στενή προσκόλληση σε παραδοσιακές συνταγές, καθώς φαίνεται, δεν είναι αρκετή για να αντιμετωπιστούν αποτελεσματικά οι τεράστιες επιπτώσεις του ηλεκτρονικού εγκλήματος και οι κατ' επέκταση αρνητικές διαστάσεις του Διαδικτύου, σε αναφορά με την αντιμετώπιση των οποίων έχουν υποστηριχθεί κατά καιρούς σενάρια αυτορρύθμισης του διαδικτυακού χώρου. Κατά τη γράφουσα, θεωρείται σημαντική η αξιοποίηση των εργαλείων και των μεθόδων που παρέχει ο διαδικτυακός χώρος και η ενδελεχής μελέτη του τρόπου λειτουργίας του Διαδικτύου από τον οποίο δύνανται να αντληθούν γόνιμες σκέψεις και συμπεράσματα. Ειδικότερα, μπορεί να προκριθεί μια ειδική sui generis νομοθετική μεταχείριση του ηλεκτρονικού εγκλήματος, ικανή να ανταποκριθεί στις τεχνολογικές συνθήκες και αρκετά φιλόδοξη ούτως ώστε να μπορεί να αντιμετωπίσει καταλλήλως τις ακόμη πιο εξελιγμένες μελλοντικές απειλές. Στο πλαίσιο αυτό, σκόπιμη είναι η διεπιστημονική προσέγγιση με την αξιοποίηση

μεθοδολογικών εργαλείων αντλούντων τη δυναμική τους από τα ευρήματα περισσότερων επιστημονικών κλάδων.

Πρόσθετο ρόλο στη διαμόρφωση ενός ολοκληρωμένου μοντέλου δύνανται να έχουν τα εργαλεία της Οικονομικής Ανάλυσης του Δικαίου, ως μεθόδου που αποσκοπεί στην εύρεση αποτελεσματικών και κοινωνικά βέλτιστων λύσεων συνεπικουρώντας το έργο του Δικαίου. Υπό αυτή την έννοια η δυναμική αυτών των εργαλείων μπορεί να συμβάλει στην εκδήλωση της προληπτικής λειτουργίας του Ποινικού Δικαίου και το μετριασμό των αποδοκιμαζόμενων φαινομένων που εξετάζονται. Οι εκφάνσεις του ηλεκτρονικού εγκλήματος είναι πολλές, ορισμένες εκ των οποίων αποτελούν αμιγώς νέες μορφές και ορισμένες άλλες συνιστούν τη μετάλλαξη γνώριμων μορφών του παραδοσιακού Ποινικού Δικαίου, πλην όμως, τα νέα χαρακτηριστικά τους ανάγονται στους ήδη γνωστούς προσδιοριστικούς παράγοντες την ανθρώπινης συμπεριφοράς, που ισοδυναμούν με τα κίνητρα που υποκινούν την εγκληματική δραστηριότητα.

Με αφετηρία τη σκέψη του ορθολογικά δρώντος υποκειμένου, η θεωρία που προσέφερε ο Becker εστιάζει στην ανάλυση κόστους-οφέλους, στην οποία προβαίνει ο υποψήφιος δράστης προτού λάβει την απόφαση της εγκληματικής πράξης. Η απόφαση της εγκληματικής πράξης για μια μερίδα εγκληματιών αποτελεί τη λογική επιλογή έπειτα από στάθμιση αφενός της προσδοκώμενης ωφέλειας, η οποία περιλαμβάνει οικονομικά και ψυχολογικά οφέλη, και αφετέρου, του πιθανολογούμενου κόστους, το οποίο εστιάζεται στις πιθανότητες σύλληψης, καταδίκης και πραγματικής έκτισης της ποινής. Η μεταβολή των πιθανοτήτων σε κάθε ένα από τα στοιχεία της ανάλυσης μεταβάλλει το τελικό αποτέλεσμα ως προς την εκδήλωση της εγκληματικής πράξης. Προεκτείνοντας τη θεωρία του Becker στο μοντέλο της αγοράς, μπορούμε να εντοπίσουμε την ισορροπία στο σημείο όπου τέμνεται η προσφορά των προσβολών ή αλλιώς το ποσοστό του εγκλήματος και η ζήτηση ως παροχή παράνομων αγαθών και υπηρεσιών. Μείωση, επομένως, της ζήτησης συνεπιφέρει μείωση της προσφοράς και μείωση της εγκληματικής συμπεριφοράς. Σκόπιμος είναι, συνεπώς, ο εντοπισμός των παραγόντων που επηρεάζουν τη ζήτηση, μεταξύ των οποίων σημαντικό στοιχείο αποτελεί το κόστος αποτροπής συνυφασμένο με τους επιμέρους παράγοντες που θα καταστήσουν τη διάπραξη του εγκλήματος περισσότερο κοστοβόρα και λιγότερο προκριτέα ορθολογικά επιλογή. Αύξηση του κόστους του εγκλήματος μπορούν να επιφέρουν περισσότεροι παράγοντες, όπως για παράδειγμα η αύξηση του πλαισίου ποινής ή των πιθανοτήτων σύλληψης, μέσα

από την ενίσχυση των αρμόδιων φορέων και του νομοθετικού πλαισίου ή η αύξηση των χρηματικών προστίμων σε περιπτώσεις εγκλημάτων που ανάγονται σε οικονομικά κίνητρα. Τα τελευταία μάλιστα ενδέχεται να συνεπιφέρουν επιπλέον οφέλη ενισχύοντας τον κρατικό μηχανισμό με έσοδα που μπορούν να αξιοποιηθούν για κοινωνικούς σκοπούς και τεχνολογική ενίσχυση των υπαρχόντων μηχανισμών εντοπισμού των δραστών, αντισταθμίζοντας περαιτέρω το κόστος της φυλάκισης ως επιβαρυντικού για το κράτος μηχανισμού. Πρόσθετα κόστη για το δράστη δύναται να επιφέρει η θεμελίωση ευθύνης των παρόχων υπηρεσιών Διαδικτύου για την παράνομη δραστηριότητα των χρηστών, η οποία, ωστόσο, δε θα πρέπει να εκτείνεται ως το σημείο να μετατίθεται η ευθύνη του κρατικού μηχανισμού στους ενδιάμεσους φορείς, γεγονός που πέρα από τις νομικές προβληματικές διαστάσεις ενέχει τον κίνδυνο περιορισμού των ευεργετημάτων της τεχνολογίας για μεγάλη μερίδα «ύποπτων» χρηστών.

Στην αντίποδα, η ενίσχυση ενός μοντέλου εσωτερικής υπακοής στο Δίκαιο στηριζόμενου στη σχετική επιστημονική έρευνα μπορεί να ενισχύσει την αποχή από την εγκληματική δραστηριότητα χωρίς να δεσμεύει κρατικούς πόρους τόσο σε τεχνολογικό εξοπλισμό όσο και σε ανθρώπινο δυναμικό, οι οποίοι είναι εκ των πραγμάτων πεπερασμένοι. Η έννοια της εσωτερικής υπακοής στο Δίκαιο αντλεί τη δυναμική της από αυτό που τα μέλη της κοινωνίας αντιλαμβάνονται ως δίκαιο και κοινωνικά ορθό. Αυτό προϋποθέτει την ανίχνευση των περισσότερων παραγόντων που επηρεάζουν τη διαμόρφωση της ανθρώπινης συμπεριφοράς, μεταξύ των οποίων η κοινωνική ανισότητα, τα παιδικά τραύματα ή η έκθεση σε συμπεριφορές που συντείνουν στην αύξηση των αισθημάτων μειονεκτικότητας, ανεπάρκειας, αδικίας ή ψυχικού πόνου και καθιστούν την εκδηλούμενη παρεκκλίνουσα συμπεριφορά αναγκαίο τρόπο εκτόνωσης αντί της αυτοκαταστροφής. Η δημιουργία, επομένως, κοινωνικών μοντέλων στοχευόντων στην καλλιέργεια της εσωτερικής υπακοής προς το κοινωνικά ορθό και βασιζόμενων στα συμπεράσματα περισσότερων επιστημών, όπως η ανθρωπολογία, η ψυχολογία, η κοινωνιολογία και η εγκληματολογία, αντί της πρόταξης ενός αμιγώς τιμωρητικού μηχανισμού, δύναται να παράσχει σημαντικά οφέλη σε ευρύτερο επίπεδο.

Περαιτέρω, στη βάση της αναζήτησης αποτρεπτικών παραγόντων ικανών να συντείνουν στον περιορισμό της εγκληματικής δραστηριότητας στο Διαδίκτυο με γνώμονα τον τρόπο ανταπόκρισης στα περισσότερα ερεθίσματα, η πρόταση του Lessig εστιάζει στη δυναμική του νόμου, της κοινωνικής νόρμας, της αγοράς και της

αρχιτεκτονικής της τεχνολογίας. Οι τέσσερις αυτές δυναμικές δεν είναι ανεξάρτητες μεταξύ τους αλλά αλληλεπιδρούν, δυνάμενες να επιφέρουν αποτελεσματικές συνταγές, συμπορευόμενες αρμονικά, μέσα από την ενεργοποίηση περισσότερων λειτουργιών ειδικά προσαρμοσμένων στις ιδιομορφίες του Διαδικτύου και των συνεπακόλουθων απειλών. Ειδικότερα, ο ρόλος του νόμου στην πρόληψη εγκληματικών συμπεριφορών είναι κομβικός, δεν πρέπει, ωστόσο, να οράται ανεξάρτητα από το κοινωνικό πλαίσιο με το οποίο αλληλεπιδρά. Μια ποινή δυσανάλογη προς το διαπραττόμενο έγκλημα ή ατελέσφορη να οδηγήσει στο σωφρονισμό και τη μη επανάληψη της αποδοκιμαζόμενης συμπεριφοράς είναι βέβαιο πως δε θα συμβάλει στην αντιμετώπιση ενός φαινομένου με αυξανόμενη δυναμική. Αντιστοίχως, η απουσία δομών ουσιαστικής ένταξης ή επανένταξης στο κοινωνικό σύνολο ενισχύει τη διαιώνιση του φαινομένου. Το ποσοστό του εγκλήματος καθορίζεται από τις δυνάμεις της αγοράς, η οποία αδυνατεί, ωστόσο, να οδηγήσει στα καλύτερα δυνατά και κοινωνικά βέλτιστα αποτελέσματα μόνη της. Στο πλαίσιο αυτό, η εξωτερική παρέμβαση μέσα από έναν κοινωνικά δομημένο νομοθετικό και τεχνολογικό σχεδιασμό που θα αξιοποιεί τις τεχνολογικές δυνατότητες και θα συνδυάζει τη δράση περισσότερων φορέων, αξιολογείται, κατά τη άποψη της γράφουσας, ως προκριτέα μέθοδος αντιμετώπισης των τεχνολογικών απειλών.

Στην κατεύθυνση αυτή, σημαντική μπορεί να αποδειχθεί η παράλληλη προώθηση μιας στρατηγικής τριών μερών που θα περιλαμβάνει τους παρόχους υπηρεσιών ως ενδιάμεσους φορείς, τα υποψήφια θύματα και τους ίδιους τους δράστες. Οι πάροχοι υπηρεσιών αποτελούν ενδιάμεσους φορείς με κεντρική θέση στην τέλεση του ηλεκτρονικού εγκλήματος. Για το λόγο αυτό, το ζήτημα της θεμελίωσης ευθύνης σε βάρος των ενδιάμεσων παρόχων έχει απασχολήσει την έννομη τάξη εγείροντας ζητήματα για τις απαιτούμενες προϋποθέσεις και το θεμιτό βαθμό ευθύνης, ωστόσο, όπως προεκτέθηκε, δεν παραβλέπεται ο κίνδυνος αδικαιολόγητης μετακύλησης του βάρους διατήρησης της τάξης που παραδοσιακά ανήκει στον κρατικό μηχανισμό και πρόκλησης μιας πιθανής τραγωδίας των ψηφιακών αντικοινών (‘tragedy of the digital anticommons’) που θα πλήξει τελικώς τα συμφέροντα του κοινωνικού συνόλου. Από την άλλη, η συμβολή των ενδιάμεσων παρόχων στον εντοπισμό των δραστών και η θεμελίωση ευθύνης, υπό τις προϋποθέσεις που τάσσει το νομοθετικό σύστημα, αυξάνουν το κόστος διάπραξης του εγκλήματος, καθότι ο υποψήφιος δράστης θα πρέπει να προσπελάσει ένα επιπλέον εμπόδιο. Στο πλαίσιο αυτό, η θεμελίωση της ευθύνης των παρόχων κρίνεται

σημαντική, πλην όμως, θα πρέπει, κατά τη γνώμη της γράφουσας να περιορίζεται σε εύλογα πλαίσια χωρίς να καταστρατηγούνται οι αρχές της έννομης τάξης.

Επιπλέον, τα υποψήφια θύματα καλούνται να θωρακιστούν προκειμένου να ελαχιστοποιήσουν την επερχόμενη ζημία χρησιμοποιώντας εργαλεία αυτοάμυνας, όπως λογισμικά και ασφαλείς κωδικούς, τα οποία, στις περισσότερες περιπτώσεις, εξαντλούνται στα εργαλεία παθητικής αυτοάμυνας που αρκετές φορές αποδεικνύονται ανεπαρκή. Η σκέψη αυτή τροφοδότησε την εξέταση ενός μοντέλου ενεργητικής αυτοάμυνας το οποίο θα μπορούσε, υπό προϋποθέσεις, να νομιμοποιεί ορισμένες μορφές αυτοδικίας στο βαθμό που κρίνονται αναγκαίες και αναλογικές ενόψει της επαπειλούμενης προσβολής. Η αυτοδικία στο Διαδίκτυο αποτελεί σύνηθες φαινόμενο που σε ορισμένες περιπτώσεις δύναται να επιφέρει θετικά αποτελέσματα, ενώ σε ορισμένες άλλες περιπτώσεις δύναται να επισύρει σημαντικούς κινδύνους για τα δικαιώματα τρίτων. Παρά τις προβληματικές διαστάσεις, η πράξη έχει αποδείξει ότι τέτοιες συμπεριφορές δεν ανάγονται στη σφαίρα του υποθετικού, συνεπώς, η θεσμοθέτηση του ήδη συμβαίνοντος και η ένταξή του σε ένα πλαίσιο νομιμότητας, είναι προτιμότερη από την απουσία νομοθετικού πλαισίου, ελλείψει του οποίου οι αυτόδικες συμπεριφορές οξύνονται.

Ο τελευταίος πυλώνας της στρατηγικής εστιάζει στους δράστες και τη δημιουργία ενός μοντέλου διαμόρφωσης προτιμήσεων μέσα από το σχηματισμό μιας ορθής κουλτούρας hacking. Στο πλαίσιο αυτό, η νομοθέτηση και χρηματοδότηση διαγωνισμών hacking, οι οποίοι ήδη διεξάγονται τα τελευταία χρόνια σε ολοένα μεγαλύτερη κλίμακα, προσφέρει μια εναλλακτική προοπτική στην προσφορά θετικών κινήτρων, όπως οι χρηματικές αμοιβές ή οι εργασιακές ευκαιρίες. Μολονότι τα οφέλη της συμβολής αυτού του μοντέλου στην καταπολέμηση του ηλεκτρονικού εγκλήματος τίθενται υπό αμφισβήτηση, καθώς επίσης, απευθύνεται σε συγκεκριμένες μόνο μορφές εγκληματικής δράσης στο Διαδίκτυο, αποτελεί, κατά τη γράφουσα, μια φιλόδοξη προοπτική που σε περίπτωση επιτυχούς υπαγωγής σε νομοθετικά πλαίσια, δύναται να επιφέρει θετικά αποτελέσματα, αποδεσμεύοντας, περαιτέρω, πόρους που μπορούν να χρησιμοποιηθούν υπέρ της καταπολέμησης λοιπών μορφών εγκληματικής δράσης.

Σε κάθε περίπτωση, η δημόσια αφύπνιση των υποψήφιων θυμάτων και η υπό προϋποθέσεις παροχή πρόσθετων κινήτρων για λήψη κατάλληλων μέτρων με παράλληλη

προώθηση μιας ορθής κουλτούρας χρήσης του Διαδικτύου από όλες τις πλευρές συνιστούν αναγκαία συστατικά ενός συλλογικού πλαισίου δράσης που απαιτεί στοχευμένες ενέργειες σε περισσότερα επίπεδα. Ακολούθως, τα περισσότερα επίπεδα δράσης προϋποθέτουν τη συνεργασία περισσότερων φορέων του ιδιωτικού και του δημοσίου τομέα, από τους οποίους, όπως εκτέθηκε, ο πρώτος συνήθως προηγείται σε τεχνολογική γνώση και υλικοτεχνικό εξοπλισμό. Επιπλέον, οι πόροι του κράτους είναι πεπερασμένοι με αποτέλεσμα η διάθεση υλικού εξοπλισμού και τεχνικών γνώσεων να είναι per se περιορισμένη. Ενόψει αυτού η συμβολή του ιδιωτικού τομέα από κοινού με την κρατική δράση συντείνει στην αποτελεσματικότητα αυτού του πλουραλιστικού εγχειρήματος που επιδιώκει να αντιμετωπίσει συνολικά ένα φαινόμενο επιδημικών διαστάσεων, το οποίο, κατά την άποψη της γράφουσας, μόνο με συλλογικές προσπάθειες από πλείονες φορείς δύναται να οριοθετηθεί. Τον τελευταίο λόγο οφείλει να έχει το Δίκαιο μέσα από την επιδίωξη ενός πραγματικά εναρμονισμένου νομοθετικού πλαισίου μεταξύ των κρατών, τα οποία πρέπει περισσότερο από ποτέ να συνεργαστούν αποτελεσματικά τόσο σε επίπεδο καταστολής όσο και πρόληψης για την επίτευξη κοινωνικά πρόσφορων και βέλτιστων λύσεων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- **Ελληνόγλωσση:**

Βλαχόπουλος, Κωνσταντίνος. 2007. *Ηλεκτρονικό έγκλημα.* Νομική Βιβλιοθήκη.

Δαλακούρας, Θεοχάρης Ι. 2018. *Ηλεκτρονικό έγκλημα*. Νομική Βιβλιοθήκη.

Κακαβούλης, Κωνσταντίνος. 2015. «Η συμμετοχική ευθύνη των ενδιάμεσων παρόχων Internet στα διαδικτυακά εγκλήματα.» *ΠοινΧρ* 2015.

Κιούπης, Δημήτριος. 1999. *Ποινικό Δίκαιο και Internet*. Π.Ν. Σάκκουλα.

Κιούπης, Δημήτριος. 1998. «Ποινική ευθύνη των εταιρειών παροχής πρόσβασης στο Internet». *ΠοινΧρ* 1998.

Μανωλεδάκης, Ι. & Ν. Παρασκευόπουλος. 1999. *Εγχειρίδιο Ποινικού Δικαίου*. Εκδόσεις Σάκκουλα.

Μαργαρίτης, Λάμπρος Χ. 2009. *Ποινικό Δίκαιο και Διαδίκτυο*. Νομική Βιβλιοθήκη.

Μυλωνόπουλος, Χ. Χρίστος. 2007. *Ποινικό Δίκαιο/Γενικό Μέρος*. Π.Ν. Σάκουλας: Δίκαιο και Οικονομία.

Σεβαστίδης, Χαράλαμπος Θ. 2019. «Σημεώσεις για τον νέο Ποινικό Κώδικα.» *lawspot.gr* (1/7/2019) https://www.lawspot.gr/sites/default/files/images/nea/simeiosis-poiniko.pdf

Σφακιανάκης, Εμμανουήλ. 2016. *Ο Κώδικας του Διαδικτύου.* All about Internet.

Χαραλαμπάκης, Αριστοτέλης Ι. 2019. *Ο Νέος Ποινικός Κώδικας: Μια πρώτη ερμηνευτική προσέγγιση του Ν. 4619/2019.* Νομική Βιβλιοθήκη.

Χρίστος Ι. Μυλωνόπουλος (2006), Ποινικό Δίκαιο, Ειδικό Μέρος, Εγκλήματα κατά της Ιδιοκτησίας και της περιουσίας [άρθρο 372-406 ΠΚ], Β' Έκδοση, Π.Ν. Σάκκουλας

- **Ξενόγλωσση:**

Antolin-Jenkins, Vida M.. 2005. ‘‘Defining the Parameters of Cyberwar Operations: Looking for Law in all the wrong places.’’ *Naval Law Review* LI 51: 132-174.

Becker, Gary S. 1968. “Crime and Punishment: An economic approach.” *Journal of Political Economy* Vol. 76: 169-217.

Biegel , Stuart . 2003. *Beyond our control? Confronting the Limits of Our Legal System in the Age of Cyberspace*. The MIT Press.

Blumstein, Alfred, Jacqueline Cohen & Daniel Nagin. 1978. ‘‘Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rate.’’ Report. United States of America.

Branscomb, Anne W. 1990. “Programs and Computer Rogues: Tailoring the Punishment to fit the Crime.” *Rutgers Computer & Technology Law Journal* Vol. 16:1-6.

Brenner, Susan W. 2007. *Law in an Era of Pervasive Technology*. New York: Oxford University Press.

Brenner, Susan W. 2007. “Should online defamation be criminalized?”. *Mississippi Law Journal* Vol. 76: 1-58.

Carlone, Ralph V. 1989. *Computers Security: Virus highlights need for improved internet management*. Report to the Chairman, Subcommittee on Telecommunications and Finance, Committee on Energy and Commerce, House of Representatives. United States General Accounting Office.

Clark, J. R. & W. L. Davis. 1995. ‘‘A Human Capital Perspective on Criminal Careers.’’ Applied Business Research.

Collier, P.A. & D.J. Spaul. 1992. “Problems in Policing Computer Crime.” *Policing and Society* 2: 307-320.

Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. 2007. “Towards a general policy on the fight against cybercrime”. *European Union Website* (22/5/2007) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14560&from=EN

‘‘Computer Crimes.’’2017. *American Criminal Law Review* Vol. 54:1025-1071.

‘‘Computer Crime Deterrence.’’ 1986. *American Journal Criminal Law* Vol. 13: 391-416.

‘‘Computer Hacking Suspect A Legend To Some, A Threat To Others.’’ 1989. *NP News* (3/1/1989) https://apnews.com/article/b83c6ccc6411f742195296ef7937cc59

‘‘Computer-Related Crimes.’’1995. *American Criminal Law Review* p. 183-210.

Council of Europe, Committee of Ministers. 1989. ‘‘Minimum List of Offences Necessary for a Uniform Criminal Policy.’’ *rm.coe.int* (18/1/1989) https://rm.coe.int/1680500b15

Csonka, Peter . 2006. “The Council of Europe’ s Convention on Cyber-crime and other European Initiatives.” Revue Internationale de Droit Penal 77: 473-501.

“Cybercrime, fraud cost UK nearly $14 billion.” 2017. *Business Insurance* (22/6/2017) https://www.businessinsurance.com/article/20170622/STORY/912314045/Cybercrime

Dau-Scmidt, Kenneth G. 1990. “An Economic Analysis of the Criminal Law as a Preference Shaping Policy.” *Duke Law Journal* p. 1-38.

De Bolle, Catherine. 2019. *IOCTA Internet Organized Crime Threat Assessment 2019.* Europol: European Cybercrime Centre.

De Bolle, Catherine. 2018. *International Organized Crime Threat Assessment IOCTA 2018.* Europol: European Cybercrime Centre.

Draper, Tony. 2002. ‘‘An Introduction to Jeremy Bentham’ s Theory of Punishment.’’ *Journal of Bentham studies*. UCL Bentham Project. P. 1-17.

Fifth Report on Card Fraud 2018. *European Central Bank* (26/9/2018) https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html

Fisher, Talia. 2014. *Economic Analysis of Criminal Law.* The Oxford Handbook of Criminal Law.

Ghosh, Sumit & Elliot Turrini. 2010. *Cybercrimes: A Multidisciplinary Analysis*. Springer.

Glaeser, Edward, Bruce Sacerdote & Jose Scheinkman,. 1996. “Crime and social interactions.” *Quarterly Journal of Economics* p. 507-548.

Goffman, Erving. 1963. *Stigma: Notes on the Management of Spoiled Identity*. Simon & Schuster Inc.

Goldberg, Rafi. 2016. “Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities.” National Telecommunications and Information Administration United States Department of Commerce (13/5/2016) https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

Goldstein, Joseph. 2014. ‘‘Street Stops Still a ‘Basic Tool’, Bratton says.’ *New York Times* (4/3/2014) https://www.nytimes.com/2014/03/05/nyregion/bratton-says-street-stops-and-fighting-low-level-crime-will-remain-crucial.html

Grabosky, Peter. 2016. *Cybercrime, Keynotes in Criminology and Criminal Justice Series.* New York: Oxford University Press.

Green, Christofer R. 2015. “Reverse Broken Windows.” *Journal of Legal Education* 65: 265-276.

Greenberg, Andy. 2013. “Google Offers $3.14159 Million In Total Rewards For Chrome OS Hacking Contest.” *Forbes* (28 Jan 2013), https://www.forbes.com/sites/andygreenberg/2013/01/28/google-offers-3-14159-million-in-total-rewards-for-chrome-os-hacking-contest/#203011a91d20

Gronin, Cat. 2019. “The Growing Threat of Cyberterrorism Facing the U.S.” *American Security Project* (25 Jun 2019) https://www.americansecurityproject.org/the-growing-threat-of-cyberterrorism-facing-the-us/

Holloway, Michael. 2016. “Stuxnet Worm Attack on Iranian Nuclear Facilities.” *Stanford University* (16 Jul 2016) http://large.stanford.edu/courses/2015/ph241/holloway1/

Holmes, Aaron. 2019. “Google is offering a $1.5 million reward to anyone who can pull off a complex Android hack.” *Business Insider* (22 Nov 2019) https://www.businessinsider.com/google-bug-bounty-increase-android-hack-2019-11

Jameson, Sarah. 2008. “ Cyberharassment: Striking a Balance between free speech and privacy.” *CommLaw Conspectus: Journal of Communications Law and Technology Policy* Vol. 17: 231-266.

Jennings, Robert & Arthur Watts. 2008. *Oppenheim’s International Law.* Oxford Public International Law Vol. 1.

Jescheck, H.-H. & Thomas Weigent. 1978. *Lehrbuch des Strafrechts. Allgemeiner Teil*. Berlin: Duncker & Humblot.

Jiow, Hee Jhee. 2013. ‘‘Cyber Crime in Singapore: An Analysis of Regulation based on Lessig’s four Modalities of Constraint.’’ *International Journal of Cyber Criminology.*

Karnow, Curtis E.A.. 2005. ‘‘Launch on Warning: Aggressive Defense of Computer Systems.’’ *Yale Journal of Law and Technology* Vol. 7: 87-102.

Katyal, Neal K. 2005. ‘‘Community Self-Help.’’ *The Journal of Law, Economics & Policy* p. 33-67.

Katyal, Neal K. 2002. ‘‘Architecture as Crime Control.’’ *111 Yale Law Journal* p. 1039-1139.

Katyal, Neal K. 2001. “Criminal Law in Cyberspace”. University of Pennsylvania Vol. 149: 1003-1112.

Kertysova, Katarina , Erik Frinking, Koen van den Dool, Aleksandar Maricic & Kumar Bhattcharyya. 2018. *Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks.* European Economic and Social Committee Study. The Hague Centre for Strategic Studies.

Kesan, Jay P. & Karol M. Hayes. 2012. ‘‘Mitigative Counterstriking: Self-Defense and deterrence on cyberspace.’’ *Harvard Journal of Law & Technology*. Vol. 25: 431-542.

Kesan, Jay P.& Ruperto Majuca. 2009. “Optimal Hackback.” *Chicago-Kent Law Review* Vol. 84: 831-839.

King, Leo. 2011. “NASDAQ Out of Date Software Helped Hackers.” *CSO Unites states* (22/11/2011) https://www.csoonline.com/article/2130229/nasdaq-out-of-date-software-helped-hackers--report.html

Koops, Bert-Jaap & Susan W. Brenner. 2006. *Cybercrime and Jurisdiction*. Information Technology and Law Series. Asser Press.

Kshetri, Nir. 2006. *The Simple Economics of Cybercrimes.* IEEE Security and Privacy Magazine.

Lessig, Lawrence. 1999. *Lessig's four modalities of constraint*. Codes and Other Laws in Cyberspace. New York: Basic Books.

Levy, Steven. 1984. *Hackers: Heroes of the Computer Revolution*. Octal Publishing Inc.

Lewis, C. Brian. 2004. "Prevention of Computer Crime amidst International Anarchy." *The American Criminal Law Review.* Vol. 41: 1353-1372.

Lewis, James 2018. "Economic Impact of Cybercrime: At $600 Billion and Counting-No slowing down." Center for Strategic and International Studies Report (21/2/2018) https://www.csis.org/analysis/economic-impact-cybercrime.

Lewis, James. 2013. "The Economic Impact of Cybercrime and Cyber Espionage." *Center for Strategic and International Studies* (22/7/2013) https://www.csis.org/analysis/economic-impact-cybercrime-and-cyber-espionage

Link, Nathan W., James M. Kelly, Joseph R. Pitts, Kelly Waltman-Spreha & Ralph P. Taylor. 2017. ''Reversing Broken Windows: Evidence of Lagged, Multilevel Impacts of Risks Perception on Perception on Incivility.'' *Crime & Delinquency*. Vol. 63: 659-683.

Maass, Peter & Megha Rajagopalan. 2012. "Does Cybercrime Really Cost $1 Tril- lion?" *ProPublica* (1 Aug 2012), https://www.propublica.org/article/does-cybercrime-really- cost-1-trillion

Majuca, Ruperto P. & Kesan, Jay P. 2009. *Hacking back: Optimal Use of Self-Defense in Cyberspace.* Illinois Public Law and Legal Theory Papers Series Research Papers Series No 08-20.

Mc Adams, Richard H. & Thomas S. Ulen. 2008. "Behavioral Criminal Law and Economics." *University of Chicago Law School. John M. Olin Law & Economics Working Paper* No 440.

McGuire, Mike & Samantha Dowling. 2013. *Cyber crime: A review of the evidence.* Summary of key findings and implications. Home Office Research Report 75.

Meares, Tracey L., Neal Katyal & Dan M. Kahan. 2004. "Updating the Study of Punishement." *Stanford Law Review* Vol. 56:1171-1210.

Miller, Arthur R. 2004. ''The Emerging Law of the Internet.'' *Law and the Internet: Georgia Law Review.* Vol. 38: 991-1007.

Monteiro, Renato L. 2011. ''Economic and Social Analysis of Cybercrimes.'' https://www.oabsp.org.br/noticias/2011/10/17/analise_economica_en.pdf

Monteiro, Renato L. 2010. Crimes Eletronicos: Uma Analise Economica e Constitutional. Fortaleza-Ceara: Univesidade Federal Do Ceara: Faduldade De Direito.

Mookherjee, Dilip & I. P. L. Png. ‘‘Marginal Deterrence in Enforcement of Law. *Journal of Political Economy*. Vol. 102: 1039-1066

Overbeck, Wayne & Genelle Belmas. 2012. *Major Principles of Media Law: 2012 Edition.* U.S.A.: Wadsworth Cengage Learning.

Owen, Tim, Wayne Noble & Faye C. Speed. 2017. *New Perspectives on Cybercrime.* Palgrave Studies in Cybercrime and Cybersecurity.

Piliavin, Irving, Rosemary Gartner, Craig Thornton & Ross L. Matsueda. 1986. Crime, Deterrence, and Rational Choice 51 American Sociological Review Vol. 51: 101-119.

Posner, Richard. 1985. ‘‘An Economic Theory of the Criminal Law.’’ *Columbia LR* 1195.

Poulsen, Kevin. 2011. Kingpin: How *One Hacker Took Over The Billion Dollar Cybercrime Underground*. Crown Publishing Book.

Quinn, Kevin. 1978. ‘‘Computer crime: A growing corporate dilemma.’’ *Maryland Law Forum* p. 48-62.

Richards, Robert D. & Clay Calvert. 2008. “Untangling child pornography from the adult entertainment industry: An inside look at the Industry’s effort to protect minors”. *California Western Law Review* Vol. 44: No2: 511-556.

Rogers, M. 2006. “The development of a meaningful hacker taxonomy: A two dimensional approach.” *Purdue University: Computer and Information Technology.* Tech Report 2005-43.

Rollins, John W. 2015. *Cyberwarfare and Cyberterrorism: In Brief*. Congressional Research Service 7-5700.

SAH, Raaj K. 1991. ‘‘Social osmosis and patterns of crime.’’ *Journal of Political Economy.* Vol. 99: 1272–1295.

Schmitt, Michael N. 2017. *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press.

Shackelford, Steve. 1992. ‘‘Computer-Related Crime: An International Problem in Need of an International Solution.’’ *Texas International Law Journal* Vol. 27:480-504.

Simundic, Slavko , Danijel Brbaric & Sinisa Franjic. 2016. Safety *on Electronic Communication and Computer Crime*. Split.

Sinrod, Eric J. & William P. Reilly. 2000. ‘‘Cyber-Crimes: A practical Approach to the Application of Federal Computer Crimes Law.’’ *Computer High Technology Law Journal* Vol. 16: 178-232.

Sklerov, Matthew J. 2009. ‘‘Solving the Dilemma of State Responses to Cyberattacks: A Justification for the use of Active Defenses Against States Who Neglect Their Duty to Prevent.*’’ 201 Military Law Review* 1 p. 1-85.

Smith, Heather J., Tom R. Tyler, Yuen J. Huo, Daniel J. Ordiz & E. Allan Lind. 1998. ‘‘The Self-Relevant Implications of the Group-Value Model: Group Membership. Self-Worth and Treatment Quality.’’ *Journal of Experimental Social Psychology* 34: 470-493.

‘‘Star Wars kip is top viral video.’’ 2006. *BBC News* (27/11/2006) http://news.bbc.co.uk/2/hi/entertainment/6187554.stm

Stigler, George J. 1970. ‘‘The Optimum Enforcement of Laws.’’ *Journal of Political Economy* 78: 526-536.

Sunstein, Cash R., Christina Jolls & Richard H. Thaler. 1998. “A behavioral Approach to Law and Economics.” *Stanford Law Review.*

Sussmann, Michael A. 1999. “The Critical Challenges from the International High-Tech and Computer-Related Crime at The Millenium.” *Duke Journal of Comparative & International Law* p. 451-489.

“The Melissa Virus, An $80 Million Cyber Crime in 1999 Foreshadowed Modern Threats.” *FBI News* (25/5/2019) https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519

Timothy, S. Wu. 1997. ‘‘Computer Crime.’’ Harvard Journal of Law & Technology Vol. 10: 648-665.

“Unique Cyber Exercise for the Private Sector is Taking Place in Tallinn.” *e-estonia* (March 2019) https://e-estonia.com/cyber-exercise-for-private-sector-tallinn/

Viano, Emilio C. 2017. *Cybercrime, Organized Crime and Societal Responses*. Springer.

We Protect Global Alliance to End Child Sexual Exploitation online. *European Commission: Migration and Home Affairs*. https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse_en

Whitney-Morris, Candace. 2018. “At the largest private hackathon on the planet Microsoft employees fire up ideas by the thousands.” *Microsoft Life* (23 Jul 2018) https://news.microsoft.com/life/hackathon/

Wible, Brent. 2003. ‘‘A Site Where Hackers are Welcome: Using Hack-in Contests to Shape Preferences and Deter Computer Crime.’’ *The Yale Law Journal* Vol. 112:1577.

Yuccas, Jamie. 2019. “80 indicted in online fraud scheme that stole millions.” *CBS News* (22 Aug 2019), https://www.cbsnews.com/news/online-fraud-scheme-that-stole-million-dozens-indicted-today-2019-08-22/

Αποφάσεις:

Airlina Coach Service and Sky Limousine Company v. Alan Giang Lee
Amphenol Corp. v. Paul
Burnett v. State
EF Cultural Travel BV v. Explorica
Florida v. Jardines
Int l Airport Ctrs. v. Citrin
Katz v. United States
Kyllo v. United States
Lavan v. City of L.A.
Leventhal v. Knapel
Licra v. Yahoo
Mink v. Knox
O' Connor v. Ortega
Smith v. Maryland
State v. Lehman
Unites States v. Ardit Ferizi
United States v. Brewer
United States. v. Carron
Unites States v. Davis
Unites States v. Forrester
United States v. Heckencamp
United States v. John
United States v. Jones
United States v. Long
United States v. Miller
United States v. Mutnick
United States v. Nosal
United States v. Rodriguez
United States v. Sheier
United States v. Simons
United States v. Steiger
United States. v. Tanimowo
United States v. Trotter
United States v. Williams
WEC Carolina Energy Solutions v. Miller
ECHR, Halford v. United Kingdom